STATE-OF-THE-ART OF SECURE ICT LANDSCAPE (DRAFT VERSION)

NIS PLATFORM

WORKING GROUP 3 (WG3)

Editors:

Mari Kert (European Organisation for Security)

Javier Lopez (UMA)

Evangelos Markatos (FORTH)

Bart Preneel (LSEC)

Table of contents

Contributors

STEERING COMMITTEE

Mari Kert, *European Organization for Security*

Javier Lopez, *University of Malaga*

Evangelos Markatos, *SysSec Project Manager, Foundation for Research and Technology - Hellas*

Bart Preneel, *KU Leuven*

CONTRIBUTORS

Magnus Almgren, *Chlamers University of Technology*

Elias Athanasopoulos, *FORTH*

Henk Birkholz, *Fraunhofer SIT*

Hugh Boyes, *University of Warwick*

Sabrina de Capitani di Vimercati, *Università degli Studi di Milano*

Hervé Debar, *Télécom SudParis*

Sotiris Ioannidis, *FORTH*

Roy Isbell, *University of Warwick*

Nicola Jentzsch, *DIW*

Wouter Leibbrandt, *NXP Semiconductors*

Joachim Posegga, *University of Passau*

Michalis Polychronakis, *Columbia University*

Vassilis Prevelakis, *Technical University, Braunschweig*

Ali Rezaki, *Tubitak*

Rodrigo Roman, *University of Malaga*

Carsten Rudolph, *Fraunhofer SIT*

Pierangela Samarati, *Università degli Studi di Milano*

Bjornar Solhaug, *SINTEF*

Christophe Sprenger, *ETH Zurich*

Theo Tryfonas, *University of Bristol*

Paulo Verissimo, *University of Lisbon*

Tim Watson, *University of Warwick*

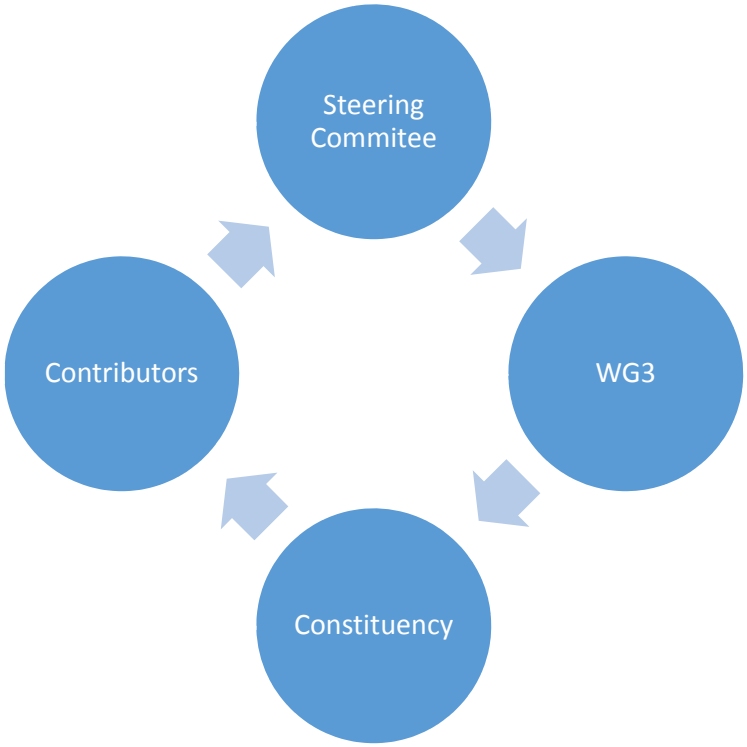
PROJECTS

CAPITAL, CYSPA, ECRYPT, NESSOS, SysSec

Executive Summary

This deliverable is part of the European Commission Network and Information Security Platform, Working Group 3 (WG3) on Secure ICT Research roadmap. Its purpose is to identify the most relevant technologies and areas that can contribute to the creation of the Strategic Research Agenda of WG3.

To complete the deliverable, a number of stakeholders at several different levels were engaged:



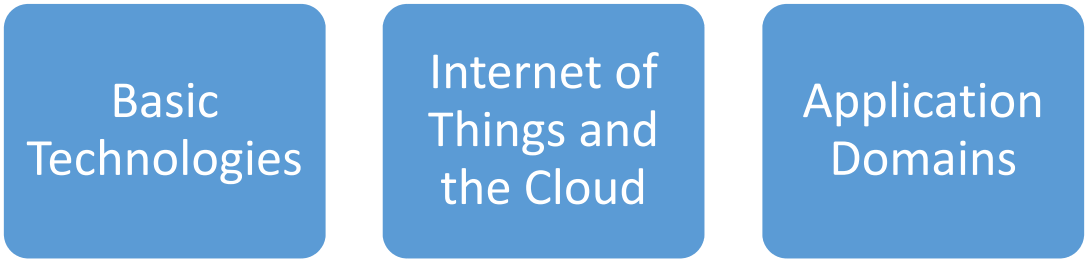
- **Steering Committee**: Charged with the overall implementation of the deliverable, the Steering Committee steered the work and the contributions of the rest of the community stakeholders
- **Working Group 3**: The Steering Committee frequently consulted the members of the Working Group 3 in order to receive feedback and contributions in the form of text and comments.
- **NIS constituency**: The Steering Committee periodically consulted members of several EU-funded projects as well as members of the Network and Information Security Platform in order to receive high-level feedback.
- **Contributors**: Those members of the NIS and WG3 groups that wanted, had the opportunity to contribute text and write sections (or parts of sections). [1]

The results of all these contributions were encoded in four sections:

1. **Introduction**. Overall introduction to the document.
2. **Basic Technologies**. This section lists the basis technologies or threats related to network and information security. Each technology/threat was described using the following structure:
    - **Introduction**: What is this technology about?
    - **State of the Art**: What is the state of the art in this area?
    - **Research Challenges**: What are the research challenges that need to be met in this area?
    - **Current Tools**: What are some current tools/systems that exist in this area?

[1] The contributors are outlined in page 4.

3. **Internet of Things – Cloud Computing**. We chose two emerging technologies (IoT and Cloud Computing) and decided to study them extensively. Two are the reasons for this choice:
    - These emerging technologies are very broad and may encompass several different basic technologies or types of threats.
    - These emerging technologies are expected to have a high penetration and high impact in the near future.
4. **Application Domains**. Although most of these domains (such as food, transportation, banking, defense, etc.) existed before the advancement of the Internet, their interaction with the digital world has created new and interesting interdisciplinary challenges that should be taken into account very seriously.



The constituency, through its contributions to the deliverable has identified several interesting challenges. Some of these include:

- **The security paradigm has changed**. Although traditional security approaches are based on the existence of a perimeter that needs to be protected, this paradigm does not hold anymore. We need to operate in a world where a perimeter is not there or has already been breached.
- **Predictive Monitoring**. Traditional security approaches take action *after* a security incident has occurred. Is it possible to predict security breaches *before* they happen? Can we start taking measures *before* we actually see an attack materialize?
- **Big Data**. We need to be able to process orders of magnitude more data that we do today. At the same time, we need to address the privacy concerns related to the collection and processing of such data.
- **The changing nature of authentication**. Currently most web systems use authentication methods based in one way or another in the traditional password paradigm. However, recent results, such as large-scale password leaks and poor password choices, show that passwords may not be effective authentication mechanisms for the years to come. We need to work on alternative approaches.
- **Support diversity**. Currently there exists hundreds of millions of devices with (almost) the same operating system and software. These “monocultures” are vulnerable to attacks. We need to support diversity that will bring robustness against attacks to specific vulnerabilities.

1 Introduction

The Network and Information Security Platform Working Group 3 (WG3) Secure ICT: Research and Innovation aims to address the issues related to cyber security research and innovation in the context of the EU Strategy for Cyber Security. WG3 identifies key challenges and desired outcomes in terms of innovation-focused, basic and applied research in the fields of cyber security, privacy, and trust. It proposes new ways to promote truly multidisciplinary research that fosters collaboration among researchers, industry, and policy makers.

The State-Of-The-Art of Secure ICT Landscapes deliverable is the first one among a series of other deliverables foreseen in the work program of WG3. The objective of the deliverable is to:

- Map current and existing technologies in the field of cybersecurity and privacy;
- Introduce and define these technologies;
- Identify threats and defences to these threats;
- Identify some of the outstanding research challenges;
- Map existing tools that are used in each of the existing technologies;
- Feed into the Strategic Research Agenda of the NIS Platform WG3.

The remainder of the deliverable is divided in three main sections:

- Firstly, this document maps **basic technologies** in cyber security. The structure of this section was developed in accordance to the ITU National Cybersecurity Strategy Guide Annex II[2] Technical Solutions that outlines and structures common cybersecurity technologies. This work establishes a thorough, technical foundation to serve as the basis for both the following sections and future roadmaps.
- The second part of the deliverable focuses on **Internet Things and Cloud computing** open challenges, models and current approaches.
- The third part of the deliverable introduces all the different **Application Domains** where cybersecurity is applied such as e-government, finance, energy, telecommunications etc.

It should be noted that the task of developing a structure and content for mapping of cybersecurity technologies is not easy. This was achieved through an extensive consultation of stakeholders involved in the activities of WG3.

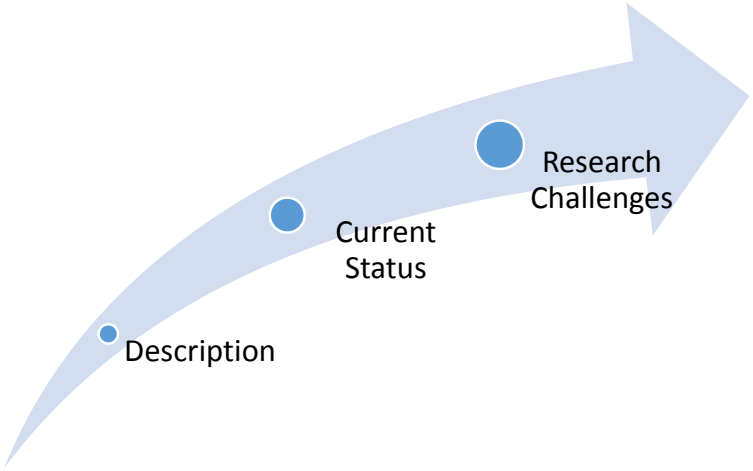
The editorial team of the State-Of-The-Art Secure ICT Landscapes deliverable hopes you will find this document useful in developing a clear overview of the current situation in ICT landscape and thanks all the contributors who took time to write the different sections.

[2] https://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf

2 Basic Technologies

2.1.1 Introduction and objectives

The purpose of this chapter is to introduce basic technologies in the area of cybersecurity, describe their current status and present the research challenges that they are likely to face in the near future.



2.2 Metrics in cybersecurity

2.2.1 Introduction

In civil engineering the question of whether and to what extent is a structure robust has been answered through the adoption of building codes, standards for the materials used, and modelling techniques, and can adequately predict the behaviour of a given structure. Cybersecurity, however, lacks most of the above, and hence it is extremely difficult to evaluate the level of security of a given system. The reasons for this state of affairs includes: (a) *rapid technological progress*: This makes established and proven techniques useless after only a few decades. For example the DES encryption algorithm introduced in the late 70s is no longer acceptable and hence any systems that mandate its use may no longer be considered secure, (b) *networking*: When computer systems are connected to a network, this changes the way they may be analysed, because the existence, or even the possibility of, a connection with other computing systems complicates the security analysis as it introduces additional dependencies and expands the attack surface, (c) *complexity*: as the capabilities of computing platforms increases, so does their complexity, e.g. compare the size of Windows NT 3.1 at 4.5 million lines of code (mloc), versus Vista at 50 mloc, (d) *the malicious nature of the threat*: Cybersecurity deals primarily with malicious intent. This implies that traditional analysis and functional testing are often inadequate measures of security in computer systems.

Any metrics selected should refer to the effect on critical aspects of the system, namely *integrity, confidentiality* and *availability*. Additionally, a number of steps (described by S. Payne in the publication "A Guide to Security Metrics"), must be taken in order to create a set of metrics: (1) Define the metrics program goal(s) and objectives, (2) Decide which metrics to generate, (3) Develop strategies for generating the metrics, (4) Establish benchmarks and targets, (5) Determine how the metrics will be reported, (6) Create an action plan and act on it, and, (7) Establish a formal program review/refinement cycle.

2.2.2 Current Status

Due to the importance of having good estimates of the security postures of systems, many efforts have been made over the years to define acceptable measures of security. For example, the International Systems Security

Engineering Association's "*SSE-CMM Project*," the National Institute of Standards and Technology's "*IT Security Assessment Framework*," the National Institute of Standards and Technology's "*Security Metrics Guide for Information Technology Systems*," the US Department of Defense's "*Information Assurance Readiness Project*," the ISO standard for "*Common Criteria*," and the "*Security Metrics"* guide published by the Center for Internet Security (CIS).

While the above efforts have met with limited acceptance by the community, the CIS guide appears to be going in the right direction and has been slowly gaining traction. It contains twenty-eight definitions of security metrics for seven business functions: Incident Management, Vulnerability Management, Patch Management, Application Security, Configuration Management, Change Management and Financial Metrics. Moreover, at 175 pages it is relatively easy to read and understand. Even so, it is far from the all purpose framework, that many security specialists seek, and often needs to be adapted to the particular environment or application.

Some researchers such as M. Satyanarayanan from Carnegie Mellon University, propose that, rather than metrics, a system of public challenges should be established to ascertain the level of security of a given system. For such challenges to be effective, however, they must be fair, and consistent, so that comparisons between challenges may be made.

2.2.3 Research Challenges

There is a need for the establishment of real world standards that are measurable, attainable, repeatable, and time-dependent (George Jelen, in "SSE-CMM security metrics"). Moreover, such metrics must be meaningful; there is no value in defining metrics on password use, or strength, when it has been established that passwords offer only a minimal level of protection. An important consideration is to identify which metrics are leading/lagging indicators of the system security posture and to consider the effects of this asynchronous nature into the security assessment.

2.3 Authentication, Authorization and Access Control

2.3.1 Authentication and Authorization

2.3.1.1 Introduction

Authentication is the process of identifying an entity, usually a user, to a system. ITU X.800 ISO 7498-2 defines authentication is a "service [...] provided for use at the establishment of, or at times during, the data transfer phase of a connection to confirm the identities of one or more of the entities connected to one or more of the other entities". This service provides confidence, at the time of usage only, that an entity is not attempting a masquerade or an unauthorised replay of a previous connection. One-way and mutual peer entity authentication schemes, with or without a liveness check, are possible and can provide varying degrees of protection. In particular the user for authenticating herself to a system has to provide information including:

- **Something you know:** a password, a PIN, or any token that can be remembered.
- **Something you have:** a token provided by something the user can carry with, such as an ATM card, a smart card, or a mobile phone.
- **Something you are:** any biometrics that can identify the user, such as a fingerprint.[3]

Various authentication scenarios can be considered based on the two entities (i.e. user and device) and the five methods (i.e. knowledge, ownership, biometrics, time, and location) below; some of these are used today, others appear rarely or not at all so far:

	User to Device	**Device to Device**	**Device to User**	**User to User**

[3] Some systems may also use **time** often in relation to **location** (i.e. proximity or absolute geolocation)

Knowledge	Standard passwords (ideally random and unique)	Shared secrets, Certificates	Shared secrets like keys	Shared secrets
Ownership	Secure tokens			ID documents, e.g. passport
Biometrics	Standard biometric features (fingerprints, etc.)	"Biometric" features e.g. PUFs, transceiver fingerprinting		Voice, style of writing, choice of words.
Time		"pairing" of devices		Agreed to or anticipated timing of actions
Location	Proximity (often correlated with time)	Proximity (often correlated with time)	Proximity	Proof of location e.g. based on time-dependent knowledge

2.3.1.2 Current Status

Today, text-based passwords are the dominant form for user-authentication for decades. Today, we are faced with a huge plethora of (1) services, all user-parameterized, (2) mobile apps, often based on user participation, and (3) web products and applications, which measure their popularity based on their user-base. All three types of developments, (1)-(3), require the creation of a user account, which, practically, means that a form of user authentication is required for accessing the service. Therefore, users are faced with practical scalability problems; they need to select, maintain, and keep secret tens of different passwords. Unfortunately, this translates to a recipe of selecting a few passwords and recycle them among different sites; an approach very vulnerable and fragile in the context of password leakage.

The need of password replacement is emerging. There have been recently proposed many different technologies, however, each one shares critical problems, which makes deployment in the wild hard. In short, compared to plain passwords, there have been proposed password managers and server-side solutions:

Password managers[4]: they delegate handling of passwords to software, however, in the presence of multiple devices software needs to be multi-platform and synchronized across all possible clients, therefore, critical usability issues make password-managers unattractive.[5]

Single sign-on services[6]: they outsource authentication across multiple applications to a single, trusted, application usually operated by a large IT vendor, such as Facebook or Google. Again, critical privacy issues make this approach also unattractive, since users implicitly pay the service by letting the trusted party to have knowledge about every site they visit.[7]

---

[4] J. A. Halderman, B. Waters, and E. W. Felten. A convenient method for securely managing passwords. In Proceedings of the 14th international conference on World Wide Web, WWW '05, pages 471–479, New York, NY, USA, 2005. ACM.
[5] S. Chiasson, P. C. van Oorschot, and R. Biddle. A usability study and critique of two password managers. In 15th USENIX Security Symposium, pages 1–16, 2006.
[6] Google+ Sign-in. https://developers.google.com/+/web/signin/, Mozilla Persona. https://login.persona.org, Sign in with Twitter. https://dev.twitter.com/docs/auth/sign-twitter.
[7] M. Miculan and C. Urban. Formal analysis of facebook connect single sign-on authentication protocol. In Proceedings of the 37th International Conference on Current Trends in Theory and Practice of Computer Science. Springer, 2011.

Personalized authentication: many services trigger a second level of personalized authentication when an incoming authentication request has different properties compared to the most recent one (for example, the IP address belongs to a different country). Obviously, these techniques suffer from the inaccuracy of the heuristics used to trigger the secondary authentication level (i.e., mobile users change frequently IP addresses), and, sometimes, a determined attacker can render them completely ineffective. [8]

Two-factor authentication: it has probably been the most successful proposal to complement password-based systems by requiring that an additional password is provided, acquired through a second independent channel. Unfortunately the overhead both in cost and effort to deploy and maintain such system has led to adoption only by high-value services such as banking sites and e-mail providers. Moreover, it scales poorly when users are required to manage multiple secondary factors for distinct services. Finally, a study has shown that it can push users to weaker passwords.

User to Device Authentication is well researched in IT security. Passwords are among the most used techniques for their ease-of-use; current research is combining passwords with other factors, like tokens or behavioural detection. Biometrics seem still error prone, or if useably unobtrusive not secure enough.

Device to User Authentication is pervasive, e.g. when authenticating the web server of your bank before typing in the online banking credentials. This is again a long standing problem in IT security.

Device to Device Authentication is receiving much more attention in research these days to emerging areas like IoT or car-to-car communication. The main challenge here is to achieve authentication without, or at least with minimal need for, any human interaction.

Many applications require combined versions of the above scenarios, e.g. where human users use devices to authenticate against other devices with combinations of time and location characteristics, e.g. keyless entry to a car, where ownership, time, and location are relevant factors. Further, authentication entities might also be groups of entities (one-to-many or many-to-one authentication), e.g. a set of sensor devices deployed in a network.

2.3.1.3 Research Challenges

Each authentication system has to resolve crucial research challenges in order to be accepted in a realistic deployment. Generically, we evaluate each new authentication technique along the following axis:

Security: the authentication system should provide strong security guarantees. For example, a 4-digit PIN is a weak authentication solution. First, the attacker can guess the pin by performing multiple access trials. Second, the attacker can see, and therefore steal, the PIN while it is entered. Third, the user may lose the PIN and thus the assets that are protected by the particular PIN.

Privacy: the authentication system should not leak information associated with the user's activity to third-party services. For example, if a user utilizes a service for authenticating her to other services, then this service should be considered trusted enough for not taking advantage of the data collected associated with successful authentication to other services.

Usability: the authentication system should be usable enough. Strong authentication systems can be implemented, which are based on multiple factors, ideally spread out to all basic authentications techniques. For example, an authentication system may require something you have, something you know, and something you are (biometric) in order to authenticate successfully a user. However, the more authentication steps, the harder for users to comply with, and therefore to accept the system.

2.3.1.4 Existing Tools

Today, there are many tools for password cracking. These tools receive as an input a dictionary with known words and a password hash. Their goal is to find a word combination, which if hashed matches the given hash.

[8] I. Polakis, M. Lancini, G. Kontaxis, F. Maggi, S. Ioannidis, A. D. Keromytis, and S. Zanero. All your face are belong to us: breaking facebook's social authentication. In ACSAC, pages 399–408, 2012.

Many tools instead of blindly trying word combinations perform statistics over a leaked password set for generating targeted word combinations. A rich toolkit for password analysis and cracking is PACK.[9]

2.3.2 Access Control

2.3.2.1 Introduction

The widespread access to information supported by the Information and Communication Technologies (ICTs) brings significant benefits allowing users to access electronic services and resources everywhere anytime. These advantages come at a price of higher privacy risks, as a huge amount of (private) information is being circulated and stored, often without direct control of its owner. The definition of a proper *access control framework* regulating information exchange and access in the interactions among parties in the electronic world is therefore a challenging problem of today's systems. This problem has been under the attention of the research and development communities and several investigations have been carried out, proposing novel access control solutions for emerging scenarios. Although these solutions represent important advancements in the access control area, many issues still need to be considered.

2.3.2.2 Current Status

Several access control solutions have been proposed, including a few variations on the "classical" mandatory, discretionary, and role-based access control models. In the last ten years, particular attention has been given to solutions departing from user authentication and, in the name of privacy and convenience, supporting *credential-based* and *attribute-based* specifications. Credentials represent statements certified by given entities (e.g., certification authorities), which can be used to establish properties of their holder. Credential-based and attribute-based access control solutions make the access decision of whether or not a party may execute an access dependent on properties that the party may have and can prove by presenting one or more certificates, and/or on properties associated with the resources/services. The basic idea behind these solutions is that not all access control decisions are identity-based. For instance, information about a user's current role (e.g., doctor) or a user's date of birth may be more important than the user's identity for deciding whether an access request should be granted. Other efforts have been specifically devoted to the development of access control solutions that aim at providing expressiveness while maintaining simplicity of use, to ensure applicability (e.g., XACML).

2.3.2.3 Research Challenges

Anonymous credentials: Existing policy languages, supporting traditional credentials (e.g., X.509 certificates), are too rigid since the release of a credential implies the release of its complete representation. Recent works have focused on anonymous credentials (e.g., U-Prove and Idemix) that allow users to make statements about attribute values, without revealing any additional information. For instance, anonymous credentials permit to selectively release a subset of the properties in a credential or the proof that they satisfy some conditions without revealing any information about their values. New generation policy languages should support anonymous credentials by permitting the use of digital certificates and anonymous proofs in policy definition.

Semantics- and context-based policies: Two interesting research directions that can be pursued for enriching the expressive power of access control models, policies, and languages consist in: 1) leveraging Semantic Web solutions to fully integrate policies with *ontologies*, thus supporting generic assertions on users, resources, and credentials within access control policies; 2) using the *contextual information* related to the technological and cultural environment where an access request takes place.

Smooth integration with Web-based technologies: Existing solutions typically provide attribute-based access control policies based on logic. Such approaches, while appealing for their expressiveness, result difficult to apply in open scenarios, where simplicity, ease of use, and efficiency are crucial requirements. In this context, eXtensible Access Control Markup Language (XACML) represents a de-facto standard for policy specification in open systems. An interesting research direction and a practical pressing need is to extend XACML policies to integrate credential support, context representation, and exception management.

User privacy preferences: The release of private personal information by users is often regulated through

[9] http://thesprawl.org/projects/pack/

approaches symmetric to the ones used by servers for the disclosure of resources to unknown users. These solutions however do not completely fit the possible protection requirements of the users, since users may want to decide which information to disclose based on its sensitivity. An interesting research challenge is then the definition of an expressive and flexible approach for regulating the release of user personal data depending on, for example, the history of past interactions with the server, and the context and purpose of the interaction.

Storage at external servers and policy confidentiality: Huge amount of user-generated data are more and more often collected, processed, and shared by external servers that may not be authorized to know the data they managed and may not be simply delegated the enforcement of the access control policy (which also might itself be confidential or leak information on the underlying data). These scenarios require novel access control techniques allowing selective access to data while maintaining sensitive information not intelligible to the storing servers themselves (e.g., data can be encrypted). Attention must also be devoted to the development of techniques for the protection of the access control policies, which may potentially reveal sensitive information.

Multi-ownership management:. User-generated data may refer to more than one user and privacy policies may come from multiple parties (e.g., privacy regulations, users preferences). It is therefore important to develop flexible while expressive solutions for combining policies and resolving possible conflicting situations.

2.3.2.4 Existing tools

Access control solutions are implemented in different ways within different systems. There are solutions that work at the application level as well as at the system level. The *eXtensible Access Control Markup Language* (XACML) has been receiving considerable attention. Examples of credential-based solutions providing support for attribute based access control are: *Identity Mixer (Idemix)*, a cryptographic library offering the cryptographic algorithms to realize anonymous authentication; and *U-Prove*, a cryptographic solution that allows users to minimally disclose certified information about themselves when interacting with servers.

2.4 System integrity - Antivirus – AntiSpyware

2.4.1 Introduction

Antivirus and antimalware scanners aim to detect and remove malicious software that might already exist on a system, and to prevent future infections. The main methods which scanners employ to identify malware and viruses include:

- **Signature-based detection:** Vendors constantly analyze new malware samples and generate signatures which are then used by the scanner to identify the presence of malware. Scanners are kept up to date with the latest set of signatures on a daily or even hourly basis. The form of the signatures varies, from simple MD5 hashes of known malicious files, to more sophisticated fingerprints using a combination of features, such as byte sequences, regular expressions, code fragments, and file properties.
- **Heuristic-based detection:** To protect against future or unknown malware and variations of existing malware, for which signatures are not available yet, scanners typically use a variety of static and runtime heuristics based on well-known properties of malicious code, suspicious behaviors and actions, and reputation metrics.

Modern antivirus scanners have moved beyond simple scanning for the identification of malware, and offer more comprehensive protection against a variety of threats, including software vulnerability exploitation, malicious emails, and network attacks. Besides periodic file scanning, such “Endpoint Protection Software” typically comes with monitoring components that constantly inspect the runtime behavior of processes, network traffic, and other system activities, to detect and prevent exploitation attempts and other threats.

2.4.2 Current Status

Antivirus and antimalware scanners are among the most standard defenses that home users and enterprises employ to protect against a variety of threats. Their effectiveness, however, is challenged by several factors:

- **Previously unknown threats:** Although modern antiviruses use dynamic heuristic-based detection to protect against previously unknown threats, the effectiveness of these techniques is typically limited against unknown malware and exploits.
- **Malware evasion:** Targeted attacks and sophisticated malware use a variety of methods to evade detection and analysis, including code obfuscation, polymorphism, metamorphism, and packing; anti-debugging, anti-emulation, and anti-VM tricks; environment-aware code, logic bombs, and other triggers based on time or environment properties; and rootkit-like functionality, memory-only operation, and other stealthy execution techniques.
- **False positives:** Heuristic-based techniques that move beyond signature matching are usually prone to falsely identifying benign files or actions as malicious. Many systems, in case of uncertainty, prompt the user for the final decision. These issues severely impact the usability of antivirus protections.

2.4.3 Research Challenges

The above issues and limitations are directly translated to research challenges towards improving the effectiveness and usability of existing antivirus and endpoint protection software. Besides more accurate detection of previously unknown threats, robustness to evasion attempts, and false positives reduction, other challenges include reducing the footprint and performance impact of the monitoring components, providing effective protection for resource-constrained devices such as mobile phones and tablets, and providing better detection and prevention coverage by correlating and analyzing a broader set of features from the system and network level.

2.4.4 Existing Tools

ClamAV is a widely used free and open source antivirus. Numerous vendors provide commercial antivirus, antimalware, and endpoint security software, including Symantec, Kaspersky, Sophos, F-Secure, BitDefender, McFee, Eset, and many others. VirusTotal is an online service that provides free checking of user-submitted files using more than 40 commercial antivirus engines.

2.5 Cryptology

2.5.1 Cryptographic algorithms: design and evaluation

2.5.1.1 Introduction

Cryptographic algorithms are an essential tool to protect data at rest and data in transit. Traditionally one divides cryptographic algorithms into algorithms for data confidentiality and algorithms for data authentication; one can also make a distinction between symmetric algorithms, in which sender and receiver share the same secret key, and asymmetric or public key algorithms, where one key can be made public and the other one remains private. Symmetric algorithms shift the protection of information to the protection of a secret key; one distinguishes between stream ciphers and block ciphers (for confidentiality) and MAC algorithms (for data authentication). Most applications need both data confidentiality and data integrity; new modes have been developed to offer these features. Public key algorithms shift the protection of information to authenticity of a public key and the secrecy of the private key; public key encryption offers confidentiality protection and digital signature schemes offer data authentication. Cryptographic hash functions are keyless algorithms; they can be used to shift the authenticity of a large file to that of a short string – they are frequently combined with digital signature schemes. Cryptographic hash functions are also used for password protection and entropy extraction. In practice one often uses hybrid schemes that combine public key algorithms and symmetric algorithms.

2.5.1.2 Current status

A broad set of cryptographic algorithms is available that offers a high level of protection against mathematical attacks. Unfortunately many legacy systems have serious weaknesses (e.g. A5/1, A5/2, E0, RC4, Keeloq, Mifare,…). An overview of recommended algorithms can be found in the ENISA report on Algorithms, Key

Sizes and Parameters Report that is a continuation of a series of reports produced by the ECRYPT and ECRYPT II Networks of Excellence.

Substantial progress has been made in creating more complex cryptographic algorithms from simpler ones using formal security reductions; as an example, one can define an authenticated encryption scheme based on a block cipher. In public key cryptography, formal reductions can be made to mathematical problems that are believed to be hard. However, all efficient algorithms are based on unproven assumptions: there are no methods known to prove that a block cipher such as AES is indeed a pseudo-random permutation; or there are no lower bounds that show that factoring the product of two large primes or computing discrete logarithms in a given group is hard. However, there is a solid body of cryptanalytic techniques that combines discrete mathematics, statistics and number theory to identify weaknesses in existing algorithms. Moreover, a growing number of tools is developed for cryptanalysis, e.g. tools for ARX constructions or for lattices.

2.5.1.3 Research challenges

For application such as the Internet of Things, implantable medical devices and sensor nodes that harvest energy from the environment there is a need for **ultra-lightweight cryptology**. There has been quite some research in the past decade on algorithms with reduced gate count, but large improvements are needed; moreover, the attention is shifting towards low energy or low latency designs. The target is to improve existing designs with one order of magnitude. There is also a need to understand at a foundational level why solving the equations for symmetric cryptosystems is hard. Algorithms for symmetric encryption and data authentication have been mostly developed and deployed separately; one can expect substantial gains if both operations are combined. The expected improvements discussed in this paragraph will require that the algorithms are fine-tuned for a specific implementation environment and threat model.

Even if Moore's law will hold for the next 10-15 years, the progress in bandwidth and storage capacity grows faster than the computing power; this means that there is a need for **ultra-high-speed cryptographic algorithms** that are fully parallelizable and that are energy efficient. This challenge is related to the challenge in the previous paragraph, but the optimization target is very different and hence completely different designs will emerge.

All widely used public key algorithms are based on problems from algebraic number theory (factoring and discrete logarithm). Some researchers claim that by 2025 a large quantum computer can be built; this would mean that all the deployed public key algorithms would be insecure; moreover, increasing the key length does not help. There is a need for public key algorithms based on other mathematical problems, that could not be solved efficiently on a quantum computer. There have been some promising results in the area of lattices, code-based crypto and digital signatures based on hash functions, but none of the existing proposals has been fully validated; in particular the performance and/or key lengths are not yet competitive with existing algorithms. Finding such systems is essential in order to ensure that we have usable public key algorithms in the next decade and to ensure **long term security**.

Security reductions in cryptology get ever more complex; moreover, these reductions can be very intricate and subtle. There is a need for tool development to verify and create such security reductions.

2.6 Audit and monitoring

2.6.1 Intrusion Detection and Intrusion Prevention

2.6.1.1 Introduction

Network Intrusion Detection Systems (IDS) are devices that monitor network activity in order to detect intrusion attempts to a computer system. There are two major kinds of IDSses:

- **Misuse-based** IDSes. These systems are equipped with a set of rules (signatures) that describe malicious behaviour. Such a rule might be: *if an outside IP address tries to log in as "root" to a computer inside the organization, then raise an alert*.

- **Anomaly-based** IDSes. These systems first try to define a model of "normal" (or "usual") behavior and then try to detect patterns that deviate from this normal behavior. Such deviations are considered anomalies and they usually raise an alert.

In some cases IDSes are placed "in-line", and if they detect an intrusion they drop the offending IP packets and reset the connection. When they operate "in-line" IDSes are called Intrusion *Prevention* Systems, because they not only detect the intrusion attempt but, by dropping the packets, they *prevent* the Intrusion from reaching the victim computer altogether.

2.6.1.2 Current Status

IDSes and IPSes are a very good line of defense. However, they still have limitations including:

- **False Positives**: not all anomalous behaviors are Intrusion attempts. They may just be legitimate behaviors that are just different. When legitimate users change their behavior, say after the introduction of new software/hardware, this change will usually be registered as anomalous behavior and may trigger several alerts that are false positives.
- **Algorithmic attacks**: Similar, in spirit, to Denial of Service attacks, *algorithmic* attacks try to overload the IDS by sending carefully crafted packets whose processing by the Intrusion Detection System requires the maximum computing capacity. Filling the network with such packets forces the IDS to quickly reach up to 100% of its capacity, at which point it will not have the computing resources to examine any more incoming packets. At that point the attacker sends the real attack hoping that the IDS, saturated at 100% of its computing capabilities, will not have the capacity to detect it.
- **Limited view – undetected attacks**: Intrusion Detection Systems usually need to process both the headers and the payload of incoming packets. If the payload is not available, maybe due to encryption, or if some of the packets are not available, possibly due to load balancing, attacks may easily go undetected.

Intrusion Detection Systems are based on the "perimeter security" paradigm. Unfortunately, this security paradigm is rapidly changing. IDSes need to adapt in order to be able to work in an environment where there is no perimeter or where the perimeter is assumed to have already been breached.

2.6.1.3 Research Challenges

- **The Changing Face of the Security Paradigm**: Intrusion Detection Systems are based on the "perimeter security" paradigm. That is, each organization has a clearly defined perimeter: everything outside it is not trusted and everything inside it is trusted. The IDS monitors this perimeter to make sure that it detects any breaches. Unfortunately, this security model is rapidly changing. The externalization of IT resources to outside providers and new approaches to hardware, such as BYOD (bring your own device), make the notion of the perimeter obsolete. IDSes need to adapt in order to be able to work in an environment where there is no perimeter or where the perimeter is assumed to have already been breached.
- **Complexity in modelling attack patterns**: rules have evolved from memoryless simple string matching to stateful automata (such as regular expressions). Yet, this is sometimes insufficient to capture the attack mechanism and describe it in a generic manner that will detect all the possible ways of carrying out the attack exploiting a specific vulnerability. Also, the increase in the complexity of protocols makes modelling their normal behaviour increasingly difficult.
- **Speed**: over the past few years network speeds have been rapidly increasing. At the same time, IDSes need to invest more computing cycles per packet either checking against more elaborate rules, or trying to detect sophisticated anomalous behaviours. These effects combined put significant stress to the computing resources needed.
- **Whole System Image**: Although traditional IDSes monitor only network events (such as incoming network packets), their efficiency and accuracy can be significantly increased when they monitor the

whole system image and correlate events happening at several different points, such as correlating network packets with system calls and buffer overfows. Collecting and correlating such data can be challenging, but it may be the only way forward.

2.6.1.4 Existing Tools

There exist several commercial IDSes. Among the freely available ones, the Snort[10] and Suricata[11] rule-based IDS seems to be very popular with end users, while the Bro[12] Intrusion Detection Systems seems to be very popular with the research community.

2.6.2 Intrusion Tolerant and Resilient Critical Information Infrastructures

2.6.2.1 Introduction

The pillars of modern, ICT-dependent societies, are *critical information infrastructures (CII)*, increasingly considered a key factor of competitiveness. This scenario may create enormous opportunities, but also bring about important security and dependability risks. It is recognised in the cybersecurity strategies of several countries that threats to critical information infrastructures are to be feared. In other words, traditional security techniques, based on intrusion prevention and detection, may not be enough to sustain and counter *advanced persistent threats* against valuable targets, calling to be reinforced by powerful techniques like *intrusion tolerance and resilience.*

2.6.2.2 Current Status

Critical information infrastructures (CII), generally designating the computerized and networked part of physical infrastructures --- such as energy, telecom, or transportation --- and a relevant example of cyber-physical systems (CPS), have been complemented over the past few years with a set of emerging computer-based CII. Increasingly relying on the Internet-Cloud complex, these infrastructures support critical assets like the finance or public administration systems, but also social networks, or health and biomedical systems like e-biobanks, whose privacy sensitiveness became an issue, with the emerging trend of massive DNA sequencing. This converging scenario points to extremely large-scale and extremely complex computer and network systems, where classical computing devices coexist with embedded devices (many of them mobile), in a practically seamless manner; these devices will be highly programmable and dynamic; information processing will coexist with real-time control; computer-caused failures may be physical as well as virtual.

The value of the assets at stake in this hugely interconnected and virtualised world is formidable and, in consequence, is attracting the attention of the organised crime and cyber-terrorism (e.g., Russian Business Network), cyber-hacktivism organisations or militias (e.g., Anonymous, LulzSec), and nation-state armies or agencies (e.g., Stuxnet, DuQu, Flame, Conficker, APT1), including the intentional weakening of security by major society actors (e.g., the NSA-PRISM-TAO affair). In other words, we need to expect and be able to counter very sophisticated *targeted attacks*, or *advanced persistent threats (APT)* against valuable targets: stealing information for commercial, industrial or political espionage; violating the privacy of individuals; disrupting the operation of critical resources (denial or service), or even their integrity (sabotage).

2.6.2.3 Research Challenges

In order to address the above-mentioned challenges, we need to investigate and develop paradigms and techniques that complement (and not replace) classical techniques based on intrusion prevention and detection, in order to endow systems with the capacity of *defeating extreme adversary power* (severe and continued threats) and *sustaining perpetual and unattended operation* (in a systematic and automatic way). Recent research on powerful and innovative automatic security and dependability techniques can be inspiring about the

[10] http://en.wikipedia.org/wiki/Snort_(software)
[11] http://en.wikipedia.org/wiki/Suricata_(software)
[12] http://en.wikipedia.org/wiki/Bro_(software)

avenues to pursue, like intrusion tolerance or Byzantine fault tolerance, resilience, secret sharing and secure multi-party computation, homomorphic encryption, erasure coding and dispersal, self-healing and diversity mechanisms.

Research themes that fall into these challenges and have a virtuous alignment with core application fields of H2020, are for example: Resilience of Cyber-Physical System infrastructures and control; Internet and Cloud infrastructures resilience; Security and dependability of embedded components; Data privacy and integrity in highly sensitive sectors.

2.6.3 Information and Event Management Tools

2.6.3.1 Introduction

Security Information and Event Management (SIEM) is considered an IT best practice for security monitoring and, for regulated industries, an audit compliance requirement. The goal is to consistently aggregate, decipher and normalize non-standard input log formats; manage massive volumes of event log data for real-time and historic analysis; correlate and consolidate complex event log data by leveraging Complex Event Processing (CEP) technologies to yield actionable intelligence; and overall maximize event log value to support the reliability of IT services and decision-making of IT security professionals.

2.6.3.2 Current Status

SIEM and CEP are not new IT technologies, but they have been significantly impacted by emerging technologies in the advent of the Future Internet, such as Big Data, Cloud Computing and the Internet of Things, to the point that further research and changes in SIEM technology are necessary in order to cope with the new challenges. Until recently, SIEM systems were deployed in closed corporate infrastructures or provided by an external service provider. As such, in this Managed Enterprise Service Infrastructure, events were collected centrally and passed only through internal customer or service provider links. The recent Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) paradigms will require new models that take into account the implications for deployment of SIEM in the cloud. Distributed networks and services are the reality these days, and SIEMs are faced with challenges and needs of various natures. They need to seamlessly integrate new event sources and types, increase scalability by orders of magnitude while maintaining near real-time processing, and provide new advanced security modelling and visualization techniques for increasingly complex attacks, processes and infrastructures, among others, in order to provide a clear overview of the security status of the system.

Furthermore, SIEM users are calling for earlier detection and mitigation of attacks, for which predictive security monitoring capabilities need to be realized in order to proactively stop attacks in their tracks before malicious users get access to critical servers, services, or data. Triggering alarms is not enough: they must be quality alerts that refer to actual high level threats, and thus need to be filtered and aggregated to be of any value to the SIEM operators. And threats are linked to sensitive business processes and information, as well as software and hardware vulnerabilities. A vulnerability in one server or service can compromise the rest of the network, which might not be readily apparent by looking at the isolated pieces of information. These need to be linked, modelled, and presented to the user in a way that empowers his security awareness of the target system and thus his decision-making. Having more fine-grained views and advanced methods for semantic storage of the different security aspects affecting the monitored system is hence essential to properly analyse and identify weaknesses and likely attack paths.

2.6.3.3 Research challenges

General challenges and opportunities in this area include:

- **Applicability to multiple domains and layers**: The main challenge faced by SIEM systems is to extend to multiple layers (physical, business, application, and service-level), domains, and contextual information that impact the security risks affecting the monitored system.
- **Privacy**: The challenge is in establishing the steps to sufficiently anonymize different data formats (sensitive data from other data), and when to apply these steps if the different phases of processing –

from pre-correlation at the sensors, to the collection and parsing and to the generation of alarms- are carried out in different logical domains (accountability issues).

- **Selection and enforcement of countermeasures**: developing advanced decision-support services and simulation tools (such as attack graphs) that provide feedback to operators with respect to the feasibility and impact of suggested countermeasures in changing conditions, as well as enforcement infrastructures that link security policies to business processes and implemented controls.
- **Security visualization and reporting**: techniques and tools are needed for the abstraction, modelling and visualization of attacks, malefactors, and of the security of events, processes, infrastructures and networks of the monitored system, which update their status based on alarms generated by the Complex Event Processing engine and can also trigger their own alarms.
- **Predictive security monitoring**: utilize a proactive approach to security to enable early detection of modern, complex multi-layer attacks that can predict them before they materialize
- **Protection and trustworthiness**: needs for guarantees with respect to security assurance, availability, resilience and trustworthiness of the core SIEM server and event processing nodes.
- **Alert quality**: The challenge is in how to recognize real threats while minimizing false positives/negatives by use of advanced correlation techniques that leverage increased expressiveness of the correlation rules.
- **Timeliness, elasticity, and scalability** of the processing: Parallelization of the processing load into multiple distributed nodes that adapt their configurations to crashes and failures in a non-disruptive fashion (automatic provisioning and decommissioning of nodes) is needed to account for the ever increasing need for scalability in the number of events that can be processed per time unit, as well as for the storage and capacity of past events and increased memory leading to an extension of the time window within which distant events can be correlated.
- **Usability**: SIEM systems are expensive to deploy and complex to operate and manage. There is the risk that new SIEMs may become excessively complex and costly as they introduce new innovations to cope with the above challenges. This indicates that usability should be a high priority in the development of new SIEMs.

Recognize real threats while minimizing false positives/negatives by use of advanced correlation techniques that leverage increased expressiveness of the correlation rules.

2.6.3.4 Existing Tools

Some notable solutions in the market implementing the above functionalities are: QRadar, ArcSight , Symantec, and Novell Sentinel, as commercial solutions, and OSSIM as open source one.

2.6.4 Computer Forensic tools

2.6.4.1 Introduction

Broadly speaking, computer forensic tools could be classified either as *proactive* or as *post incident*. The former have significant overlap with Intrusion Detection Tools and Techniques (see section 2.6.1 in page 14) and may only add features with respect to evidential integrity, i.e. the ability to claim that a set of data retained as evidence has been maintained in a way that guarantees that it is a true copy of the original evidence in a potential scene of cybercrime. As such, proactive forensic tools will be omitted from the discussion below. Post incident examination tools implement techniques that enable an investigator to develop an insight of past events and prove or disprove allegations relating to the use of computers to perform criminal acts. In the following section we discuss the nature and challenges that the development and use of such tools bring to the relevant community and broadly to society.

2.6.4.2 State of the art for post-incident examination tools

Although different texts may adopt proprietary classifications of tools and techniques for computer forensics, a review of state of art sources shows that they can be usually grouped by scope of applicability, i.e.

- **Computer (system) forensics tools,** including applications for evidence acquisition, analysis of filesystems, event logs, retrieval of contents of interest (e.g. multimedia files), retrieval of deleted items, application activity (e.g. browsing history) etc.
- **Network forensics tools,** including applications for data packet capturing, network server log analysis (e.g. time of connection, originator's address etc.), deep packet inspection where feasible, and similar functionality.

Another distinction between tools can be made on the basis of whether they are applied to "live" evidence or not (i.e. from a working computer/network that has not been subject to a traditional "pull the plug" data acquisition), in which case we talk about live forensics tools, usually dealing with main memory contents acquisition and analysis. Such tools are very useful e.g. for the analysis of non-persistent malware, i.e. software that only lives in memory.

Forensic tools may come packaged in integrated platforms offering capability of analysis of both system and network related evidence, as well as case management and secure evidence retention capability, or as specialised applications for the examination of a single, or limited types of evidence only (e.g. Internet browsing, email analysis, image retrieval etc.). Both types may be using simple, record based interfaces for the representation of evidence such as logs and filesystem metadata. Most would offer the ability to construct a meaningful timeline of events so that incidents can be investigated in chronological order and potential causal relationships to the explored through the concept of advancing time. More advanced visualisation techniques could be based on graphs and social networks (e.g. representing network configurations or communicating users), animations and 3D plots of events and other graphical means that may enhance an investigator's understanding of digital evidence.

2.6.4.3 Research challenges

Based on the nature of cybercrime, a number of challenges exist or emerge with respect to the use of forensic tools and include in particular:

- The debate about investigation practices versus **privacy**; particularly the development of tools that can support investigations in a privacy-legislation-compliant manner.
- The mere **volume of the evidence** that could potentially be examined; contemporary cybercrime scenes may involve multiple computers, mobile devices, large network traffic records etc. and so the growth of relevant evidence, and thus the time to process (and space to store), could be exponential.
- **International co-operation and co-ordination** of investigations of crimes affecting multiple jurisdictions; due to the nature of the Internet, cases may include illicit activities committed to more than one jurisdiction and so investigators may need to combine evidence for which different authorities in different nations may have the responsibility to acquire and handle. Co-ordinating such task is by no means a trivial task.

2.7 Configuration Management and Assurance

2.7.1 Policy Enforcement Applications

2.7.1.1 Introduction

Policy enforcement applications are useful for system administrations in order to perform centralized management according to an organization's security policies. These tools are capable of identifying authorization-related problems on desktops and servers that are results of misconfiguration. Moreover, they provide valuable feedback that can help administrators to solve these issues.

2.7.1.2 Main Functions

Policy enforcement applications are based on four basic functions:

- **Policy Definition:** Policy enforcement applications can be used to construct policy rules. Such rules can be password requirements and user right access to specific applications.

- **Compliance Checking:** The next step, after the creation of the policies, is to compare the current status of the system in terms of configuration when compared to the defined policies. Compliance checking can be applied to many different administrative domains and operating systems though a central console. An example of compliance checking is the checking the password requirements as drawn from the defined policies (e.g., checking if the passwords are strong in terms of number of characters and symbols, or checking whether the passwords are periodically changed).

- **Reporting:** Policy enforcement systems have to produce reports with appropriate information to the system administrations. Such reports may inform administrators for example of hosts that run unpatched versions of specific software and may be at risk.

- **Remediation:** Many policy enforcement applications can proactively discover and fix various issues. For example, they can monitor and keep the monitored software updated by automatically downloading and installing any security related updated that are available.

2.7.1.3 Research Challenges

- **Self-Adaptability:** Current policy enforcement solutions can provide centralized monitoring control based on a set of predefined policies of an organization. The need of defining the policies for such applications is vital for their effectiveness. Any changes on the monitored environments imply changes in the predefined policies in order the applications to work properly. An open issue is how we can design policy enforcement applications that can adapt to changes introduced by the monitored environment.

- **Universality:** Another challenge of policy enforcement applications is the universality they offer in terms of platforms they support. Most of the tools do not work on all operating systems, and most of the time, the installation and configuration across different platforms can be a tedious and painful process.

2.7.1.4 Existing Tools

There exist a great variety of available policy enforcement solutions with different applications such as: antivirus solutions, host-based application firewalls, disk encryption and file system-level encryption, network access control, and others.

2.7.2 Network Management

2.7.2.1 Introduction

The scale and complexity of both networks and corresponding network management continues to grow. The factors that contribute to this growth are manyfold, e.g. embedded devices that start to compose the Internet of Things (IoT), new constitutions of administrative domains in BYOD or CYOD scenarios, or virtualization techniques that can either increase or decrease the number of manageable or observable endpoints. In addition, the fluctuation of the effective topological layout the network endpoints compose also increases. Mobile devices, mesh networks, load balancers or multiple redundancy measures on various layers are examples of factors that have a significant impact on how network management methods will have to adapt. An overarching target in the development of network management is automation. In order to support automation an

improvement of interoperability and new measures that unify the foundation (and primary processes) of network management are required.

2.7.2.2 Current Status

Most of the time, network endpoints do not facilitate management and monitoring processes directly, but offer interfaces to provide and modify endpoint attributes that can be used by management tools. This results in external tools and databases (such as CMDBs) that have to be updated and aligned with the current configuration and state of network endpoints, the use of pull mechanisms, various transports and heterogeneous data models. Devices under external authority are difficult to assess (and manage) without corresponding context knowledge. Additionally, the assessment and management of observable network traffic (especially regarding external devices that are not part of a local administrative domain) becomes increasingly difficult due to end-to-end encryption between discernible, unique endpoints. Endpoint identification is often based on endpoint attributes that are not very reliable, such as addresses, or via a set of identifiers with a low level of assurance. Management databases make use of multiple sources of information to compensate this, which increases the chances to create a more complete representation of the current network but also introduces the need for context information about provenance of acquired endpoint attribute values.

2.7.2.3 Research Challenges

The design of future management tools, protocols and techniques must not only facilitate interoperable network management automation but also provide incentives for vendors and consumers to adopt and deploy them. Unification and homogenization of transports and corresponding data models must not interfere with flexibility and vendor-specific extendibility. Unique identification of endpoints is a mandatory prerequisite for effective network management. Technologies and processes that can provide unique, reliable and trustworthy endpoint identification in every scenario require further development, especially regarding interoperability. Legacy technologies or endpoints with an unusual long life-cycle that can be found, for example, in industrial control systems (ICS), must be taken into account by the design of next generation network management processes and tools. Availability of services provided by endpoints that effectively support and maintain businesses processes is essential. Unfortunately, formal availability or network reachability analysis in large networks is increasingly difficult. Simulation of subsets of a network and its endpoints to automate tests and evaluation procedures can offer a promising alternative. Typically, the categorization and assessment of unknown endpoints in an administrative domain remains a challenge. Dedicated tools that are able to support the profiling of endpoints via their observable traffic in automated network management processes can benefit from domains such as machine learning or anomaly detection.

2.7.2.4 Existing Tools

Vendor-specific network management tools, such as Cisco NMS, IBM Tivoli or HP Service Activator already combine the functionalities of CMDBs, network management suites, and in some cases even semantic asset representation. Cryptographically strong technologies, such as the hardware-rooted Trusted Platform Module, provide a basis for reliable endpoint identification, but are not always available. Cloud management frameworks try to automate network management in a specific domain of service models, but are not flexible enough to satisfy the requirements of heterogeneous enterprises. There is preliminary research to support network management with appropriate traffic analysis methods, unifying representations or process architectures that focus on automation, but further research regarding the combination and interoperability of these domains is required.

2.10 Software security and secure software development

2.10.1 Software Design for the Future Internet

2.10.1.1 Introduction

The Future Internet (FI) will not only force society and software developers to reconsider how services are exposed and delivered, but also how to enable continuous improvement and adaptation of services on the fly while maintaining end-to-end security and privacy. The rapidly evolving nature of FI applications will change

the way software engineering is carried out. Boundaries between design and runtime will shrink, and there will be an increased need for real-time verification, monitoring and assurance to facilitate and ensure security properties such as confidentiality, integrity, and availability. The very traditional model for software development lifecycle will need to be revamped, as all stages of development will be impacted. Indeed, the complexity of FI services requires that security and dependability, up to now considered secondary aspects of system development, will need to be considered in the early stages of the system development life cycle SDLC, just as other functional and non-functional requirements.

2.10.1.2 Current status

Today´s ICS systems are typically not designed and built with security and privacy in mind. Consequently, security and privacy is often dealt with retrospectively, when security or privacy problems arise. In fact, incidents that involve personal data can often be traced back to software failures, which can be prevented through enhanced engineering practices, and new methods and tools for software requirements elicitation, design, and testing. This integration includes the collection and analysis of security and privacy requirements, reconciling often ambiguous, inconsistent and conflicting requirements, as well as the development and evaluation of software designs based on established privacy principles such as those suggested by Privacy-by-Design, including how to analyse design alternatives to reduce threats to personal privacy.

Furthermore, FI services will be composed of other services through flexible and modular architectures, and involve a high number of heterogeneous and distributed artefacts, sensors, and stakeholders. Pre-defined trust relationships between components, applications, and environments may no longer be taken for granted. Making sense of security aspects amid this new reality for services requires new models that link security to business goals and organizational needs, especially as different stakeholders need to assure compliance for specific parts of a given FI service. Context also needs to be taken into account to enable dynamic configuration of security that adapts to changing conditions and incomplete information. Trust in these new services thus requires a systematic assessment of security properties and enforcement of security policies, which must be supported by all stages of SDLC: monitoring the execution of new services to measure how well they conform to a set of criteria and metrics established at design time, and deployment of new policies and reconfiguration of system properties as required.

2.10.1.3 Research Challenges

There are two overarching challenges that need to be addressed. First, *security and privacy risk and cost assessment* need to be embedded as a separate activity of the overall SDLC process, closely interacting with the service engineering activities during each iteration of the SDLC. The second challenge is *to provide security and privacy assurance* during the different stages of SDLC. More fine grained challenges include:

- Automatization of secure and privacy-aware service engineering
- Increased security for services and service composition
- Compliance with regulations and standards
- Increased interoperability
- Enhancement of users' experiences and awareness
- Implementation of privacy and Privacy-by-Design
- Context-awareness and self-reconfiguration

2.10.1.4 Existing Tools

Different technologies are used depending on the functionalities provided during SDLC stages. Different categories for which specific solutions are developed to support and incorporate security into the SDLC include: 1) application risk analysis; 2) Requirements specification and formalization, including the definition of privacy requirements; 3) attack models; 4) code review; 5) static application security testing; 6) dynamic application security testing; 7) vulnerability analysis; 8) vendor (third-party) application security testing, and; 9) penetration testing. There exists also a number of hot topics which encompass the whole SDLC and which are the focus of new solutions. These technologies are at a less mature state and include mobile application security, secure service composition, privacy-enhancing technologies and embedding privacy into the SDLC, application

perimeter monitoring, web application discovery and monitoring, and trusted execution environments. Horizontal to the above, new methodologies and models for i) ***secure testing***, including static binary, dynamic and manual analysis, ii) ***software assurance***, such as the Software Assurance Maturity Model (SAMM), iii) ***assessing cost-benefit ratio*** of secure software development, and iv) ***security and privacy requirement analysis***, are essential but underdeveloped and need to be incorporated in future research in security and privacy engineering.

2.10.2 Risk Introduction

Understanding and managing risk is a key factor of the overall management of ICT systems, and risk should serve as a driver for decision makers and other stakeholders. Information security risk management is a particular concern with respect to ICT system security, software security and secure software development. Methods, techniques and tools for security risk assessment aid developers and stakeholders to identify the most critical threats and vulnerabilities, and to identify adequate means and options for mitigating security risks so as to maintain risks at an acceptable level for all stakeholders.

2.10.2.2 Current Status

There exist several standards, guidelines and industrial best practices for risk management, including ISO 31000 on risk management and ISO/IEC 27005 on information security risk management, that aid stakeholders in identifying, assessing and identifying security risks. However, such guidelines and practices are most commonly applied for existing ICT and software systems, and less throughout software development. During the recent years there has been an increased focus on secure software development, the objective of which is to build security into systems already from the requirements and design phases. The Microsoft Security Development Lifecycle (SDL) is such a process, where threat modelling and risk identification is conducted during the software design phase.

Software and service systems of today are ever more dynamic, heterogeneous, compositional and evolving, where Future Internet systems like cloud services are a predominant example. Such characteristics, as well as the fact that stakeholders are multiple with sometimes conflicting interests, make many of the established methods and techniques for risk management and assessment inadequate and less fit for purpose. In the following we highlight some of the pressing and timely research challenges.

2.10.2.3 Research Challenges

Traditional methods for risk assessment are monolithic in the sense that systems are understood and analysed as a whole. For large, compositional and dynamic service systems, such methods easily become too heavy and costly to apply, and existing analysis results rapidly become outdated. Understanding how to cope with this requires research in several directions.

- **Risk aggregation.** In order to accommodate to a modular software development process, as well as effectively handling the heterogeneous and compositional nature of service systems of today, there is a need to focus on a modular approach to the analysis of security risk and cost. Such an approach should also have the capacity to involve the perspective and requirements of several competing stakeholders such as service vendors, service providers and service consumers. When services are compositional, so are risks, and should therefore be understood, modelled, and analysed as such. This requires methods for aggregating the global risk level through risk composition.
- **Evolution.** The setting of dynamic and evolving services and software systems implies that also the security risks and the set of adequate mitigations and security mechanisms are dynamic and evolving. Thus, in order to maintain a valid and up to date risk picture, there is a need to continuously reassess security risks and identify cost-efficient means for risk mitigation. Such reassessment should not imply that systems need to be analysed from scratch every time a change, such as a service substitution, occurs. Novel methods and techniques are needed to systematically handle change, which could include techniques for modular risk assessment and run-time risk assessment.

- **Legal aspects.** Many legal aspects are strongly related to information security, including privacy, data protection and contracts on service level agreements. While systems become increasingly cross-organisational and cross-national, the legal requirements become more complex to understand, including which jurisdictions that may be relevant. Hence, legal risk assessment should be an integrated part of security risk assessment, so as to systematically assess the potential legal implications of security breaches.
- **Cost.** Industry and service providers need to ensure properties such as security, compliance, privacy, trust and identity protection while making business. Without techniques to assess security cost and to ensure return on investment (RoI) in security, such properties may fail the competition with other business priorities. Novel techniques are needed that not only ensure RoI in security, but also clearly demonstrate it at a business level.

2.10.2.4 Existing Methods

Existing industry best practices, as well as standards such as the aforementioned ISO/IEC 27005, are always relevant, and existing methods, techniques and tools for security risk management should comply with such established guidelines. Considering the identified research challenges, there are various recent works that make some substantial progress on risk aggregation[13,14], risk evolution[15], legal risk assessment[16] and security cost assessment[17]. Considering the research challenges and the current research landscape, there is still a gap to close, and also a need for substantial industry liaison.

2.10.3 Assurance

2.10.3.1 Introduction

Assurance plays a central role in the development of software-based services to provide confidence about the desired security level. We distinguish different activities according to the SDLC phases:

- **Early Assurance.** Early detection of security failures reduces development costs and improves assurance in the final system. The techniques here include algorithmic verification of services and extraction of models for verification from common design languages (e.g., UML).
- **Assurance for implementation.** Several complementary assurance techniques are available to ensure the security at the level of an implementation. This includes different forms of testing (such as penetration testing and model-based testing) and debugging as well as runtime monitoring and enforcement.

2.10.3.2 Current Status

We discuss the current status and the main limitations according to the categories above.

- **Early Assurance.** There are efficient techniques and tools for the verification of services. Most of these works with a symbolic model, assumes perfect cryptography (Dolev-Yao intruder) and focuses on standard trace-based security properties such as secrecy and authentication. Such verifiers can also be adapted to enable secure service composition. These tools and techniques need to be extended or

[13] A. Refsdal, Ø. Rideng, B. Solhaug and K. Stølen: Divide and conquer - Towards a notion of risk encapsulation. In Advances in Engineering Secure Future Internet Services and Systems. LNCS 8431, Springer, 2014
[14] J. Viehmann: Reusing risk analysis results – An extension for the CORAS risk analysis method. In: Proc. 4th International Conference on Information Privacy, Security, Risk and Trust (PASSAT). pp. 742–751. IEEE, 2012
[15] B. Solhaug and F. Seehusen. Model-driven risk analysis of evolving critical infrastructures. Journal of Ambient Intelligence and Humanized Computing, 5(2):187-204, 2014
[16] K. Beckers, S. Faßbender, J.-C. Küster, and H. Schmidt. A pattern-based method for identifying and analyzing laws. In Requirements Engineering: Foundation for Software Quality (REFSQ'12), LNCS 7195, pp. 256–262. Springer, 2012
[17] L. M. S. Tran, B. Solhaug and K. Stølen. An approach to select cost-effective risk countermeasures. In Proc. 27th Annual IFIP WG 11.3 Working Conference on Data and Applications Security and Privacy (DBSec'13). LNCS 7964, pp. 266-273, Springer, 2013

complemented to cover strong secrecy and privacy properties as well, which can be formulated as equivalences between systems. Alternatively, formal models can be extracted from commonly used design models (e.g., SecureUML) by translating their constraint languages into the language of an SMT solver or other automated reasoning tools.

- **Assurance for implementation.** Functional testing and security testing are closely related and certain algorithms for test generation can be reused in both cases, while oracles have to be specifically defined for security testing. Current research in debugging focuses on two different areas. Differential slicing is an efficient technique for debugging security vulnerabilities based on binaries (as source code is often unavailable). Early detection is a runtime approach for finding and diagnosing use-after-free and double-free vulnerabilities (still frequent due to use of legacy languages). Runtime monitoring is a complementary assurance technique used at the implementation and deployment level. Recent work has significantly extended the expressiveness of the logical property specification languages that can be used in runtime monitoring. This is needed, for instance, to state complex usage control properties.

2.10.3.3 Research Challenges

The following four research challenges are relevant for the assurance topics listed above.

- **Expressiveness** We need more expressive modeling languages and attacker models in order to represent faithfully the manifold aspects of future internet services (e.g., for modeling authorization and usage control policies, privacy properties, compromising intruders, and trust models).
- **Distribution** In order to obtain a better coverage and stronger guarantees, testing and runtime verification techniques have to consider the entire distributed system instead of the prevalent approach of separately testing and monitoring individual components or services of distributed applications (e.g., client side/server side).
- **Linking abstraction levels / SDLC phases** The integration between different phases of the SDLC needs to be improved. In particular, the different abstraction levels need to be related in a semantically sound and practically useful way.
- **Modularization** is a natural way to decompose complex systems into simpler parts. Unfortunately, security is not compositional, that is, new vulnerabilities may arise from the composition of modules or services, even if each of these is secure individually. Further study is needed to identify sufficient conditions for secure module and service composition.

Basic techniques do exist in many cases, but they require substantial extensions to tackle today's distributed and highly dynamic services and their demanding security requirements.

2.10.3.4 Existing Tools

There are a number of tools for security protocol verification, most notably AVANTSSAR (including CL-ATse, OFMC, and SATMC), Maude-NPA, ProVerif, Scyther, and Tamarin. Regarding testing, Smartesting CertifyIt is an automated test generator based on UML models, which has recently been integrated with security protocol testing to generate test cases for security protocols. X-CREATE (XaCml REquests derivAtion for TEsting) is a tool for the automated derivation of a test suite starting from an XACML policy. Several tools exist that support advanced debugging techniques: differential slicing is supported by a tool implementation. Undangle is a tool for finding and diagnosing use-after-free and double-free vulnerabilities. For runtime monitoring, the MONPOLY tool covers policies formulated in an expressive specification language based on first-order temporal logic.

2.10.4 Secure Coding & Secure Programming Languages

2.10.4.1 Introduction

The technical and scientific communities offer several promising approaches to language-based security. Some of them require rebuilding parts or all of the software that needs to be secured: for instance when designing innovative programming languages with built-in security features, elaborating new software building tools and environments, advocating alternative coding practices, or mandating the use of dedicated software libraries.

On the contrary, source code analysis techniques leverage tools and methods to provide software developers with strong and demonstrable confidence in existing artefacts. Overall, these techniques allow the developers to

verify that programs and their functionalities behave according to their specified behavior. These techniques can be further divided into two classes:

(a) The analysis of programs in a non-runtime state, called **static analysis**, proceeds across the source code just like a compiler would, looking for patterns indicative of unexpected behaviours.
(b) The analysis of programs in a runtime state, called **dynamic analysis**, runs the compiled source code on sets of predefined input values to detect unexpected behaviours.

The fact that source code analysis techniques do not require software redesigns lowers their costs, allowing the analysis of legacy systems, and enabling the use of commercial off-the-shelf libraries.

2.10.4.2 Current status

Over the past decade program analyzers have been tackling a neighboring problem, i.e. the safety of critical systems. These are often embedded systems, written in limited subsets of low-level languages such as C and assembler, and using constructions of modestly complex behaviour. Program verification is used in this field to achieve demonstrably equivalent levels of safety than with traditional methods for critical systems, but at a lower cost. These practices have made it into various domain-specific certification standards (DO-178B/C, CENELEC EN 50128, IEC 60880, IEC 61508, ISO 26262, etc.).

Transferring this existing expertise into tools that validate secure coding and code properties is the subject of burgeoning efforts in the international community.

Here you could mention some current strategies and technologies that are used today, such as:

- Secure Coding Guidelines for the Java Programming Language (http://www.oracle.com/technetwork/java/seccodeguide-139067.html)

- Some dialects that aim to thwart common languages vulnerabilities (e.g. http://cyclone.thelanguage.org)

- Open-Source and commercial tools for static security analysis. You can check a list here: https://www.owasp.org/index.php/Source_Code_Analysis_Tools

2.10.4.3 Research challenges

While source code analysis techniques hold some promise, they do not yet meet the needs of security-critical software verification. Several important technological and scientific roadblocks need to be lifted before they can be industrialized:

- The first roadblock is the definition of **formal classes of security failures**, and their characterization in terms of statically or dynamically detectable behaviours.
- The second roadblock is the matter of **programming language coverage**: as of March 2014, the five most popular programming languages are Java, C, C#, C++, and Objective-C. Web-based languages such as PHP and Javascript are also part of the top 10[18].

Tackling these first two items require extensive knowledge of both programming language intricacies and of security threat models.

- The third roadblock is the design of **exhaustive** analyses. That is, given a class of security properties and a target language, the design and implementation of source code analysis algorithms that catch all possible violations of these properties, for all values in the input domains, on all programs in this language. This third property is often referred to as the **soundness** of an analysis, and is required when a proof of absence of a class of errors is requested.
- The fourth roadblock is the **performance** of the analyses, in terms of execution time and of number of false alarms.
- The fifth roadblock is the application of source code analysis techniques to **industry-specific systems**.

These three last items require serious advances of the state of the art in computer science, combined with a capability to transfer scientific progress into technological features.

[18] http://www.tiobe.com/index.php/content/paperinfo/tpci/index.html

2.11 Network and mobile security

2.11.1 Network security

2.11.1.1 Introduction

Firewalls have been traditionally used to inspect and filter incoming connections and traffic. Indeed, traditional firewalls are placed in the periphery of an organization and make sure that they forbid all incoming connections towards any IP address inside the periphery. Any computer that needs to service incoming connections, such as an email server or a web server needs to be placed outside the periphery.

*Firewalls have to become more "active" inspecting not the **appearance** of the incoming packets, but the **behaviour** they invoke once they reach their destination application..*

2.11.1.2 Current Status

There are several categories of firewalls:

- **Network packet filters**. Placed at the periphery of an organization, and armed with a set of rules these firewalls inspect traffic (usually) at the IP level and filter out any traffic that matches a rule.
- **State-full firewalls.** Although network packet filters make decisions based entirely on the information contained in the current packet, statefull firewalls usually operate on a flow basis. For example, they make sure that they have seen a valid TCP handshake before they apply a TCP-level rule.
- **Deep-packet Inspection Firewalls**. Although most firewalls inspect only IP/TCP headers, such inspection is usually not enough to find attacks hidden deeply inside the payload. To address this problem, deep-packet inspection firewalls are able to apply rules that inspect not only TCP/IP headers but also the packet payload.
- **Host level**. Although network-level firewalls have the potential to protect several IP addresses at the same time, they are challenged when faced with encrypted traffic and/or rules that operate based on application-level semantics. Such cases can be addressed with host-level firewalls, that is, firewalls that run at the end host. These firewalls monitor not only IP packets, but also (unencrypted) application input and output. Thus, they are able to protect hosts even when attacks are hidden inside encrypted streams.

2.11.1.3 Research Challenges

Firewalls are usually the first line of defence against attacks from the outside world. However, they are bound to face several challenges including:

- **The changing model of secure periphery**. Firewalls are based on the notion of the "periphery". Every computer inside the periphery is considered to be trusted and every computer outside the periphery is potentially not trusted (unless whitelisted). Unfortunately, this model is rapidly changing. As employees spend an increasing percentage of time working "on the go", the boundaries that define the periphery have started to blur. Firewalls need to work in a distributed environment where they assume that there is no periphery or that the periphery has already been breached.
- **The role of encryption**. Over the past years we have been an increasing percentage of our communication to be encrypted. We expect that the trend will continue and we will reach a point where only a tiny percentage, if any at all, of our communications will be left unencrypted. In this world, firewall-related functionality should be moved to a place after the data have been decrypted, most probably at the application level.
- **The active nature of the attacks**. Most firewalls are based on "pattern matching". That is, if they see a pattern in the header or payload of an incoming packet, they match a rule. Unfortunately, attacks have become very sophisticated and can easily "evade" such simple pattern-based matching approaches. In the next years firewalls have to become more "active" inspecting not the *appearance* of the incoming packets, but the *behaviour* they invoke once they reach their destination application.

2.11.2 Mobile security

2.11.2.1 Introduction

Mobile devices are currently the main clients to access Internet services, in addition to have the usual telco facilities for voice communication. Thus mobile security is a main area of research. It inherits many of the PC security problems amplified by the specific nature of mobile devices, e.g. access to owner credit lines, and sensors availability. There is indeed a proliferation of malware for mobile devices as well as for new attacks on these devices.

2.11.2.2 Current Status

Intrusion detection/prevention systems (IDS/IPS). There are several approaches to detect and further prevent the malware intrusions on smartphones that resemble the approaches in the PC, still with specific features, being the features of mobile phones peculiar (as sensor presence):

a) prevention-based approaches: using cryptographic algorithms, digital signatures, hash functions, important properties such as confidentiality, authentication or integrity can be assured; in this scenario, IDSs have to be running online and in real-time; b) detection-based approaches: IDSs serve as a first line of defence by effectively identifying malicious activities. Intrusion can be detected with two main approaches, anomaly detection and signature based, i.e. 1) *anomaly-based* (anomaly detection, behavior-based), which compares the "normal" behavior with the "real" one; 2) *signature-based* (code-signature detection, knowledge based, detection by appearance), based upon patterns recognition of specific features. Most of the actual approaches are currently on signature based mechanisms. For anomaly detection, there are also some approaches mainly focussed at specific levels of observation. We can summarise as follows these layers: user; application; virtual machine or guest OS; hypervisor; physical. Recently, also multi-layers approaches have been developed.

Application security frameworks. There are several existing frameworks for the protection of applications for mobile devices:

- **Static mechanisms:** These allow to classify applications on mobile device through code inspection at load time. Techniques as control/data flow, model checking and related activities have been adopted. Proof carrying code techniques are also investigated for embedding proofs of properties of application code in the downloaded package. Multi-criteria analysis methods have also exploited to rank and classify the risks related to applications running on the devices (mainly based on static factors).
- **Application Policy Run-time Enforcement:** The basic idea of these activities is to impose policies on specific applications and enforce those at run-time trough application monitoring. Several policy models can be enforced. Recently usage control policies have been enforced on such devices, using rich authorization and obligation languages (as variant of XACML).
- **Hybrid approaches:** Rich approaches in security merge static and dynamic approach as security-by-contract that merges proof carrying code with run-time policy enforcement.

Trusted platforms. There are also specifications for trusted mobile phone platforms as the Mobile Trusted Module (MTM) from TGC. MTM to increase the security of smartphones by providing basic cryptographic capabilities, such as random number generation, hashing, protected storage of sensitive data (e.g. secret keys), asymmetric encryption, as well as generation of signatures. These cryptographic primitives can be exploited to implement hardware-based security services, such as device authentication, integrity measurement, secure boot, and remote attestation. The MTM provides a root-of-trust for smartphones in the same way as the TPM does for personal computers. In principle, the MTM is an adaption of the TPM for smartphones and, hence, its specification is similar to that of the TPM, which facilitates interoperability within the existing trusted computing framework for personal computers.

2.11.2.3 Research Challenges

Several of the research topics mentioned above are still relevant fields of research, we can also highlight some recent trends as:

- **Personal data management.** The huge plethora of sensors that collect information of several types and the need to protect such personal information are two main aspects to be faced. On the one hand we need to protect the user from delivering unwanted personal information, on the other one we need to balance with the need of applications that need to know information for working properly as in participatory sensing applications for emergency management, where integrity of data should be enforced.
- **Bring Your Own Device (BYOD) is** a main trend in organizations, several solutions have been depicted, still this is a very relevant research challenge, mixing several of the topics previously mentioned.
- **Managing the lack of diversity.** Currently there is one billion of devices with just one operative system. Vulnerabilities in this OS could affect a wide variety of devices. We need to consider diversity and lack of diversity in the future scenarios.
- **Repackaging of applications.** Several mobile applications available in one market are taken, slightly modified (often with the insertion of malware) and then repackaged and made available in the same market or in others. This is a main vector of infection for end-users as well as of economic damage to application vendors.

2.11.3 Security of supporting infrastructures

2.11.3.1 Introduction

The current operation of the Internet heavily relies on a set of infrastructure protocols and associated services that form a critical environment. These protocols and services can be separated in two categories:

- Routing protocols and services ensure that packets traverse the network from source to destination, according to the most efficient path. There are wide-area routing protocols such as the Border Gateway Protocol, and local area routing protocols such as OSPF and RIP. In the same category, there are segment management protocols such as STP, and MPLS that heavily relies on routing techniques to provide virtual private networks.
- Access protocol and services enable devices to obtain network access. The two best known such protocols are DHCP (which provides devices with IP addresses) and RADIUS (which provides authentication and billing). In this category, we also include the Domain Name Service, which associates addresses and names.

All these protocols are vital to the proper operation of the Internet. Yet, many of them have also been heavily used by attackers, either as attack vectors or as command and control channels.

2.11.3.2 Current Status

- **We have come to heavily rely on these protocols**, even though their original design does not take security into account. More secure alternatives have been designed for a long time. There seems to be a significant progress towards securing the DNS infrastructure with DNSSec, but S6BGP is not near deployment. Other capabilities, such as traceback and authentication of origin, have been abandoned even when specifications exist.
- **These protocols are highly vulnerable to attacks**. DNS is probably the best known case of both an attack vector (due to a wealth of protocol and software vulnerabilities) and a command and control channel. BGP has been the subject of incidents with very significant consequences, mostly due to human errors, but there is a trend showing malicious activity.

2.11.3.3 Research Challenges

- **Propose secure alternative to these protocols that are both operationally and economically feasible**. One of the main drawbacks of existing solutions is that they require costly changes in hardware as well as additional manpower to manage them.
- **Expose protocol behaviour to users**. Users and operators have very little visibility on the underlying behaviour of these protocols, which are extremely complex and exchange thousands of messages. Current work focuses on after-the-fact analysis of traces. Yet, it takes many months before failures and attacks are detected and made public, except in cases where their impact is mmediately perceptible

through loss of service. There is a need for faster and more accurate tools to detect attacks against all these protocols.

2.11.3.4 Existing Tools

There are many open implementations of these protocols and services, such as Freeradius, OpenDNS, BGP, etc.

2.12 Cybersecurity threat technologies/ Offensive technologies

2.12.1 Introduction

Offensive technologies are defined as the mechanisms and tools that cyber attackers use in order to achieve their malicious purposes. Ranging from viruses, to worms, to botnets, and, (why not?) social engineering, offensive technologies continue to evolve on a daily basis trying to stay ahead of any known defense mechanisms.

2.12.2 Current Status

Before the era of the Internet, computer attacks used to spread in the form of viruses on floppy disks. However, the advent of the Internet clearly demonstrated that attacks can compromise hundreds of thousands of computers in a few hours or so. The ability to remotely compromise a computer coupled with the value that a compromised computer may bring quickly moved organized crime into the cyber world completely changing the motives and dynamics of the cyber security scene. Although the cyberattacker of yesterday was often seeking fame and peer recognition through a massive cyberattack that would demonstrate his/her computer skills, the modern day attacker prefers to stay below the radar, move around the Internet undetected secretly seeking financial and/or political rewards. To achieve their goals cyberattackers employ a number of offensive mechanisms including:

- **Malware**: Malicious software is usually the most common mechanism to remotely control a computer. Being installed immediately after a computer is compromised, malware is used to communicate with the attacker, receive instructions and perform malicious and illegal tasks
- **Botnets**: Compromised computers, also called bots (from robots), are usually organized into networks called botnets. These networks may grow as large as tens of thousands of machines having a significant firepower than can not be easily mitigated.
- **Buffer Overflows**: In order to compromise a remote computer an attacker usually triggers some bug that diverts the flow of control from its usual legitimate path to a path favourable to the attacker. Buffer overflows are the most common such bug. They enable the attacker to write arbitrary data in the stack (or heap) of a vulnerable process and even divert the flow of control to the attacker's code. Although safe programming languages and non executable stacks have limited the effectiveness of software exploitations, buffer overflows have not been eliminated and can still be used coupled with new programming styles such as return-oriented programming.

2.12.3 Research Challenges

Over the past years we have witnessed a co-evolution of attackers and defenders. That is, as soon as defences address a given type of attackers, attackers evolve their approach to a new stage that can not be addressed with the developed tools. At the time of this writing it seems that pressing research challenges in the area of mitigating offensive technologies include:

- **Polymorphic/Metamorphic Attacks – the changing face of the attack**. Attackers usually masquerade their malicious code to look like a legitimate program. They even change the appearance of their attack so that no two instances of the same attack look the same. This implies, that it is getting increasingly difficult to identify and detect attacks. We need to develop sophisticated environments that are able to identify such carefully masqueraded attacks.
- **Undetected Threats**. There exist attacks that can not be detected by most, if not all, antivirus systems out there. This implies that some systems are compromised and continue to operate without their owners realize that they are compromised. Such systems may include not only clients, but also servers

out there. These threats want to stay below the radar as much as possible and thus limit any obviously suspicious activities, such as sending of SPAM email, and, instead, concentrate on capturing information available to or accessible by the compromised system. Operating in a compromised world and containing the damage that a persistent threat can do is a challenging problem that we have only started to address.

- **Advanced Persistent Threats**. By using the increasingly large amount of software exposed to external attacks, and the large amount of flaws it contains, attackers are now launching attacks that attempt to be both stealthy, and continuously ongoing. They exploit flaws that range from subtle protocol misbehaviors, to intricate software implementation vulnerabilities, to complex systemic interactions, and more. Developing these attacks requires both high-level capabilities and strong intents, which only large entities can dispose of.

2.13 Information Sharing technologies

2.13.1 Introduction

Cybersecurity Information Sharing can be defined as the set of technologies, data formats, messaging protocols, policies, and frameworks that enable the exchange of cybersecurity-related information between peers or within a community of entities. The Information Sharing Systems are secure platforms designed to efficiently and effectively distribute critical information about offenders, crimes, and cyber-attacks incidents, in order to enhance prevention and apprehension activities by law enforcement.

As far as cyber security is concerned, there exist many different standards and initiatives that attempt to provide solutions for cyber security information exchange. These tools have recently begun to attract interest of information security agencies and organizations, and are gaining more and more acceptance. One might say that Information Sharing has become a fundamental piece in the fight against cyber threats and as a means for building a comprehensive situational awareness. The information may relate to threat intelligence (actors, TTP, campaigns, etc.), malware, vulnerabilities, attack patterns, cyber observables, security incidents, etc.

2.13.2 Current Status

There are several standards and proposals aimed at defining the technical aspects of information sharing.

Making Security Measurable (MSM) initiative led by MITRE presents a comprehensive architecture for cyber security measurement and management, where current standards are grouped into processes and mapped to the different knowledge areas, each of which refers to a process (put in parentheses): Asset definition (inventory); Configuration guidance (analysis); Vulnerability alerts (analysis); Threat alerts (analysis); risk/attack Indicators (intrusion detection); and incident Report (management). Next Table relates current MSM standards to these areas:

	CPE	OVAL	SWID	XCCDF	CCE	OCIL	CCSS	CVE	CWE	CVSS	CAPEC	CVRF	MAEC	CybOX	IndEX	STIX	IODEF	CPE	CEE	RID	RID-T	CYBEX	CWSS
A	•	•	•															•					
C		•		•	•	•	•																
V		•						•	•	•		•											
T								•	•	•	•		•	•	•	•	•		•	•	•		
I	•							•					•	•	•	•	•	•	•	•	•		
R	•	•			•			•	•	•			•		•	•	•			•	•	•	•

Source: Jorge L. Hernandez-Ardieta, Juan E. Tapiador and Guillermo Suarez-Tangil. *Information Sharing Models for Cooperative Cyber Defence*. 2013 5th International Conference on Cyber Conflict (CyCon'13). K. Podins, J. Stinissen, M. Maybaum (Eds.) 2013 © NATO CCD COE Publications, Tallinn.

Other remarkable initiatives for Information Sharing are:

- TAXII™ (Trusted Automated eXchange of Indicator Information), which, using STIX language, defines a set of services and message exchanges that, when implemented, enable sharing of actionable cyber threat information across organizational, product line and service boundaries.
- TLP (Traffic Light Protocol) is a set of designations used to ensure that sensitive information is shared with the correct audience.
- CybOX (Cyber Observable eXpression) is intended to be a set of fundamental data types for communicating details of campaigns, threat sources, malware characteristics, and other cyber security events that are valuable for a large number of cyber-security use cases. Such use cases are, for example, event management/logging, malware characterization, intrusion detection/prevention, incident response, and digital forensics. CybOX's main objectives are the consistency and the interoperability across this wide range of use cases through providing a common structure and content types. As of this writing, CybOX is an evolving specification.
- STIX (Structured Threat Information eXpression) and MAEC (Malware Attribute Enumeration and Characterization) are two composite data structures that are built on top of CybOX. STIX conceptualizes and organizes different traits of threat information into independent and reusable constructs (data types). As of this writing, STIX is an evolving specification. Currently, STIX is comprised of seven main constructs:
    - **Campaign** is typically linked to a series of Incidents and can be linked to specific Threat Actors, since a Campaign typically employs specific TTP and individual Incident can be linked with common set of Indicators. TTP stands for tactics, techniques and procedures; it can be used to link a series of Incidents to a specific Campaign.
    - **Threat Actor** can be linked to a set of TTPs. Incident can be linked to specific TTP used by specific Threat Actor. During incident response, a set of Indicators may be identified. Incident can keep a record of Course of Actions that were taken during incident response.
    - **Indicator** is typically linked to a set of relevant cyber observables. An Indicator can be linked to Course of Actions, or to TTPs.
    - **Course of Action** characterizes both preventive measures and response measures.
    - **Exploit Target** characterizes vulnerabilities or weaknesses that were targeted by specific TTPs. Exploit Target may suggest potential Course of Action, e.g., configuration changes or software upgrade.
    - **MAEC** specializes in communicating details of malware. MAEC conceptualizes malware at multiple levels of granularity – mechanism, behaviour, action and its implementation – and bridges them through grouping primitives called bundle and package. Unlike traditional virus names that fail to convey deeper technical insight, MAEC tries to capture both behaviour and mechanism of malware in a structured manner.

2.13.3 Research Challenges

There are many requirements that Information Sharing Systems need to meet[19]. In this section we briefly discuss some of the most important ones.

Objectives:

- **Reusability:** There is a need of a complete security ontology that can be reused and extended, and the security community can trust.
- **Scalability:** There is a need of mechanisms that can automatically share large quantities of information.

Challenges:

[19] http://www.ccdcoe.org/publications/2013proceedings/d3r1s5_dandurand.pdf

- **Storage volume:** The ever growing volumes of data stored on the Internet or included in specific products, such as vulnerability repositories, signatures used by anti-virus products, etc., make it difficult to access and eventually share the desired information.
- **Different sources:** The large number of different sources can lead to inconsistencies of the collected and about to be shared information due to the existence of erroneous data.
- **Confidentiality:** There are concerns regarding the confidentiality of exchanged data. Effective means by which redistribution can be satisfactorily controlled must be addressed.
- **Speed:** Cyber attacks execute and succeed in computer time, so we need information sharing mechanisms that operate within the same order of magnitude. Contrary to this, current approaches for information sharing heavily depend on the human factor. We need to design new frameworks that minimise the human intervention during the information sharing processes. To achieve this, we need to explore other relevant dimensions of the information sharing problem that have been less researched so far, notably those related to deciding on what to share, with whom, when, as well as reasoning about and adapting to the repercussions (risk) of sharing. To meet this in an automated manner we need contributions from different areas, such as graph analysis and trust/reputation. Decision-making support tools for specific scenarios where human intervention is required is also a potential field of research.
- **Flexibility:** The intrinsic flawed and highly vulnerable nature of technology leads us to conclude that absolute trust cannot be achieved in cyber space. We should not rely, in absolute terms, on any information independently of who is the source. This demolishes the requirement that current approaches claim in mandating full trust in the peers that are part of an information sharing community. This situation is aggravated by the fact that we cannot foresee who will have the knowledge needed to prevent or respond to certain incident. Consequently, static, rigid procedure-based information sharing communities will for sure perform ineffectively. We need new approaches where information sharing communities can be dynamically adapted (dynamic composition) based on context, trust, and need-to-share requirements.

2.14 Big data

2.14.1 Introduction

Big Data refers to very large, dynamic, multi-sourced data sets. Analysis of Big Data could reveal relationships and insights that would be very valuable for businesses, governments and organizations to understand their environment and challenges. Therefore, collecting, storing and analyzing big data is essential to develop strategies, policies and solutions to pressing problems. The use of Big Data technologies applied to different markets is already showing a great impact by improving processes performance and in consequence affecting the global productivity.

The current economic situation in Europe demands new solutions and innovation in the use of these technologies. Given that data has become a new factor of economic competitiveness and production, it is essential to have the right technological basis and organizational structure to acquire and exploit data. While major US based companies are widely recognized for their exploitation of Big Data, European organizations, including SMEs, are not exploiting Big Data to similar levels, thereby overlooking an important contribution to competitiveness and innovation and creating a dependency on technologies coming from outside.

2.14.2 Current status

Big Data is directly generated by users or indirectly derived from their activities by the tools, systems and processes they use. Part of it is also generated automatically by the systems that make up our digital environment. As such, the volume and sources of big data multiply continuously. Classical

approaches are not well suited for big data analysis due to the scale of the data and its dynamic sources and varying structure. This is instead made possible by a variety of novel and original enablers, such as data mining techniques, parallel and distributed processing technologies, NoSQL databases and in particular by the emergence of cloud computing. These capabilities are collectively referred to as Big Data Analytics techniques.

Security mechanisms in the Big Data domain need to address *speed* and *scalability* as major concerns, so *data at rest*, *data in transit* and *data in use* need to be secured under these constraints. In addition, malicious nodes and sources could destabilize the Big Data environment and therefore they need to be secured. As a new technology domain, security considerations are emerging as problems arise in the implementations rather than security requirements being included in designs from day one.

2.14.3 Research challenges

Emergence of Big Data is significant for the ICT security research community from two perspectives. One is the challenge to secure Big Data, given its huge volume, rate of change and distributed sources; the other is the opportunity to derive new security tools and systems using big data analytics techniques applied to security data.

- **Speed and scalability:** Creating efficient logging, monitoring and auditing mechanisms and implementations is a major challenge due to the huge volume of the data and the large number of events and operations that take place. Applying encryption at scale and speed is also a major challenge.
- **Privacy preservation:** The advanced correlation and intelligence capabilities of Big Data analytics techniques creates a challenge for privacy preservation. It is indispensable that Big Data analytics strikes a balance between privacy preservation and the usefulness of its tools and applications. Encryption is an essential tool in this domain. Additional measures to add transparency and accountability are key, such as efficient logging, auditing tools, authorization, authentication and access control. These would collectively provide privacy safeguards around big data technologies.
- **Data ownership:** In addition to the directly provided data, a lot of the derived data about users is not visible to the users themselves. While there is the potential for very helpful services created out of these data, the potential for exploits is also there. Many threats to users and systems might emerge out of the malicious use of these data such as social engineering attacks, targeted attacks, financial fraud and identity theft. Creating mechanisms to identify data ownership, tag data accordingly and to exert control over that data are important challenges.
- **Proactive security:** In the domain of big data analytics for security intelligence, big data capabilities are envisioned to add predictive and proactive capabilities to existing security tools and systems. With the inclusion of correct data sources and types and the application of adequate correlation functions the threat environment and the attack surface can be analyzed in real time and appropriate countermeasures could be applied to prevent attacks, rather than responding to them. This would be a major change and breakthrough from the current information security practice where attackers seem to be one step ahead of the defenders. The underlying challenge in this respect is to be able to create a data set that includes the correct inputs, then to correlate these inputs in the right context using the correct analytical tools.

2.14.4 Existing tools

Big Data technologies can be divided into two groups: batch processing, which are analytics on data at rest, and stream processing, which are analytics on data in motion. An example of batch processing is the MapReduce programming framework; different implementations of this approach have been done, but the most common one is Hadoop, which has become a de-facto standard framework for 'Big Data' to store, process and analyse hundreds of terabytes, and even petabytes of data. The stream processing technologies include Storm which is an open source distributed and fault-tolerant real-time

computation system designed for supporting real-time processing of large scale streaming data on clusters of horizontally scalable commodity machines. Other examples include Spark (provides tools to combine SQL, streaming and complex analytics with Hadoop) and Dremel (scalable, interactive ad-hoc query system for analysis of read-only nested data).

In the Big Data for security intelligence domain large companies like IBM and RSA provide emerging security analytics tools. In the coming 3 to 5 years these tools are envisioned to multiply with SME's increasingly taking part in the market. With the democratization of cloud infrastructures and the availability of open source solutions, the tools SME's need to innovate in Big Data are coming together.

2.15 Data Protection

2.15.1 Introduction

The growing amount of information daily collected and produced by users and organizations has contributed to the success and rapid evolution of novel scenarios, where the techniques for processing, storing, communicating, sharing, and disseminating information have radically changed. Data outsourcing, cloud computing, and social networking are examples of such emerging scenarios that have brought enormous benefits in terms of the availability of a universal access to data as well as of elastic storage and computation services. Such scenarios, however, introduce new risks and pose new research challenges, especially with respect to the protection of sensitive data. In fact, in today's digital infrastructures, it is harder to guarantee that sensitive data remain properly protected and that users maintain the control on who can access their data when they are stored at an external server.

2.15.2 Current Status

When data are stored at external servers, it is of primary importance to provide means of protecting the confidentiality and integrity of the information, while guaranteeing its availability to legitimate users. Typically data are encrypted for storage at external servers. Although cryptographic techniques enjoy today a limited cost and an affordable computational complexity, encryption carries the burden of managing keys and affects the ability to perform queries over data. Fragmentation approaches have also been investigated, in conjunction or in alternative to encryption, for protecting confidentiality of data associations.

2.15.3 Research Challenges

Data protection techniques: A first problem that has to be considered when storing data on an external server is to guarantee confidentiality, integrity, and availability to the stored data themselves, even to the provider's eyes. Data protection techniques should be able to satisfy generic privacy constraints corresponding to different privacy needs. Such constraints, for example, can state that the values assumed by some attributes (e.g., phone numbers or email addresses) are considered sensitive and therefore cannot be stored in the clear or that the association between values of given attributes (e.g., patients' names with illnesses) is sensitive and therefore should not be released. The proposed solutions should also be robust against possible inferences that can be drawn exploiting data dependencies. Ensuring integrity and availability of data in storage requires providing users and data owners with techniques that allow them to verify that data have not been improperly modified or tampered with, and that their management at the provider side complies with possible availability constraints specified by the data owner.

Fine-grained data access: Since the storing and processing servers should not have access to the plaintext data, data cannot be decrypted for query execution. Also, evaluation of conditions over encrypted data provides very basic and either inefficient or leaking information. Metadata information (indexes) can be provided for supporting query functionalities. Indexes should be clearly related to the data behind them (to support precise and effective query execution) and, at the same time, should not leak information on such data to observers, including the storing server. Also, there may exist the need of combining indexes with other protection techniques (e.g., fragmentation or access control restrictions) and such combinations should not introduce privacy breaches. The design of inference-free indexes that can be combined with other protection techniques without causing privacy violations are all aspects that still require further investigations.

Data computations integrity: As we move further into the information age, we face many challenges regarding

the integrity of computations possibly involving different (and untrusted) data sources. The integrity of computations is a critical issue since the data obtained as a result of a computation are often used to take accurate decisions that may have a serious impact on the human life. This problem is clearly not new and many solutions have been proposed (e.g., there are solutions based on specific data structures or signature methods). Some of these solutions however rely on the presence of trusted components for the verification of the computed results or do not provide a support for complex operations such as many-to-many joins on different (possibly distributed) datasets. An interesting research direction is therefore the design of efficient and effective solutions able to verify the correctness of the results computed through complex operations, also using modern architectures such as MapReduce.

Distributed query processing under protection requirements: The correct definition and management of protection requirements is a crucial point for an effective collaboration and integration of large-scale distributed systems. This problem calls for a solution that must be expressive to capture the different data protection needs of the cooperating parties, as well as simple and consistent with current mechanisms for the management of distributed computations, to be seamlessly integrated in current systems.

Query privacy: In several scenarios neither the data nor the requesting user have particular privacy requirements but what is to be preserved is the privacy of the query itself. Consider, for example, scenarios allowing users to query external medical databases. The fact that a user queries the data in search for treatments for a given illness discloses the fact that the user is interested in the specific illness (and therefore the user, or a person close to her, might be suffering from it). It is therefore important to design techniques that enable users to query data while not revealing information about the specific query (i.e., the data the users are looking for) to the server holding the data. Note that effective protection of query confidentiality requires not only protecting confidentiality of individual queries, but also protecting confidentiality of access patterns.

2.15.4 Existing tools

Basic data protection typically is ensured by encryption solutions, requiring however decryption (and hence exposing information to the server) for query execution. Only prototypal approaches exists for some of the noted challenges.

3 Internet of Things - Cloud Computing

3.1 Internet of things

3.1.1 Privacy and trust in IoT

3.1.1.1 Introduction

From the many definitions of the Internet of Things (IoT) paradigm, we can infer that one of its basic tenets is "A worldwide network of interconnected entities". Beyond this tenet, the IoT has other specific features that differentiate it from other paradigms:

- **Heterogeneity.** The IoT is composed of multiple actors (e.g. passive tags, embedded systems, wireless sensor networks, traditional computing devices). All these devices have different capabilities in terms of computational power, user interface, power consumption, storage, communication capabilities, etc.
- **Distribution.** In the IoT vision, its elements will be scattered all over the globe, and will use the Internet to collaborate with each other. Therefore, the concept of 'perimeter' will become fuzzy.
- **Large scale.** A huge amount of objects (from the 'billions' considered by some authors to other, more conservative, estimations) will have the ability to produce and consume services over the Internet. These data produced by these objects will have to be visualized and processed in an efficient way.
- **Dynamicity.** The interactions between the objects of the IoT will change according to the actual needs of their users. Moreover, many of the IoT objects will be mobile, such as cars in vehicular networks.

3.1.1.2 Current Status

The paradigm of the Internet of Things is, as of today, constantly evolving. Numerous research projects are tackling various IoT research challenges, studying open issues such as architecture, sensing-as-a-service, smart spaces and environments, industrial applications, and many others. In fact, many nations, such as UK and China, have publicly mentioned the Internet of Things as one of their research priorities. Moreover, major players, such as General Electric, Intel, ARM, and Cisco, are currently developing various IoT-related platforms.

3.1.1.3 Research Challenges

- **Large-scale infrastructure**. The creation of an IoT infrastructure is not trivial, as it is necessary to manage the identification, discovering, monitoring and collaboration of a myriad of heterogeneous objects located in multiple contexts. It is also essential to assure the interoperability between all IoT technologies, using various strategies such as compatible protocols, intelligent gateways, etc. Without proper interoperability, the IoT will never evolve beyond the 'Intranets of Things' ("islands") phase.
- **Data management**. As most objects are expected to produce and consume data and services, it is essential to assure semantic interoperability between all heterogeneous systems. Note that we assume that all data and processes are not completely reliable (e.g. due to faulty devices, rogue systems), thus it is necessary to develop efficient collaborative technologies to manage this uncertainty.
- **Processes and Analytics**. The research community must develop event-driven architectures that can help business processes to collect, verify, and manage numerous events from multiple, world-wide sources. Moreover, as the processes themselves can be highly distributed, tools are necessary to compose, verify, and adapt these distributed processes.
- **Self-adaptive systems**. Cognitive technologies and contextual intelligence are crucial within the context of the IoT. Such systems will allow IoT elements to be aware of their physical and digital environment. This awareness can also enable the development of a self-learning, self-repairing, and self-organizing autonomic network. Nevertheless, the network must be transparent about its actions.
- **Eco-friendly systems**. Some IoT applications assume that the devices will be discarded once their task is completed. Thus, it is necessary to develop nature-friendly technologies: from energy harvesting systems (solar, thermal, vibration...) to biodegradable materials.

3.1.1.4 Existing Tools

At present there are various standards that have been tailored to the needs of the IoT ecosystem. Examples are the Constrained Application Protocol (CoAP) and the IPv6 over LoW Power wireless Area Networks protocol (6LowPAN), both defined by the IETF. Other standards are being defined by various bodies, such as ITU-T, ISA, IEEE/ISO/IEC, and others. As for HW devices, there are multiple platforms available for both hobbyists (e.g. Arduino) and professionals. Other tools, such as semantic interoperability, are still in the research phase.

3.1.2 IoT Models

3.1.2.1 Introduction

As with any other infrastructure, the IoT will be targeted by various malicious entities, as there is benefit (e.g. fame, profit, damage, terror) on attacking the system. For the IoT in particular, its major threats are as follows:

1. **Crashing**. Prevent the IoT devices and/or its elements (resources, communication channels) from functioning properly. This threat is quite serious, due to the limited resources available to some IoT devices.
2. **Extracting**. Attackers can extract information from the IoT devices. While constrained IoT devices are especially vulnerable, attackers targeting local systems will probably obtain little global information.
3. **Capturing and Poisoning**. An attacker controls one or more IoT devices, disrupting the services of the system. In fact, this is one of the reasons data and processes cannot be considered as completely reliable. Still, the scope of this attack is limited to the current role of the devices.

As any of these threats will actually affect not only the virtual world (data), but also the physical world (physical systems, users' environment), it is essential to develop strong security foundations that can enable the creation of a fault-tolerant IoT system.

3.1.2.2 Current Status

While there are various security mechanisms that provide protection to existing IoT actors (e.g. sensor network security infrastructures, RFID identification systems), these solutions were not designed to protect the IoT as a whole. Moreover, as the sum is greater than its parts, other limitations arise:

- **Identity and Authentication**. Various identification systems (e.g. ucode, EPCGlobal, IMEI) can be used to globally identify various underlying IoT technologies (e.g. RFID tags, mobile phones). However, not only these systems are not designed to be compatible with each other, but there are also other issues (identification using attributes, multiple "soft" identities) that must be taken into account.
- **Access Control**. Traditional access control mechanisms are difficult to apply in the IoT context, due to scalability and management issues (in ACL systems), and due to the need of defining interoperable roles (in RBAC systems).
- **Protocol and Network Security**. The current IoT landscape is composed of "islands", where gateway devices with enough resources implement the security protocols (e.g. TLS) while internal systems implement their own proprietary systems – tailored to the constrained devices. Efforts are being made to develop fully interoperable protocols (e.g. 6LowPAN, CoAP), although the integration of efficient security mechanisms and primitives is still a challenge.
- **Privacy**. Conceptually, users could make use of various tools (e.g. data minimisation, granularity, homomorphic encryption) to protect both their personal data and any data they produce when interacting with other IoT entities. However, although such tools are available for non-IoT environments, they have not been actively integrated in existing IoT protocols and systems.
- **Trust**. Trust is closely related to accountability: it allows IoT entities (including users) to deal with uncertainty by understanding the state of their surroundings. However, it is still necessary to answer the following questions: How can an IoT entity obtain, store and share information about the state of other IoT entities? How can all entities implement transparency policies, allowing all users to know the state of the virtual world that surrounds them?
- **Fault Tolerance**. While there are various mechanisms that help to provide fault tolerance (e.g. intrusion detection systems), such systems can only detect problems in local environments. Some

solutions allow different detection systems to provide a holistic point of view of the state of the whole network, but they need to be optimized for IoT systems and their threats.

3.1.2.3 Research Challenges

The inherent features of the Internet of Things impose various challenges in the development of scalable, efficient and reliable security mechanisms:

- **Heterogeneity.** This feature affects the development of almost all security mechanisms, as all systems should be able to interoperate with each other in order to realize the vision of the IoT. This is not a trivial task. For example, constrained devices might not be able to implement all security services, and different communication networks can also have different capabilities (e.g. packet size, throughput).
- **Distribution.** As the notion of 'perimeter' becomes fuzzy, various security mechanisms (from access control to intrusion detection systems) must be designed to take this openness into account. Moreover, there is the need of developing mechanisms that enable the secure collaboration between multiple entities located in different contexts – without completely relying on centralized systems.
- **Large scale.** The scale of the IoT mainly affects the authentication mechanisms, as entities that probably do not know each other in advance will have to identify themselves. Besides, as there will be a myriad of objects (and owners!), it will be necessary to clearly define who owns the 'things', and how they can be managed. It influences other mechanisms as well, such as trust and fault tolerance, where it is necessary to securely and efficiently create a mental model of the status of the network.
- **Dynamicity.** All security mechanisms must be prepared to cope with a dynamic environment where peers can appear and disappear anytime – or delegate their functionality to other peers.

3.1.2.4 Existing Tools

Very few IoT standards consider explicitly the integration of security mechanisms, and only some advances exist in the area of communication protocols (e.g. DTLS in constrained environments). Still, the research community is currently studying IoT-specific security tools (e.g. key management systems, trust mechanisms, ticket-based access control), and various groups have defined tentative roadmaps that describe the most important security mechanisms that should be developed in order to create a secure IoT ecosystem.

3.1.3 Current Approaches/Projects

There are multiple ways to design and implement the underlying infrastructures that will provide the IoT services. Such IoT models can be mainly categorized into Internet-centric (Centralized) or Object-centric (Distributed):

- **Centralized IoT model**: All data processing and service providing systems are located in one single, central entity (e.g. a Cloud Computing infrastructure); data acquisition networks (e.g. sensor networks, intranet of things) will mainly work as passive data providers. This strategy has various benefits, such as good service uptime (due to the use of the underlying cloud infrastructure), and good interoperability (all data sources only need to interact with the API of the centralized systems).
- **Distributed IoT model**: Similar to a peer-to-peer system, all entities are interconnected and can produce and consume services. Central systems might exist, but they are no longer the vertebral column of the IoT. This strategy can be able to provide a highly scalable and robust infrastructure.
- **Hybrid IoT model**. Beyond a purely centralized or purely distributed system, it is also possible to combine both models in certain deployments. For example, various central entities can exchange information with each other, effectively increasing the scalability and availability of the IoT infrastructure. Moreover, it is also possible to allow local entities to process their information and serve it to its local customers instead of becoming mere data providers.

3.1.3.1 Current Status

Every IoT model (centralized, distributed, hybrid) influences over the design and deployment of the security mechanisms. Such models simplify how certain processes are implemented, but also impose certain limitations.

- **Centralized IoT and Security**. The centralization of resources facilitates the implementation of various security mechanisms. As IoT data providers (data acquisition networks) interact mainly with one central system, the number of communication protocols that must be protected is greatly reduced. Also, authentication and access control policies can be implemented in the central entity, as producers and consumer do not interact directly with each other but through the central service provider. However, privacy becomes more difficult to enforce, as central systems usually require the users to send all their information in order to provide meaningful, up-to-date services. Moreover, as centralized systems do not collaborate with each other, the availability of the IoT infrastructure can be at risk.
- **Distributed IoT and Security**. As every entity can become a service provider and consumer, the implementation of the security mechanisms becomes more complex. For example, in authentication and authorization, there is the need to deal with multiple enforcement points and conflicting policies. On the other hand, user-centric security mechanisms (e.g. privacy mechanisms) can benefit from this model. For example, in terms of privacy, users can specify their own data access policies, and also can manage how the data is presented to other data processing systems in terms of granularity (e.g. coarse location instead of fine location) and content (e.g. limited user's profile instead of full profile).
- **Hybrid IoT and Security**. There are security mechanisms that can benefit from the combination of centralized and distributed security mechanisms. One of these mechanisms is the network awareness and intrusion detection systems. A central system can have a holistic point of view of a large section of the IoT, thus it can be able to analyze the consistency of the data by running various statistical analysis methods. In contrast, local entities can acquire more detailed information (e.g. control messages, information flow) that can be used by intrusion detection systems.

3.1.3.2 Research Challenges

- **Optimization**. As aforementioned, certain IoT models simplify the design and implementation of various security mechanisms. Therefore, it is necessary to analyze not only how every mechanism can be adapted and optimized for every model, but also what are the benefits and drawbacks of such optimizations. We also need to analyze how certain mechanisms can benefit from a hybrid approach.
- **Specific weaknesses**. When developing security mechanisms for the IoT models, we also need to consider their weaknesses. For example, in the centralized IoT model, the central entity becomes a single point of failure; and although the number of attack vectors is usually smaller, a single vulnerability or misconfiguration can damage the whole network. As for the distributed IoT model, the impact caused by a successful attack will be smaller, but the number of attack vectors will surely increase. Note that, in all approaches, the data providers (the things) can be highly constrained and physically accessible devices – easy targets.
- **IoT Models and Heterogeneity**. The Internet of Things will surely remain heterogeneous, with multiple companies and infrastructures providing their services using their own standards. This heterogeneity will also affect the development of the security mechanisms for the IoT models: not only we might develop security mechanisms tailored for the different IoT models, but also we need to ensure that those mechanisms can interact with each other.

3.1.3.3 Existing Tools

As of 2014, there are various startups (e.g. Thingworx, Xively) and MNE (e.g. General Electric) that make use of the centralized IoT model to provide their services. There are also other companies (e.g. Sensinode) which provide local solutions that can enable distributed infrastructures. Nevertheless, the current status of security solutions for both centralized and distributed IoT models is still at its infancy, with security solutions developed mostly under the umbrella of research projects. Still, it should be noted that existing centralized solutions can provide some security using traditional WWW security mechanisms and protocols.

3.2 Cloud

3.2.1 Introduction

Cloud computing is a business model that combines a multitude of technologies to provide remote, dynamic and flexible IT services. Since its emergence, there was a tendency to consider cloud computing security as the security of its technical components. However, as its initial years pass and the obstacles that prevented its proliferation are studied, it emerges that there are security considerations that are specific to cloud deployments.

Cloud computing signifies a transformation of the established ICT deployments for organizations and individuals: from an on-premise IT infrastructure to an off-premise IT service. The associated security controls and mechanisms are also migrating with the infrastructure: security is no longer in the hands of the user. What is lost in the process is the “sense of security and control of the user/IT manager”, which is the most difficult to re-establish.

The above is mostly true for public clouds and hybrid clouds. Private clouds are exposed to similar threats as in-house ICT infrastructures and do not represent novel security challenges – except perhaps related to their size, which might make them attractive targets. As the level of abstraction increases and one moves from IaaS and PaaS models to SaaS models the sense of ownership, control and security gets even more damaged.

Therefore, what lies at the heart of cloud security is the matter of exerting control over ICT assets (systems, networks, data and applications). When individuals, other than the legitimate owners and users of the assets, exert this control, this creates threats and associated risks for these assets. Cloud computing makes it more difficult to assert control and cloud security tools are meant to make this process easier.

3.2.2 Current status

It was often stated that the security responsibility, which was with the in-house IT department before has now move to the cloud service provider security specialists. However, it is now seen as a joint responsibility, and tools and techniques are being developed to help both of these groups.

A significant portion of the research is being carried out to make cloud computing more transparent and accountable:

- Log and event management in the cloud,
- Monitoring, auditing, compliance and incident management,
- Data security: confidentiality, integrity and availability,
- Mitigation of insider threats,
- Cloud systems forensics tools,
- Access control technologies,
- Business continuity and disaster recovery.

Other research areas impacting cloud security are encryption technologies, physical security technologies and work related to securing hybrid and federated clouds. Users' control over their assets is also directly related to cloud vendor data formats, interoperability and portability. Although not related to security directly, these are closely related subjects which might render security mechanisms useless if proper cooperation is not ensured. Data security related aspects of cloud security are closely overlapping with Big Data security technologies. Therefore, they are not covered here once more.

Current projects: A list of cloud computing related EU projects are published here: www.cloudwatchhub.eu/Projects. Cloud Security Alliance (CSA) and ENISA regularly compile documents presenting best practices and frameworks for securing cloud deployments and services.

3.2.3 Research challenges

Many challenges exist in the effort to make cloud computing more secure and to provide more control to users and owners of data and applications. They can be categorized as follows:

- **Technology accessibility:** Most public cloud services rely on proprietary implementations. Their data structures, middleware technologies and security mechanisms are guarded as trade secrets. As a result,

efforts to make them more secure remain within the domain of the associated companies. However, these companies might not always feel compelled to make their systems more transparent and accessible to users and researchers. This provides a major challenge for cloud security research as well as interoperability, not mature yet, and compliance efforts. Incentives need to be created for these companies to move to more open structures and operation models as well as the promotion of open source alternatives. Scalability (for security, compliance, data retrieval and indexing) is also needed.

- **Increased target vector***:* As many services and data are concentrated in cloud service provider data centres, these become very attractive targets for attackers. While experienced security personnel run these systems, it is still a challenge where so many valuable assets and services are concentrated. Denial of Service attacks and disaster recovery become even more significant under these circumstances.
- **Insider threats:** As almost total control of data and applications and infrastructure is transferred to cloud service providers, insider threats within these providers become a major concern.
- **Cloud Model Selection***:* Most companies and individuals might prefer to move to a public cloud to minimize their costs and might prefer SaaS as the least technologically demanding solution. However, a proper risk assessment needs to be carried out on the assets and targets of each company, and a proper model needs to be selected based on the threats and risks identified. A hybrid or community cloud might be less risky for some organizations. As long as organizations do not make this assessment in cloud service and model selection they place themselves and their dependents under major risks. Proper risk assessment tools need to be provided for this purpose.
- **Trust erosion***:* The biggest challenge for the current clouds, however, is concerning to methods to establish presumptive trust on an evidence base, and to nurture the initially established trust relationship into one of trustworthiness in order to facilitate social and economic transactions. In dynamic systems and applications, such as in cloud computing, the sole expression of access rights is not enough. Policies for dynamic systems usually allow data providers to express which attributes may or may not be collected, but we need to allow data providers to specify provisions and obligations.
- **Privacy***:* Privacy challenges in future cloud computing are related to the need to protect data on-premise and in-transit and ensure access to it by authorized parties only, including transaction histories for potential privacy-enhancing user tools as well as for compliance and forensic purposes.
- **Software and hardware architecture used by cloud providers***:* Current cloud computing relies on virtualization technologies to isolate client data and applications, which carry new technical controls with implications on privacy and security. Providers also rely on client-side, perimeter, and web browser security. It is important to understand all the technologies used by cloud providers for their services. This translates into an expanded attack surface and, consequently, new risks and threats. Just recently new vulnerabilities have been found in virtualization solutions, which gives an idea of the challenges with respect to the underlying architecture used in cloud offerings.
- **Authorization and Authentication**: data protection, federated identity management issues.

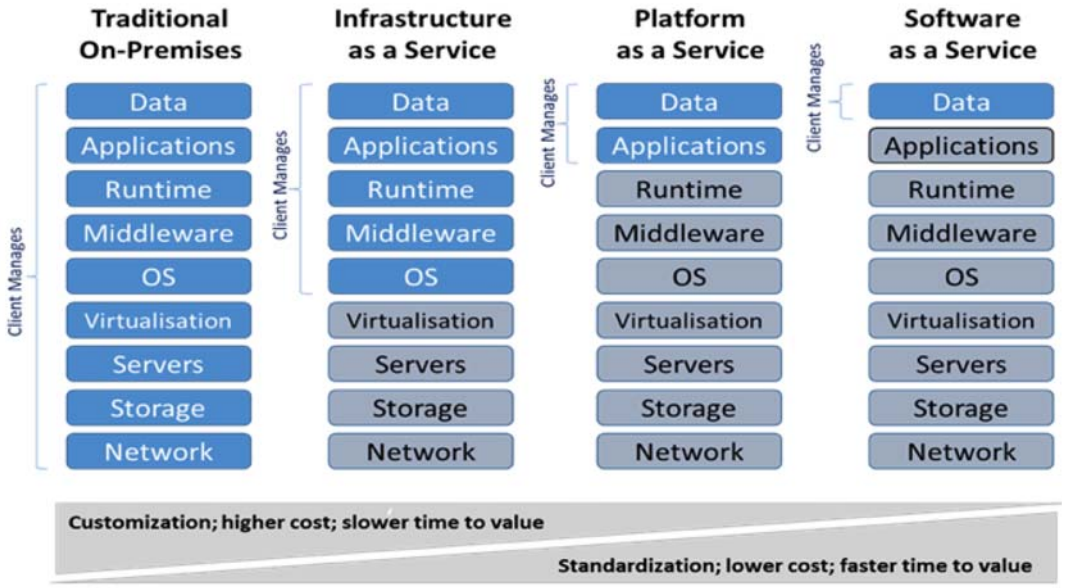
3.2.4 Existing tools

There is an explosion of tools and services for cloud computing security. Many EU projects and private companies are generating tools to secure the cloud. Available tools and services can be found on the link provided for EU projects above: www.cloudwatchhub.eu/Projects as well as through the CSA member companies.

Cloud services are characterized by the layer of abstraction to which they are offered (IaaS, PaaS and SaaS), as shown in the figure below. As shown in the figure, two important enabling technologies for Cloud are virtualization and middleware. Virtualization is now a mature technology in which the combination of HW and SW features are used to virtualize a hardware platform in many isolated virtual machines that can be allocated to each different customer. They will have the guarantee and experience of using a dedicated hardware platform. Formally, virtualization involves the construction of an isomorphism from guest state to host state. Virtualization, over the years became very efficient and flexible offering different approaches and solutions: software virtualization (i.e. VMware), paravirtualization (i.e. Xen), and hypervisors (i.e., Viridian).

Middleware is the technology on which PaaS relies upon. At this level, important technology relates to reliability and scalability as well as sometimes distributed computing. Frameworks such as Hadoop (sometimes combined with MapReduce) address these issues. As part of middleware there are also distributed file systems

that provides high-throughput access to application data and data warehousing that allow the storage of big amounts of data.



In terms of security, most if not all cloud services, no matter at which level, provide basic security mechanisms. In particular, they offer end-to-end secure communication using TLS/SSL and onsite encryption capability to store data in encrypted form. Many also cover authentication of users with a wide range of option going from username and password to more complex identity management and public key certificates using scheme such as OpenID or similar. Furthermore, an increasing number of cloud providers are certified by ISO27001:2013, so they deploy also the basic security mechanisms (i.e., firewall, IDS/IPS, etc.) to secure their data centres.

4 Application Domains

4.1 e-Government

4.1.1 Introduction

e-Government", as defined by the European Commission, is about "using the tools and systems made possible by Information and Communication Technologies (ICT) to provide better public services to citizens and businesses. While e-Government is often thought of as "online government "or "Internet-based government," many non-internet "electronic government" technologies (instant messaging, telephone, tracking systems, smart cards and so on) can be used in this context.

The outcome of e-Government is to transform the entire relationship between the public sector and users of public sector through a creative utilisation of electronic delivery systems, in a way that strengthens a nation and increases the economy immeasurably in a more transparent, cost effective and premeditated way.

The primary delivery models of e-Government can be divided into:

- Government-to-Citizen (G2C), this is the communication link between a government (mainly the public administration) and private individuals or residents.
- Government-to-Business (G2B) is the online non-commercial interaction between local and central government and the commercial business sector.
- Government-to-Government (G2G) is the online non-commercial interaction between different Government organizations, units, departments, and authorities at national, regional and local level among each other , as well as with foreign governments.
- Government-to-Employees (G2E) is the online interactions through instantaneous communication tools between government units and their employees

Attacks to e-Government services are driven by different motivations that include self-benefit, political objectives or even personal recognition. They are carried out by a wide variety of actors or attackers, including cyber criminals, hacktivists, cyber terrorists, state-sponsored spies or disgruntled employees. Attacks to e-Government services can be classified by their operational impact, their nature, and their informational impact. The attack called denial of service, in particular its distributed version, is considered the major attack executed in this sector.

4.1.2 Current Status

IT security is essential to preserve the continuity of e-Government services, but most attacks to services cannot be considered critical despite their severity if we take into account the classic definition of "critical infrastructure". Indeed, only specific services such as emergency response (including medical, police, fire, and rescue), those that ensure the continuity of government (national defence and military operations), and those that support a small fraction of public administration (diplomacy, the armed forces, decision-making) are considered as "critical". This consideration of e-Government services as a "critical infrastructure" only appears explicitly in the US Executive Order 13010. The linkage is not so clear in the European Programme for Critical Infrastructure Protection (EPCIP), which set the overall framework for activities aimed at improving the protection of critical infrastructure in Europe - across all EU States and in all relevant sectors of economic activity.

General factors that have an impact on the vulnerability of any e-Government system are:

- ***Technical and technology factors.*** Any structural weakness caused by critical flaws or errors of technical oversight usually during the design, development, implementation, configuration or maintenance of the system. Also, hardware failures and technological obsolesce are factors to be

considered within this category. Two of the most common web application vulnerabilities are Cross Site Scripting (XSS) and Structured Query Language (SQL) Injection. These simple attacks have been known for several years, but e-Governments are still vulnerable. The vast majority of dynamic e-Government Web applications are vulnerable to XSS or SQL injection. Europe has the highest ratio of countries vulnerable to either XSS or SQL injection. More than 90% of European e-Governments have a vulnerability.

- ***Networking factors.*** The proliferation of ICT has increased the operational dependence on digital systems. In addition, many ICT systems are strongly interconnected and depend on each other. A cyber-attack can thus create a cascading effect, where the disruption of one system is the result of the disruption of another.
- ***Human factors.*** A growing majority of security breaches occurs because of a human error inside an organisation. Accidents or simple unintentional mistakes, such configuration or design mistakes can leave the network ports open so the firewalls become vulnerable, and as a consequence, the systems unprotected.
- ***Economic factors.*** Security technology can be costly, and so is qualified staff to implement, operate and maintain it. Vulnerabilities related to economic factors come from reducing investments on security or the tendency to prefer using an economical solution with short-term benefits.

4.1.3 Research Challenges

The following are the main barriers that currently weaken cyber security in e-Government:

- **Lack of specialists:** Implementing cyber security measures requires skilled manpower. However, most countries face a shortage of skilled people to counter such cyber-attacks, and more so in the case of specialists of cyber security in e-government services.
- **Access to the cybercrime market:** Cybercriminals do not necessarily require considerable technical expertise to act. A marketplace offering cybercrime tools and services provide the would-be criminals with sufficient resources to launch an attack. Most of these services are clearly administrated by cybercriminals. This is called the “Cybercrime-as-a-Service”.
- **Cyber security is a supply-chain problem:** Many agencies and departments are not fully aware of the security control in place within the supply chain, which can be widely outsourced. This also imposes the risk of sharing information with their suppliers. Moreover, there are not well-defined responsibilities for maintaining common situational awareness of emerging critical operational developments.
- **Different levels of national cyber readiness**: There are differences between countries in terms of cyber preparedness. The less sophisticated and widespread a country's connection to the Internet, the lesser the cyber threat. The more services are on line, the higher the risk of cyber-attacks. On the other hand, the countries that are best prepared to react to a cyber-attack are those that are cyber and Internet literate. A McAfee cyber security survey on cyber preparedness, conducted by the Security and Defence Agenda (SDA) organisation and based on leading experts' perception of a nation's defences, concluded that Israel, Finland, and Sweden are leading other countries in “cyber readiness.”
- **Cyber security is a borderless issue**: More global cooperation at legal and technical level is needed to combat cybercrime. However, so far, the discussion on how to set international standards has been very low profile and largely confined to the margins of the UN. Many countries have expressed a concern over new cyber laws, due to disagreements over the national sovereignty matters and concerns for human rights.
- **Tight cyber security regulation may hamper the normal operation of services**: States are not likely to consent to new international rules that restrict the use of cyber weapons.
- **Cooperation is always complex and subject to different stakeholders' interest: nations, corporations, institutions and even individuals**: Cultural differences between countries also play a role when dealing with information-sharing and transparency. Lack of cooperation is one important factor that results in lack of prevention of cyber threats that could have been avoided with closer or smarter cooperation.

4.2 Energy-GRIDS

4.2.1 Energy

4.2.1.1 Introduction

At the moment, grid communication is an inhomogeneous environment. For example, in Germany there are about 900 different system operators and public utility companies. But they use no common protocol for communication. Moreover, the electricity market is equipped with its own private communication network. While other areas have to use facilities of the telecommunications sector, e.g., radio (mobile networks) or landlines, for communication, signals within the electricity market can be transmitted via the high-voltage lines, i.e. by using the powerline-carrier(PLC)-system.

One of the most prominent initiatives for electric utility networks today is the "smart grid". Generally, users within the energy sector use all kinds of telecommunications networks, which enable data transfer to collect data from any kind of sensors, for remote control systems, or for remote administration (e.g. to control smart grids and virtual power plants)[20,21].

4.2.1.2 Current Status

The current situation of cyber security in the energy sector can be described by the following three main points:

- The electric grid is the target of numerous and daily cyber-attacks.
- Most utilities only comply with mandatory cyber security standards and have not or not fully implemented voluntary recommendations.
- Many utilities have not taken concrete steps to reduce the vulnerability of the grid.

Additionally, the PLC systems are often only weakly protected against attacks which try to control this kind of network. This is due to the widespread opinion that these systems are protected by the nature of carrying high-voltage electricity.

Another big topic is the security features of smart meters. These may be deemed inadequate under future cyber security standards, and the earliest smart meters may have been developed without taking into account the NIST Guidelines for Smart Grid Cyber Security[22].

Along with the increase of decentralised and stochastic electrical power injections and more and more extensional trading, this makes the energy system/infrastructure more vulnerable and the risks of outages more likely in the future.

4.2.1.3 Research Challenges

- Critical infrastructures require confronting a number of very basic societal and economic questions about interdependencies of our critical infrastructure, the acceptance of risk and the acceptance of costs to reduce the risks. Additionally, privacy topic in both major types of grid data, the operational data and the electricity consumption data, have to be considered.
- In order to define the threats in a special sector, e.g. the energy sector, the first step is to assess vulnerabilities, possible attack vectors, and the potential impact of attacks. This is a running topic and needs continuous research.
- Further specific security challenges are related to the smart meters which have already been installed[23] and which do not have sufficient security measures.

[20] http://de.wikipedia.org/wiki/Fernwirken
[21] http://en.wikipedia.org/wiki/Smart_grid
[22] http://csrc.nist.gov/publications/PubsNISTIRs.html#NIST-IR-7628
[23] https://www.gov.uk/government/publications/statistical-release-smart-meters-great-britain-quarter-3-2013

4.2.2 Big industrial control systems

4.2.2.1 Introduction

Industrial Control Systems (ICS) are vital for the well-functioning of industrial processes as they monitor and manage these processes. ICSs are typically applied to control critical processes such as the production and distribution of electricity, water treatment and rail electrification. Most ICSs consist of supervisory software installed on (a network of) servers, which acquire real-time data from remote devices that control local operations. These supervisory data generally encompass indicators on product, process and environmental conditions (e.g. meter readings) and are displayed to an operator on (a) central PC(s), often called the control centre. Based on the data retrieved from network devices the control centre sends automated or operator-driven supervisory commands to network devices. These feedback and feed forward loops enable the ICS and operator to supervise the industrial process and to take action when needed.

As regard the security of ICSs, several sources (e.g. RISI, the US ICS-CERT) report a substantial increase in cyber threats in the last decade. From 2006 to 2012, the number of cyber incidents reported to the US ICS-CERT increased with 782%. This proliferation is caused by more companies reporting, but it is also caused by a substantial growth in vulnerabilities and numbers of attacks. According to the RISI, increased use of collaborative networks has made systems more susceptible to attacks. Approximately 65% of the facilities registered in the RISI database allow remote access to their ICSs and around 35% of the ICS security incidents in 2011 were initiated through remote access. In line with this, Bologna et al. (2013:4) found that in 2012 the number of vulnerabilities in SCADA systems detected between 2010 and 2012 was twenty times higher compared to the 2005-2010 period.

4.2.2.2 Current status

To address security issues, companies face several key technical challenges, among which:

- *Improper input validation.* Not all ICS contain code to validate input data. The validation of input data is needed in order to ensure that the content provided to an application does not grant an attacker access to unintended functionality or privilege escalation.
- *Poor code quality*. ICS code review indicate that ICS software has not been designed or implemented using secure software development concepts in general.
- *Insufficient access control*. Many (functions of) ICS make use of password/username combinations for access control or do not require authentication at all.
- *Missing encryption of sensitive data.* The widespread use of unencrypted plain-text network communication protocols.
- *Network security weaknesses.* Many ICS networks are not properly secured, e.g. lack of properly configured firewalls, connections to the ICS LAN which are not routed through the firewall, weak firewall rules and network devices which are not securely configured.

4.2.2.3 Research challenges

Some of these challenges can be addressed by taking the right measures, but some require more in-depth examination. ICS research challenges which have been identified so far in the CAPITAL project include the development of (new) code to increase ICS security, exploration of crypto techniques to ensure network security and methods and tools for security by design. But also challenges related to legal, criminological and social sciences emerged, such as the exploration of legal possibilities for privacy, anonymity and access rights, origin of attacks, attack prevention and detection and drivers and barriers for security solutions development and implementation. Finally, a demand for more interdisciplinary research can be discerned.

4.2.3 Smart GRIDS

4.2.3.1 Introduction

In Europe and elsewhere, the electrical grid is being transitioned into the *smart grid* in order to increase flexibility and accommodate large scale energy production from renewable sources. This transition involves, among other steps, the installation of new, advanced equipment – for example, the replacement of traditional domestic electrical meters with smart meters - and remote communication with devices – for example, allowing remote access to unsupervised energy production sites. Even though the integration of information and communication technologies into the traditional grid improves its adaptivity, such a change may also make the grid vulnerable to cyber attacks.

4.2.3.2 Current Status

The conceptual model proposed by the U.S. National Institute of Standards and Technology (NIST) contains seven different domains:[24] bulk generation, transmission, distribution, operation, market, service provider, and the customer domain. Upgrades and interconnections are envisioned throughout the system, but the development is faster in some domains. For example, the EU mandates that all metering devices in the distribution network should be replaced with smart meters by 2020 to better control and monitor energy consumption.

This rapid change creates security challenges, especially since traditionally these domains have not prioritized security. For one, the deployed resource-constrained devices may not have sufficient resources to run traditional security mechanisms and they interface legacy systems or use protocols never built with security in mind. Many of these devices are also placed in remote locations where the physical security of the devices cannot be ensured, thus putting doubts on the validity of the remote measurements collected, where such values may be an important part when calculating grid stability. Furthermore, the life cycle of components are long from an ICT point of view and it may be impossible to immediately shut down and patch a machine that needs to run 24/7.

Given that traditional ICT environments are faced with security challenges, it is expected that also ICT components in the smart grid are vulnerable to similar attacks (memory corruption, vulnerable protocol stacks, etc.). There are also challenging new problems originating from the intersection between the electrical engineering and ICT domains, for example where a cyber attack (buffer overflow) in turn affects properties of the electrical grid (power quality), which in turn may propagate back to the ICT domain (control loop vulnerability). An interdisciplinary approach is required to identify both challenges and potential threats as well as possible solutions. Given the life time of the systems, it is important to be proactive before deployment.

4.2.3.3 Research Challenges

- **Development of an analysis methodology for resource-constrained devices:** The research community has commenced to investigate how to enable complex dynamic analysis of embedded firmware. Such analysis is the basis for reverse engineering, malware analysis, vulnerability discovery, and vulnerability assessment of the resource-constrained devices deployed in the smart grid.
- **Detection of attacks in a resource-constrained distributed environment**: The placement of intrusion detection systems in the largely distributed grid is challenging. Each resource-constrained device needs to have mechanisms to fend for itself, and collected measurements need to be validated through collection and correlation of a diverse set of data. However, current generation of IDS and firewalls are not adapted to the challenges of this domain so new network services need to be developed.
- **Real-time analysis of large datasets**: To run the grid closer to its operational limit, more data are collected. The validity of the data needs to be confirmed in real time before they are used as a basis for grid operations. Intricate malicious changes could lead to grid instabilities.

[24] http://www.nist.gov/smartgrid/upload/NIST_Framework_Release_2-0_corr.pdf, 2012

4.2.3.4 Existing Tools

The European research community is building test beds and tools suited for analysis of smart grid environments, but more effort is needed. For example, many protocols are proprietary meaning that they cannot properly be analysed by the research community or a third party.

4.3 Smart transport/Automotive

4.3.1 Introduction

What makes transport vulnerable to cyber attacks is the increasing inter-connection and inter-dependence of information systems and networks (e.g. information technology and infrastructure merging), merger of information systems (seen in the deployment of ITS systems, E-enabled transport), increased connectivity and reliance on the Internet, embedded devices, complexity and scale of the transport industry as well as intricate public-private interactions.

The potential for system access resulting from the interoperability of transport systems exposes assets to infiltration and subsequent manipulation of sensitive operations. Assets include **static field devices, dynamic transport management systems, connected vehicles and freight transport management systems**.

4.3.2 Current Status

There are two general methods an attacker can use:

- **Altering data storage** and prevent access to servers: sabotage of the system through physical alteration or destruction of system components, jamming or denial of service type of attack, infection of servers with malwares in order to make the data unusable;
- **Altering exchange of information:**
  - falsification of messages (e.g. key extraction or physically removing a vehicle's credentials and using these credentials to create and distribute seemingly legitimate messages to neighbouring vehicles), selective dissimulation of messages, selective delay of messages, infection of the system with malware, framing attacks (e.g. an attacker makes a vehicle's on-board equipment appear to be malfunctioning by generating false messages to contradict the target vehicle's legitimate messages);
  - software manipulation (e.g. installing malicious software on the vehicle's on-board unit to create messages containing arbitrary or altered information);
  - sensor manipulation (e.g. interfering with the vehicle's sensor output to alter, inject, or suppress messages that originate from internal vehicle systems or interfering with the sensor input that directly reports vehicle behaviour or external circumstances);
  - denial of services (these attacks result in valid messages being suppressed or not received)
  - message linking (e.g an attacker sniffs vehicle to vehicle, attempting to use information found within messages to identify a particular vehicle or a driver's whereabouts.

4.3.3 Research Challenges

The main measures that are in place are the following, although they are not applied uniformly in the transport sector and their quality greatly varies.

- **Authentication and Digital Signatures**
- **Messaging Protocol** (Stability in communication is difficult to achieve due to rapid network changes and since ITS applications are constantly evolving. These protocols are not applied throughout applications and vary in quality);
- **Message Encryption**

- **Information Privacy** (transport information must be treated as privacy information. This is important to ensure that this information is not breached through any unauthorized access);
- **Non-repudiation** (capability to identify the attackers even after the attack happens which are important to prosecute attackers and to prevent them from denying their crimes by storing all related information in the device which should be made as compulsory for all transport users).
- **Secure Routing** (to secure ad hoc routing protocols, a proactive approach is starting to enhance the existing ad hoc routing protocols. Securing ad hoc routing also means restricting ad hoc nature of networking which are known to be open for all network protocol).

4.5 Banking and finance

4.5.1 Financial Services

4.5.1.1 Introduction

The term "Financial Services" can refer to a broad spectrum of organisations and services operating in different areas, and each of these could warrant its own detailed section. Focus here is on the retail banking services and related infrastructures, with some overlaps in other areas of financial services. The EU financial services market can be described as having a 'bank-based' model, where the majority of enterprises are financed by banks, as opposed to capital markets, for example. Indicative of this is the fact that the share of banks in credit intermediation in Europe represents around 70%-75% of debt financing to households and enterprises. In the US, this number is around 20%-30%. The European financial services sector, specifically the banking sector, is the largest in the world.

4.5.1.2 Current Status

The specific trends within the financial services shaping the landscape for the future of the industry include Single Euro Payments AREA (SEPA) Regulation No 260/2012 which will make all electronic payments across the euro area as easy as domestic payments within one country, new entrants to the market which are retail merchants and telecom providers leveraging on customer trust and enable weak barriers of entry, digital and mobile banking that will have to adopt mobility solutions, mobile payments, influence from online retail sector, adoption of cloud computing and the bring your own device culture (BYOD). Common types of threats within the financial services sector include threats to online banking, threat to payment processors, threat to financial markets and securities. The main tools and techniques used by threat actors to creat cyber disruption include installed malware, social engineering, targeted attacks, Advanced Persistent Threat (APT), Denial of Service Attack (DoS) and Distributed-denial-of-service Attack (DDoS).

4.5.1.3 Research challenges

Some of the research opportunities in the financial services sector could include evaluation of existing cyber security solutions in order to help mitigate the impact of cyber threat, developing standards for threat and incident information sharing practices, European cyber security incident management practices, and identifying and promoting awareness of the emerging threats.

4.5.1.4 Existing tools

Security of financial services operations relies on both robust technical and non-technical controls. The non-technical controls range from effective governance, employee and user training and awareness, disaster recovery and business continuity planning and deployment of Security Operations Centres (SOCs). Furthermore, appropriate technical measures are implemented. Network security in financial services refers to the provisions and policies adopted by a financial institute to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources. Most commonly and widely adopted practices within the financial services include: Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), design and implementation of Secure Applications, Strong authentication for online transactions (e.g. chipTAN authentication), inbound email sandboxing (used to combat phishing by deploying a solution that

checks the safety of an email link when a user clicks on it and go some way to mitigating the risk of phishing) and real-time analysis and inspection of web traffic.

4.5.2 Mobile payments

4.5.2.1 Introduction

The way we pay for our daily goods and services is changing at a never high pace. In the past an Embedded Secure Element (eSE) was required to perform a payment. The market is now migrating to apps without hardware support that run on our mobile phones. As a result instead of paying with cash, cheque, or credit cards, a consumer can now use a mobile phone to pay for services, digital goods and hard goods. The migration from *classical* payment methods to mobile payments has started a few years ago yet recently from October 2013 this has taken a significant acceleration.

4.5.2.2 Current status

In October 2013 Google introduced Android 4.4, more commonly known as Kit Kat, which includes a NFC feature known as Host Card Emulation (HCE). Since its introduction HCE has drawn much interest in both the NFC and mobile payment industry as it opens up the possibility to perform NFC based card emulation without the need of an Embedded Secure Element (eSE) being present in the handset. The advantages of a software based solution like HCE are obvious where ease of deployment and full-control over the previsioning are the most interesting. Recently the interest of the industry has increased further due to the introduction of the first large-scale software payment application deployment in the form of the new HCE based implementation of the Google Wallet.

Currently the majority of financial institutions, governments and commercial companies are developing HCE based payment applications or are investigating this. Due to these developments HCE is considered the most likely candidate for the standard in mobile NFC based payments.

Certainly HCE is an important development and it has the potential to speed-up the deployment of mobile payment solution and the adoption of NFC in mobile devices. However it is that the deployment of new technologies goes also along with new processes and infrastructures. It is these potentially introduce new security vulnerabilities that could allow an adversary to steal and misuse payment data.

A major level of security in software based payment solutions depends on to the operating systems ability to ensure the confidentiality and integrity of credentials on the mobile device. In the case of HCE the Android OS itself is not a proven secure location to store this information yet the risk of misuse can potentially be reduced by introducing countermeasures such as devaluating (credentials are only valid for a single transaction), risk assessment and location of a consumer.

Any form of devaluating has a direct impact on the freedom and usability for the consumer. Also in software based solutions off-line payments are either not supported or only in very limited form (such as a maximum number of payments or a fairly low amount).

4.5.2.3 Research Challenges

Mobile payment solutions are still at a fairly early stage of development and deployment. Although there is awareness that purely software solutions have a less strong security model these are currently handled by infra-structural countermeasures (typically cloud based). Although the trend currently is to move away from hardware support for mobile payment the following is yet to be investigated further:

- As there are currently no large scale deployments of mobile payments apps that come close to the scale at which conventional payment solutions are currently deployed. Are infra-structural countermeasures without hardware support on the hand-set sufficient to withstand all attack scenarios in the present and future?
- The provisioning of mobile devices (at least for part of the users) will partially rely on the reliability of the MNO's. Is there a need for an ensured level of security in their network is when this is used for payment solutions?

- Current mobile platforms where originally not designed for (purely software) payment applications
- Various specifications for software based payments are currently being released (for example Visa and EMV) yet there is still much unknown. Who will setup a standard for everyone to use or will the market be flooded with proprietary solutions?
- Can the security drawbacks of pure software based solutions be strengthened by (partial) hardware support?

4.6 Smart cities

4.6.1 Introduction

The world's major cities are facing a number of significant challenges that arise from the trend for greater urbanisation, the pressure for sustainable use of energy and resources and the greater connectivity of the citizen with the physical infrastructure and/or assets. It has been suggested that a city can be regarded as 'smart' when investments in human and social capital, the traditional city infrastructure and information and communications (ICT) technologies create sustainable economic development, a high quality of life and wise management of natural resources through participatory action and engagement[25].

4.6.2 Current Status

A vision that is typically painted of a smart city is one that involves greater integration of the physical infrastructure with the use of knowledge, information and communications technologies and social infrastructure to deliver urban competitiveness. The smart elements may be considered in terms of the citizen, city operations and city infrastructure. The citizen elements focus on education, health care, social programmes and the availability of information to aid personal decision making, e.g. availability of transport. The city operations element relates to local government planning and management of their public services and use of information to achieve smarter buildings and urban planning. The infrastructure element relates to the utilities (energy and water), urban transport systems, and environmental aspects, including handling of waste, pollution, etc.

Given the complex legacy environments of established cities in the developed world there are considerable barriers to delivering smart cities. Where development is occurring is through piecemeal investment, e.g. the European implementation by 2020 of universal domestic smart metering will provide information about energy consumption, but there has to date been limited investment in the tools and techniques to allow citizens to actively manage their energy demand.

A number of 'smart' cities concepts are based on the use of sensor networks, including widespread use of wireless sensors, to enable real-time measurement and management. There have been trials of some of these technologies, but little is known about the resilience or accuracy of these sensor networks and what steps would be required to ensure they are sufficiently robust and adaptable to become part of a long-term city management solution.

4.6.3 Research Challenges

- **Managing the personal right to privacy in the smart city large dataset:** The collection, storage and use of large datasets in a future smart city will have significant implications for the privacy of individuals. Already significant volumes of data are collected by services providers, e.g. transport operators, mobile phone companies, etc. Smart cities are likely to require sharing of some of this data and its integration with data from other city resources and sensor networks. The challenge is to understand how this data can be safely collected, stored, processed and used without citizens felling constantly under surveillance and without their privacy being compromised.

[25] Caragliu, A; Del Bo, C. & Nijkamp, P (2009). "Smart cities in Europe". Serie Research Memoranda 0048 (VU University Amsterdam, Faculty of Economics, Business Administration and Econometrics).

- **Developing analysis methodologies for complex city-wide systems-of-systems:** The concept of a smart city is predicated on the greater interaction and integration of city-wide systems. This interaction of systems has significant implications from a resilience perspective, where the failure or impaired performance of one system could disrupt or severely degrade the operation of the city. Existing methodologies focus on single standalone systems, whereas the capability is needed to investigate and model complex system-of-systems behaviour, where the city is effectively an integrated platform.
- **Managing cyber security and resilience in complex systems:** Traditional information security techniques focus on establishing boundaries around an information system and then controlling security within the boundary. These techniques do not readily scale to handle complex system-of-systems situations, where the security protocols and architectures of individual systems may undermine the security of the whole. The protection of data, information and control systems at a city-wide level needs to be considered and techniques developed to allow this to be modelled and assessed. Work is also required to understand and model the complex information flows that will occur within a smart city so that the consequences of failures, interference or lack of capacity can be understood.

4.6.4 Existing Tools

A number of major cities are experimenting with smart systems, but these are at best embryonic smart cities and have not addressed the research challenges identified above.

4.7 Telecommunications/ICT services

4.7.1 Mobile

4.7.1.1 Introduction

The most important kinds of applications used on mobile devices are social networking tools, communication apps, entertainment, travel information and location based services, and education. Connecting with other people and context dependent information even change the way our society goes.

The telecommunication ecosystem driving mobile computing consists of three layers: 1) the (hardware) communication infrastructure (devices, stations, cables, etc.), network services (GPRS, EDGE, UMTS, LTE, VoIP, etc.), and communication applications (E-mail, VPN, HTTP, etc.). The communication infrastructure layer enables the effective and efficient generation, transmission and delivery of data by hardware, people and processes; 2) Services and applications layer that require standardized protocols. It covers different ISO/OSI-layers. GSM/GPRS (2nd generation) is the world's most ubiquitous wireless data service. Its architecture also supports EDGE and UMTS networks with a limited amount of hardware upgrades. The bandwidth of UMTS (3rd generation) and LTE (4th generation) is large enough to allow all multimedia applications known from stationary systems, and; 3) application level - Virtual private networks (VPN) extend private, physical networks to the mobile world. It uses secure end-to-end cryptographic protocols to secure private data communication over public networks. VPN protocols include IPsec, SSL/TLS and PPTP. Firewalls and virus scanners are also available for smartphones and tablets.

4.7.1.2 Current status

There are seven major trends for emerging mobile computing technologies: Usage of WiFi instead of cellular networks, mobile augmented reality, open source and customizable cell phones, mobile payment and near field communication (NFC), tactile feedback, cloud integration, body area networks (BAN). On the software side, two trends accompany mobile computing: The development of platform-independent web applications and the increasing importance of closed-shop, platform specific applications, distributed by monopolized app stores. Both ways of software distribution and engineering attract small and innovative developers. From a security perspective, app stores constitute a single gateway, where applications can be checked for vulnerabilities and malware. Most mobile computing architectures provide a sandbox environment for the applications Thereby, a single misbehaving software component can, in general, not affect other components and the overall system.

4.7.1.3 Research challenges

Some research challenges identified in the area include surveillance by ubiquitous audio and video sensors, person tracking, mobile malware, lost and stolen mobile devices, insecure communication, jailbreaking, usage of 3rd party app stores, bring your own device (BYOD), vulnerable development frameworks, misperception of the security of mobile devices, availability of information, increased interoperability and social coherence.

4.7.1.4 Existing Tools

The ***end-to-end encryption*** of mobile communication is supported by apps like Private Phone (which will be integrated in PrivateOS of Blackphone) and Threema, as well as by special smartphones like the SiMKo 3. The apps can already be bought, but lack the market penetration necessary for daily use.

Apps like TaintDroid and UC4Android [Feth2012] allow ***real time privacy monitoring*** on smartphones. They support to taint sensitive data and to watch which applications share this data with other applications or via the network. It is also possible to taint data from specific sources (camera, GPS sensor, microphone, etc.) automatically, giving an overview where such data flowed to. This technology is still under development and is not fully integrated into operating systems.

Sandboxes and smartphone virtualization (Blackberry Balance, Samsung Knox, Bizztrust) makes it possible to ***separate corporate data from private applications***. Either by running multiple operating systems on a single device or by providing separate, integrity checked containers for each data type. This technology can already be bought on the market and is in an advanced state, but is not rolled out to many customers.

HTML5 is fully developed and is gaining market penetration since the rollout of Firefox OS. HTML5 based applications benefit from openness and cross-system compatibility. But it cannot be anticipated, if HTML5 will be commonly used for all mobile computing environments.

The ***UMTS*** mobile cellular system is widely adapted all over Europe. The technology is state-of-the-art and one can no longer think of a smartphone without it. The fourth generation ***LTE*** standard slowly gains market share, but is not implemented in all smartphones yet. Its spatial coverage is still well below that of UMTS.

(Smart) Sensors and signalling components like cameras, microphones, NFC and RFID tags, Bluetooth, Wifi, gyroscopes, and GPS are implemented in many mobile devices. As they are so various, it is hard to define an overall level of maturity. But it can be said that they are already well adapted by the mobile computing domain.

Privacy patterns, as mentioned on http://privacypatterns.org/, are not fully collected or systematically applied to mobile computing. There are ad hoc solutions, which may result in common patterns across systems, but they are not well defined yet. The closest to privacy patterns are the OWASP Top 10 mobile controls and design principles.

4.7.2 Social media/networks

4.7.2.1 Introduction

Over the past few years we have seen the impressive rise of one-line social networks. Moving our social interactions to the digital age, on-line social networks enable people to interact with their friends, relatives, and colleagues. On-line social networks have been a blessing to several people: long-lost friends were re-united, relatives living apart were able to keep up with their families, groups were able to organize and disseminate information timely and effectively. At the same time, however, people have started to share a disproportionately large portion of their lives: the songs they listen to, the videos they see, the places they go, pretty much most of their lives.

4.7.2.2 Current status

As we move our social interactions on-line several new kinds of threats have started to emerge:

- **Social engineering**: People tend to trust their friends and acquaintances in real life. A recommendation or a piece of advice coming from a friend has a certain weight to it. Similarly, a recommendation

coming from a friend in a social network has a similar weight. Compromised user accounts may easily be used to social engineer people in a social network.

- **From private space to public domain**: users of on-line social networks have repeatedly discovered that data they tend to consider private may be available to third parties. Indeed, relaxed privacy settings, compromised "friend" accounts, or just careless friends may easily leak private data all the way to the public domain.
- **Third party applications**: To enhance the experience of their users, social networks frequently enable third party applications to operate on top of them. Although they use a predefined API and need to have explicit user permission, third party applications may ask permission to access more data than they need. Interestingly, if they are not given permission for everything they ask for, they just refuse to operate.
- **User tracking**: To enhance the browsing experience of their users, social media collaborate with third party web sites to provide a personalized version differently tailored to each individual user. Such personalization services include the display of comments made by friends, a list of friends who have "liked" a visited site, etc. Although personalization can be a very positive experience, it is currently implemented based on heavy ser tracking: to personalize a web site for a given user, the social network requests to know that the user visited the web site. As a result, social networks get to know the web browsing patterns of their users.

4.7.2.3 Research Challenges

The threats associated with social networks are still being mapped out. To make matters worse, the continually evolving nature of social networks makes a complete mapping of the treats a moving target. In this fluent and rapidly evolving world some research challenges include:

- **Lack of research data:** Most popular social networks belong to corporations that are very reluctant to share their data – even with Universities. To make matters worse, most of them do not allow the crawling of their web sites, not even for their publicly available data. Thus, without any data it is difficult, if not impossible, to make any meaningful research in the area.
- **Tracking of information:** It is not clear how social networks and their associated third-party applications propagate user information. If user information is eventually found leaked, it is not clear who leaked it and how. Developing mechanisms, such as honeypots, to track information propagation is a challenging research topic.
- **Compromised account identification:** We need to find ways to identify compromised (or fake) accounts. Such accounts can be used to leak private information, propagate false advice, and even impose financial loss to the victims.
- **Give users back the control of their data**: Enable users to (i) know which data they have shared within the social network, (ii) track the movement of these data within the social network, (iii) prohibit the movement of the data beyond certain domain, and (iv) completely erase the data from the social network and its broader ecosystem.

4.9 Food

4.9.1 Introduction

Food production and distribution industries are heavily dependent on the use technology, particularly in the control of complex cyber-physical systems. Areas of intensive ICT use include the management of logistics in the supply chain, control of production processes and the control and management of food storage, e.g. frozen and chilled environments.

4.9.2 Current Status

Food production operates on an industrial scale, with supply chains spanning continents and specialist suppliers performing specific roles in the delivery of the food from farm to the consumer's plate. Recent food quality and contamination fears in the European Union (EU) have illustrated how the raw materials and ingredients for processed foods can be shipped from country-to-country during the production process. This has led to increasing concerns about traceability of foodstuffs and requirements for improvements in record-keeping.

These records are typically reliant on complex information technology systems. For example, in Norway, RFID tags are used to track shipments of North Sea cod from trawlers through the supply chain to food processors and bulk caterers.

High-volume food processing and production is largely carried out in large industrial premises with automated systems under the control of industrial control systems. Such systems are vulnerable to cyber security threats, including hacking, malware and the lack of trustworthy control software. The vulnerability of the system will significantly increase where Internet connectivity is provided or utilised in order to manage the production and supply chains.

4.9.3 Research Challenges

Managing trust in a food global supply chain

The consumer and regulatory requirements for greater traceability of raw materials in the food supply chain can only be reliably achieved the data collected by the supply chain is trustworthy. As the supply chains often span multiple jurisdictions there may be significant issues regarding the degree to which the collected data can be relied upon. The business processes and local legal and ethical practices may have further bearing on the trustworthiness of data collected by technical means. Further research into these areas could include the definition of appropriate trust models that can be implemented in order to support these complex supply chains.

4.10 Drinking water and water treatment systems

4.10.1 Introduction

Due to changes in weather patterns, increasing populations and rising demand for water in cities, the global availability of clean drinking water is likely to be a cause of international friction and conflict in the future. The issue of water shortages may become particularly acute in cities with large legacy infrastructures, especially where there is a significant volume of leakage between water treatment and its delivery to the consumer. There will also be issues regarding water management in areas prone to flooding, where there may be a greater need for proactive management of reservoirs, rivers and other watercourses.

4.10.2 Current Status

Changes in rainfall patterns, demand and abstraction of water for human consumption, agriculture and industrial use all have an impact on rivers and aquifers. Water management and treatment is a complex process, managed using sensors and distributed industrial control systems. To manage supplies to large urban areas, there is a need to accurately monitor available supplies and balance the abstraction of ground water or use of alternative sources. The control systems employed by water treatment organisations are vulnerable to cyber-attacks and interferences.

In addition to the supply of treated water, there are potential issues regarding the handling, treatment and discharge of waste water, e.g. sewerage, water from industrial processes, etc. This water needs to be treated prior to discharge into watercourses, lakes or the sea. The treatment processes are again managed by industrial control systems and, as demonstrated by the Maroochy incident in Australia, vulnerable to interferences and cyber-attacks.

Allied to the treatment of drinking water and waste water is the management and control of water in rivers and other watercourses. With rising sea levels and changes in rainfall frequency and volumes there is a need to manage flows to prevent or minimise flooding of developed areas. This is typically handled through the control via industrial control systems of pumps, sluices, tidal barriers and other water management systems. Information on water levels, flow rates, tides and precipitation is collected and analysed by sensor networks and communicated to central control rooms.

4.10.3 Research Challenges

Managing the cyber security and resilience of distributed industrial control systems

Water treatment and flood management systems are controlled by a variety of industrial control systems, some standalone and others integrated in SCADA systems. Work has been done in the United States on the development of a "Water Security Roadmap to Secure Control Systems in the Water Sector". Similar work is required in Europe to consider water security and management at regional, national and international levels.

4.11 Agriculture

4.11.1 Introduction

There is an increasing use of information and communications technologies in agriculture in all phases of the agricultural production process. The concept of e-Agriculture was one of the action items emerging from the World Summit on the information Society (WSIS). In 2005, the "Tunis Agenda for the Information Society" [https://www.itu.int/wsis/docs2/tunis/off/6rev1.html] was published, with the actions agriculture being assigned to the UN Food and Agriculture Organisation (FAO).

4.11.2 Current Status

Agricultural businesses are increasingly dependent on the Internet and ICT for access to information and to managed business operations. Initially, this was to replace or automate manual tasks such as the completion on stock records or submission of returns to government authorities. With the need to increase production to keep up with rising demand from expanding populations, there has been need to improve productivity and yields, whilst maintaining a competitive cost base.

This has led to greater use of geo-positioning systems (GPS), geographic information systems (GIS), automation, radio frequency identification (RFID) and knowledge management systems. For example, the use of GPS, GIS and automation on tractors to optimise the delivery of insecticides, weed-killers or fertilizer onto crops. In the UK there has been an extensive use of GPS and GIS in order to manage applications and payments from Rural Payments Agency for Common Agricultural Policy schemes. Farmers are also using RFID tags for the management and tracing of livestock.

The global nature of agricultural and supply chains as discussed in section 4.9 has implications for farmers. For example, the need to harvest and ship fresh produce on a just-in-time to fulfil orders requires farmers to have reliable and resilient ICT infrastructures. This may be difficult to achieve in some rural areas.

4.11.3 Research Challenges

The main challenges are likely to be those related to the food industry (see section 4.9) and to the security of industrial control systems (see section 4.2.2).

4.12 Cyber security awareness and training

4.12.1 Introduction

Cybersecurity training comprises the technologies and pedagogical aspects that facilitate the acquisition and perfection of knowledge, skills and aptitudes needed to effectively take on professional activities in the cybersecurity domain. On the other hand, cybersecurity awareness typically aims at raising consciousness of a certain situation or problem, and related to the way a person, an organisation or a nation deals with it.

4.12.2 Current status

There are two approaches for cybersecurity training:

- Simulators, software/hardware tools that model the state and internal properties of the simulated system, being able to produce identical (ideal simulator) observable effects and properties like those of the real system (performance, interactivity, etc.), that is, emulating the behavior of the real system.
- Emulators, software/hardware tools that seek to mimic the observable properties (not the internal state) of the emulated system, in a manner that the behavior is as close to the reality as possible.

In practical terms, emulators are typically used as substitutive elements of the real system, whilst simulators are mainly used for analysis, experimentation and training.

Simulators, in turn, can be classified according to LVC (Live-Virtual-Constructive) approach. Next Figure depicts the LVC classification for simulators based on the different dimensions: personnel, systems, commands and environment.

	COMBAT	LIVE	VIRTUAL	CONSTRUCTIVE
Personnel	**Real**	**Real**	**Real**	**Simulated**
Systems	**Real**	**Real**	**Simulated**	**Simulated**
Commands	**Real**	**Simulated**	**Simulated**	**Simulated**
Environment	**Real**	**Real**	**Simulated**	**Simulated**

As for cybersecurity awareness, cyberdefence exercises (CDX) are one of the most relevant initiatives. In CDX, different stakeholders collaborate or compete in a simulated scenario, typically using virtualized systems and remote communications, with the aim to test and observe at first hand some problems or situations in the cyber domain.

4.12.3 Research challenges

Current solutions have limitations that leave the next challenges unanswered:

- Student monitoring and real-time performance assessment, being able to dynamically adapt the difficulty of the exercise as well as provide automated support and guidance.
- Exercise monitoring and evaluation of its state, being able to control the progress of the exercise, detect inconsistencies and hard-to-solve situations, etc.
- Definition and creation of new scenarios and cyber threats in a cost and time-effective manner, and that better achieve the pedagogical objectives for a wide variety of student profiles.
- Cyber attacks tools capable of adapting complexity to student skills without compromising flexibility.

Index