



Funded by the European Commission

Seventh Framework Programme



CyberROAD

Development of the Cybercrime and Cyber-terrorism Research Roadmap

Grant Agreement N. **607642**

D4.1 - Technology Landscape Report

Date of deliverable: 31/05/2015

Actual submission date: 31/05/2015

Start date of the Project: 1st June 2014. Duration: 24 months

Coordinator: UNICA – University of Cagliari, PRA Lab - Pattern Recognition and Applications Lab

Version: 1.0

Project funded by the European Commission Directorate-General Home Affairs in the Prevention of and Fight against Crime Programme		
Restriction Level		
PU	Public	✓
PP	Restricted to other programme participants (including the Commission services)	no
RE	Restricted to a group specified by the consortium (including the Commission services)	no
CO	Confidential, only for members of the consortium (including the Commission)	no



D4.1 - Technology Landscape Report

Funded by the European Commission under the Seventh Framework Programme

Page 1 of 76

Revision history

Version	Object	Date	Author(s)
0.1	Creation	17/11/14	Carpine Francesco, Guardi Giovanni
0.2	Revision	24/11/2014	Valentini Alessia
0.3	Modification	25/11/14 to 25/03/2015	Carpine Francesco, Guardi Giovanni
0.4	Revision	25/03/2014	Valentini Alessia
0.5	Revision and modification	28/04/2014	Valentini Alessia and all partners
0.6	Revision and modification	5/05/2015	All Partners
0.7	Bibliography correction	10/05/2015	Valentini Alessia
0.8	Styles and summary correction	15/05/2015	Giovanni Guardì
0.9	Semi-Final draft	15/05/2015	Valentini Alessia , Giovanni Guardì
1.0	Final document	31/05/2015	Javier Martínez-Torres, and All Partners.





D4.1 Technology Landscape Report

Responsible

VITROCISET

Contributor(s)

TUD
INDRA
POSTEIT
SM
FORTH-ICS
NCSRD
SBA
CEFRIEL
RHUL

Summary:

This deliverable outlines the current technological context in which modern cyber-attacks take place. Today cyber attackers make use of the potential offered by modern technologies to increase the effects of their attacks, both when conducted by cybercriminals and cyberterrorists. This document describes a high level technology landscape, with focuses on recent and emerging technologies, and current and future ICT trends and paradigms.

Keywords: cybercrime, cyberterrorism, security, privacy, technology

TABLE OF CONTENTS

1	INTRODUCTION	8
1.1	ORGANISATION OF THE DOCUMENT.....	9
2	PARADIGMS.....	10
2.1	BIG DATA	10
2.2	ADVANCED, PERVASIVE AND INVISIBLE ANALYTICS	12
2.2.1	The opportunities.....	13
2.2.2	The issues	13
2.3	CYBER SECURITY AND PRIVACY ENGINEERING.....	13
2.3.1	Everything as a Service	14
2.3.2	Digital Rights Management	14
2.3.3	Encryption By Default	14
2.4	RISK-BASED SECURITY AND SELF-PROTECTION	15
2.4.1	Dynamic Risk Management	15
2.5	OPEN SOFTWARE	17
2.6	OPEN HARDWARE	17
2.7	FUTURE SECURITY AND PRIVACY INCIDENT MANAGEMENT.....	18
2.7.1	Security Information and Event Management	18
2.7.2	Security Incident Response.....	19
2.8	PARADIGM SHIFT IN INDUSTRIAL CONTROL SYSTEMS	19
2.8.1	Paradigm Shift in SCADA Systems	19
2.8.2	Paradigm Shift in Resilient Control Systems (RCS)	20
2.9	INTRUSION MANAGEMENT SYSTEMS.....	20
2.9.1	Intrusion Detection Systems	20
2.9.2	Intrusion Prevention Systems	21
2.10	UBIQUITOUS / NOMADIC COMPUTING	22
2.10.1	Ubiquitous Computing	22
2.10.2	Nomadic Computing.....	22
2.11	CONTACTLESS TRANSACTION	23
2.11.1	Near Field Communication for Contactless Transactions.....	23
2.11.2	NFC Technology Overview	23
2.12	TRUST AND IDENTITY	25
2.12.1	One Time Password (OTP).....	25
2.12.2	Personal Card Reader	25
2.12.3	“On-card” challenge-response devices	26
2.12.4	One-Time Password via SMS.....	26
2.12.5	Certificate-based authentication.....	26
2.12.6	Mobile One-time Password (OTP).....	27
2.12.7	Mobile Transaction Data Signing	27
2.12.8	Voice recognition	28
2.12.9	Face recognition.....	28
2.12.10	Iris Recognition.....	29



2.12.11	Fingerprint recognition.....	29
2.12.12	Pattern based recognition.....	30
2.12.13	Image Based authentication.....	30
2.12.14	Comparative Analysis.....	31
3	TRENDS.....	32
3.1	SMART CITIES.....	32
3.1.1	Smart Cities State Of The Art.....	32
3.1.2	Cybersecurity And Its Role On Smart Cities.....	33
3.1.3	Concluding Remarks.....	34
3.2	INTERNET OF THINGS/QUANTIFIED SELF.....	35
3.2.1	Quantified Self.....	35
3.3	MOBILE BIOMETRY.....	38
3.4	UNMANNED SYSTEMS.....	42
3.5	SMART TRANSPORT (AUTOMOTIVE).....	45
3.6	LOCATION BASED SERVICES.....	48
3.7	SOCIAL NETWORKS.....	50
3.7.1	Impacts And State Of The Art.....	50
3.7.2	Cyber Security Risks Associated With Social Networks.....	51
3.7.3	Conclusions.....	52
3.8	BYOD.....	52
3.8.1	BYOD State Of The Art.....	52
3.8.2	BYOD And Cybersecurity Issues And Challenges.....	53
3.8.3	Conclusions.....	54
3.9	VIRTUALIZATION.....	54
3.9.1	Impacts And State Of The Art.....	54
3.9.2	Cyber Security Risks Associated With Virtualization.....	55
3.9.3	Conclusions.....	55
3.10	CLOUD COMPUTING.....	55
3.10.1	Adaption To The New Paradigm.....	56
3.10.2	Cybersecurity And Its Role On Cloud Computing.....	56
3.10.3	Conclusions.....	57
3.11	AUTO TAGGING.....	57
3.11.1	State Of The Art.....	58
3.11.2	Cyber Security Risks Associated With Auto-Tagging.....	59
3.11.3	Conclusions.....	59
3.12	SMART GRIDS.....	60
4	APPENDIX A: HIGH LEVEL SCENARIOS.....	62
4.1	SMART CITIES.....	62
4.2	INTERNET OF THINGS/QUANTIFIED SELF.....	62
4.3	MOBILE BIOMETRY.....	63
4.4	UNMANNED SYSTEMS.....	63
4.5	SMART TRANSPORT (AUTOMOTIVE).....	64
4.6	LOCATION BASED SERVICES.....	64
4.7	SOCIAL NETWORKS.....	65



4.8	<i>BYOD</i>	65
4.9	<i>VIRTUALIZATION</i>	66
4.10	<i>CLOUD COMPUTING</i>	66
4.11	<i>AUTO TAGGING</i>	67
4.12	<i>SMART GRIDS</i>	67
5	CONCLUSIONS	68
6	BIBLIOGRAPHY AND REFERENCES	70
6.1	REFERENCES	70
6.2	BIBLIOGRAPHY	75



The main objective of this deliverable is to describe current and emerging technologies, trends, and paradigms suitable to be considered as a general scenario background, where subsequent CyberROAD's tasks and deliverables can build upon. In fact, such trends and paradigms can be thought of as a starting point to be further enhanced to identify domain-specific scenarios and views, including those particularly focused on cybercrime and cyberterrorism.

In CyberROAD, a scenario, which draws on the definition given in “Tutorial on Scenario Analysis & Roadmapping”, is:

“a concise and schematic representation of a state (actual or future), aimed at identifying threats and defenses.”

Similarly, a view is defined as:


“[...] elements of a scenario concerning only a given subject, e.g., workforces, private transports. For the sake of brevity, the term VIEW will also be used, with a different meaning with respect to its use in relational data bases”.

This deliverable is the result of task T4.1. As per DoW, it requires the following technologies to be analyzed:

1. “New or recent paradigms such as the Internet of Things (IoT), the Web 2.0 or ubiquitous computing, and relevant services associated to them, like Location-based Services (LBS), auto-tagging, social networks, user-centric technologies, etc.;
2. Specific platforms for end users, like smart phones and other mobile devices, and desktop platforms;
3. Platforms and technologies specifically focused on industrial control systems, such as SCADA systems and industrial software;
4. Other models and trends not specifically bound to end users or industrial control systems, like virtualization and cloud computing and the associated paradigms (IaaS, SaaS, etc.)”

As per details outlined in the DoW, the deliverable covers trends, paradigms, and emerging technologies as well as traditional and out-dated ones: from desktop environments to the new generation of smartphone, and from management software to real-time embedded software [1], just to name a few . Out-dated technologies cannot be completely dismissed because they are either still used in legacy datacenters, or provide basic infrastructure on which innovative services to citizens and customers are being implemented, nowadays. Not only this increases the management costs of such technology (especially for no longer supported software and systems), but it also leaves security loopholes that can be easily exploited by attackers. Being stuck with legacy technology is however a complex topic that usually stems from the lack of funding for a continuous technological renovation (e.g., local government), adversity against cultural changes, or the need to operate costly and slow-paced (from a technology perspective) hardware.

The DoW requirements for the deliverable D4.1 is entirely reported herein below:

	D4.1 - Technology Landscape Report
	Funded by the European Commission under the Seventh Framework Programme
	Page 8 of 76

“This report will comprise an analysis of the current and emerging technological trends and paradigms, including the IoT, social networks, user-centric technologies, BYOD, ICS/SCADA systems and more. The report will also include an appendix with a series of high-level scenarios that represent an abstract architectural view of those trends.”

To ease the understanding, the technologies have been divided in main and general categories, each of which has been divided in subtopics to represent the most suitable granularity related with current and emerging threats, attacks, techniques, and defence countermeasures that will result from other deliverables and will be mapped on this technological landscape. In the following, each single technology topic has been described giving a formal definition, including an explanation—where applicable—on the implementation characteristics or the constituent technological basic elements.

To achieve the DoW requirements, an appendix is dedicated to a collection of (specify correct number) scenarios, which are described in detail and supported by a high-level architectural view. These scenarios will be useful for further in-depth cybersecurity-related analyses, such as attacks, countermeasures, and type of attackers in a general threat-centric approach that represent the “leitmotiv” of all the CyberROAD project.

All the technologies outlined in the deliverable can be considered as potential targets towards which current or emerging offensive action can be directed. In fact, the “threat-catalogue” for CyberCrime and CyberTerrorism will build on the outcome of this deliverable.

1.1 ORGANISATION OF THE DOCUMENT

The document is organised as follows:

- Section 1. INTRODUCTION includes an overview of the work conducted by the consortium, and the organisation of the document.
- Section 2. PARADIGMS contains the context of current technological paradigms, with an explanation to describe the landscaping.
- Sections 3. TRENDS covers the description of relevant trends that nowadays or in future will affect the lifestyle of citizens.
- Section 5. APENDIX A: HIGH LEVEL SCENARIOS provides a graphical representation for each identified Trend. The diagrams are easy to understand for non-technical experts and they include involved agents, hardware elements, communications means and a characterization of the scenario.
- Section 6. Contains the REFERENCES and BIBLIOGRAPHY used to elaborate the deliverable.



As described in [Dosi, 1982], “[...] we shall define a ‘technological paradigm’ as a set of procedures, a definition of the ‘relevant’ problems and of the specific knowledge related to their solution.”. Therefore, when we talk about a technological paradigm, we are referring to the sets of new technological innovations that extend their influence to the whole economic system and have strong repercussions even on the social sphere. For example, each new technological paradigm involves strong changes in the consumer tastes, an evolution of skills required from employees, and new innovative products requested on the market. It is therefore important to analyse the role economic and institutional factors play in the selection, and the implications of the establishment of those technological paradigms in our society. In this section we list the main modern ICT paradigms and models.

2.1 BIG DATA

Big Data refers to the appearance of collections of data which exceed the capacities in the systems and traditional technologies for the information management and analysis. Big Data is associated to the management of massive volumes of information but when data can be considered massive depends on the solution type, ambit of use, and activity sector. From the point of view of information systems, Big Data is a major challenge but not only from the point of view of storage, but from the point of view of data collection, processing and analysis. In addition, Big Data also means to create new business models in different business activity sectors [Manyika, 2011].

Traditionally, the Big Data paradigm is characterized by three properties – volume (large volumes of information), velocity (high velocity to data management) and variety (variety in sources and data format) –they are commonly referred to as the three Vs [Gartner, 2015]. However, these are technical properties that depend on the evolution of data storage and processing technologies. Value is a fourth V which is related to the increasing socioeconomic value to be obtained from the use of big data. It is the potential economic and social value that ultimately motivates the accumulation, processing and use of data.

Some projects dealing with Big Data have been founded by the European Commission in FP7 programme. Among them, BIG project [Big-Project] which ended at the end of 2014 has provided a clear picture of existing technology trends and their maturity. BIG processes turn around the Data Value Chain which identifies the following activities: 1) **Data Acquisition** is the process of gathering, filtering and cleaning data before it is put in a data warehouse or any other storage solution on which data analysis can be carried out. 2) **Data Analysis** is concerned with making raw data, which has been acquired, amenable to use in decision-making as well as domain specific usage. 3) **Data Curation** is the active management of data over its life-cycle to ensure it meets the necessary data quality requirements for its effective usage. 4) **Data Storage** is concerned about storing and managing data in a scalable way satisfying the needs of applications that require access to the data 5) **Data Usage** covers the business goals that need access to data and its analysis and the tools needed to integrate analysis in business decision-making. The different technologies which have been addressed in BIG project are displayed in this diagram and fully described in his final whitepaper:

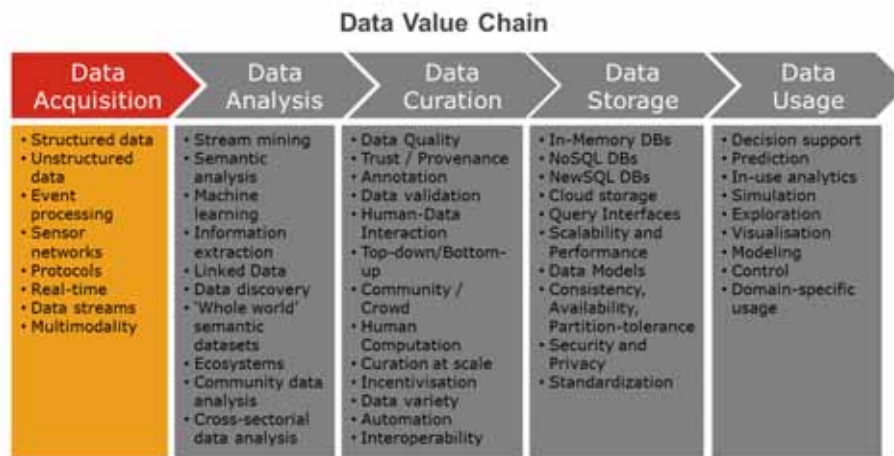


Figure 1. Different technologies addressed in BIG Project

Another currently running project is BYTE (<http://byte-project.eu/>), which will assist European science and industry in capturing the positive externalities and diminishing the negative externalities associated with big data in order to gain a greater share of the big data market by 2020. It has already produced some interesting deliverables. The analysis of current technologies for dealing with variety, velocity, and volume of data – especially how they evolved, gives a way of comparison for capabilities and needs. There is no single tool, or choice of a platform that will remedy all of the challenges of Big Data business. On the other hand, businesses are classified in three main application categories: 1) operational efficiency subsumes all applications that involve improvements in maintenance and operations in real-time or a predictive manner based on the data which comes from infrastructure, assets, and end users, 2) customer experience applications combine data from usage with other sources where end users are active, 3) new business models, especially when applications allow monetization of available data. These applications require a range of analytics capabilities. Especially, predictive and prescriptive analytics enable businesses to reap value from investments into Big Data technologies and infrastructure: Whilst predictive and prescriptive analytics enable the extraction of foresight and options for action based on these insights, Big Data can improve predictive models and enable the testing of actions and evaluating their outcome.

BigDataEurope [BigDataEU] is another project which is starting to run which focuses on providing an integrated stack of tools to manipulate, publish and use large-scale data resources; tools that can be installed and used freely in a customised data processing chain with minimal knowledge of the technologies involved and integrating and industrially hardening key open-source Big Data technologies and European research prototypes into a Big Data Integrator Platform, i.e. an ecosystem of specifications and reference implementations that are both attractive to current players from all parts of the data value chain while also lowering the entry barrier for new businesses. It addresses societal needs (Climate, Energy, Food, Health, Transport, Security, and Social Sciences)

Finally, a Big Data Value Association (BDVA) has been founded in 2014 to boost European BIG DATA VALUE research, development and innovation to foster a positive perception of BIG DATA VALUE (<http://www.bdva.eu>) in a European framework. The BDVA shall present an industry-led contractual counterpart to the European Commission for the implementation of the Big Data Value PPP cPPP. Big data promises challenges and opportunities for organizations. The capacity to quickly and flexibly react to changing requirements is increasingly recognized as a crucial element of everyday business. Big Data impact is not only technological, new challenges must be faced. In the SRIA



(Strategic Research an Innovation Agenda), the BDVA defines the big Data ecosystem as a collection of dimensions to address all these challenges: a) Data: availability of data and the access to the data sources is paramount. b) Skills: A key challenge for Europe is to have people with skills to deliver Bi Data Value with applications and solutions. c) Legal: Importance of data ownership and usage, data protection and privacy, security, liability, cybercrime, IPR, data rights. d) Technical: Real-time analytics, low latency and scalability in processing data, new and rich interfaces; e) Application: The target of the PPP would be the business and market applications. f) Business: Creation of business models on top of Big Data Value. g) Social: Big Data will provide solutions for major societal challenges in Europe.

Nowadays, there are many trends around big data and analytics but the technology is evolving so quickly that cannot be an excuse to start working in such technologies:

- Increasing importance of data interpretability, Importance of legal and security aspects.
- Hadoop success as running many different kinds of queries and data operations will make it a low-cost, general-purpose place to put data that you want to be able to analyze [ApacheHadoop].
- Big data lakes. Traditionally you design the data set before entering any data but the trend is to enter data before having a data model.
- More predictive analytics. The predictability increases because there are a large number of records with many attributes to process and the computer power has increased and even if you can formulate problems with machine-learning algorithms than before could not be accomplished.
- SQL on Hadoop let business users who already understand SQL apply similar techniques to that data instead of using Java, JavaScript and Python)
- NoSQL use
- Deep learning. Machine-learning techniques based on neural networking which are evolving but shows great potential for solving business problem. It allows to deduce relationships without needing specific models or programming instructions.
- In-memory analytics, which is an approach to querying data when it resides in a computer's random access memory (RAM) as opposed to querying data that is stored on physical disks. This results in vastly shortened query response times, allowing business intelligence (BI) and analytic applications to support faster business decisions.

2.2 ADVANCED, PERVASIVE AND INVISIBLE ANALYTICS

With the exponential increase of ICT and user-related data produced every day, analytics is becoming increasingly important. This occurred especially in recent years with the rapid spread of mobile devices capable of producing a huge amount of both structured and unstructured data (the Big Data paradigm). Analysing such information is crucial: “[...] *organizations need to manage how best to filter the huge amounts of data coming from the IoT, social media and wearable devices, and then deliver exactly the right information to the right person, at the right time. Analytics will become deeply, but invisibly embedded everywhere.*” [Cardenas, 2013]. Analytics is becoming crucial for corporate and SMEs as it allows to identify trends, spot weaknesses and predict the right conditions for taking the best decisions about the future. Not only this facilitates the creation of better services, but it also contributes to make the right investments, thus increasing the overall revenue.



Big Data analytic can be seen as both a huge opportunity and a serious issue when referring to cyber-security. Here below, the opportunities and issues are briefly discussed.

2.2.1 THE OPPORTUNITIES

As reported in [Cardenas, 2013] and [Yen, 2013] big data analytics approaches are starting to gather very interesting results in cybercrime-related fields, such as:

- Facilitating a wide variety of industries to build affordable infrastructures for security monitoring (e.g. credit card fraud detection);
- Improving the information available to network security analysts by correlating, consolidating, and contextualizing even more diverse data sources for longer periods of time;
- Allowing the incorporation of unstructured data and multiple disparate datasets into a single analysis framework (e.g., to mine meaningful security information from not only firewalls and security devices but also website traffic, business processes, and other day-to-day transactions).

2.2.2 THE ISSUES

As reported in [Yan], “[...] *the availability and accessibility of a large amount of real-time data from different sources creates new risks of system intrusions.*”

Moreover, high value associated with big data sets has rendered big data storage systems attractive targets for cyber attackers, whose goal is to compromise the confidentiality, integrity and availability of data and information [Madan, 2014].

Finally, as discussed in [Tene, 2012], *“The harvesting of large data sets and the use of analytics clearly implicate privacy concerns. [The tasks of] ensuring data security and protecting privacy become harder as information is multiplied and shared ever more widely around the world. Information regarding individuals’ health, location, electricity use, and online activity is exposed to scrutiny, raising concerns about profiling, discrimination, exclusion, and loss of control.”*

2.3 CYBER SECURITY AND PRIVACY ENGINEERING

With the evolution of the Internet and the services it is able to provide to users, it has become of common use and on a daily basis to transmit sensitive and confidential information in the web. This suggests that the lives of citizens are becoming increasingly digital and, therefore, protecting their data and digital identity is becoming a crucial requirement. However, with the increasing complexity of services offered by the Internet, the complexity to safely handle the transmission and services has increased too. Malicious users use extremely sophisticated techniques to exploit vulnerabilities of systems to steal information and money from the users. Similarly, attackers are also developing powerful capabilities to disrupt, destroy, or threaten the delivery of the most essential services. The cyber security landscape will thus be one of the next paradigms that will play a key role in the society of the future. Due to these strong security requirements, privacy engineering is becoming increasingly important: as it is “[...] *a collection of methods to support the mitigation of risks to individuals of loss of self-determination, loss of trust, discrimination and economic loss by providing predictability, manageability, and confidentiality of personal information within information systems*” [NIST Privacy].



2.3.1 EVERYTHING AS A SERVICE

Several IT organizations have repurposed their business model from selling standalone hardware or software products to selling services. A good example is given by smartphones: legacy phones were hardware products you could buy in a store. Afterwards, no more support was needed from the manufacturer during normal operations (except for warranty and repairs). Modern smartphones need a lot of support from their manufacturer after they have been sold. Typically, the device comes with a number of cloud-enabled programs that need cloud services for example to fetch a weather report or to synchronize their address book. In addition, specific hardware may need to be properly initialized by downloading suitable configuration settings (e.g., AGPS record for a GPS receiver). Although a smartphone is a simple example, more complex systems, such as cars and ERP systems, might need the availability of (sometimes continuous) services offered by the manufacturer to operate properly. To complicate the matters, such services are often not standardized, which makes interoperability or functionality harder to achieve, should a manufacturer fail to provide a specific service. While having continues support by a manufacturer can be convenient for several applications, it also creates dependencies and sometimes single point of failures for a non-negligible number of IT systems.

2.3.1.1 Automated Updates

Automated updates are a special kind of service. Most applications come with an automated updater, or the framework they have been designed in (for example Android and the Google Play Market) provide an automated update mechanism. This can be a huge advantage for security, since once a security problem is fixed by the manufacturer; a patch can be deployed to millions of devices, with no further delays. Unfortunately, automated updates could also be abused by attackers (e.g., vulnerability in the update process or the communication channel) to automatically generate exploits from patches [Brumley et al. 2008] or deploy malicious code to millions of devices at once.

2.3.2 DIGITAL RIGHTS MANAGEMENT

Digital Rights Management (also referred to as Digital Restrictions Management, DRM) is a technology that limits the usage of any kind of digital goods. It is mostly known in the music and movies industry. A song or a movie a user buys might only be played on a limited number of devices in specific Countries. In general, most DRM protected content cannot be transferred to other users or resold in any way. That technology is also comparable to restrictions in the license management of software programs, which can only be installed and used on a single computer at a given time. Such restrictions are not only used for consumer software, but also for commercial software. For example software that is used to manage diagnoses of patients in a hospital comes with a component to limit concurrent usage by doctors.

2.3.3 ENCRYPTION BY DEFAULT

While encryption in software products and network protocols was seldom used 20 years ago, it is often a default today. An increasing number of websites have been switching to HTTPS by default, and many applications use secure connections for either communication with other peers or for fetching updates from their manufacturer. In general, this is a huge step forward for network security since communication cannot be easily altered or read by an intruder, but it is also a big



challenge for firewall designers. Typically, last-generation firewalls have the ability to inspect the traffic they relay through: the deep inspection of network communications is clearly hindered by the use of encryption, which makes it harder to detect and contain malicious network communications.

2.4 RISK-BASED SECURITY AND SELF-PROTECTION

When we speak of the future of our society, security plays a central and crucial role. Therefore, it is of paramount importance to understand what types of investments organizations need to make to secure their environment and protect their business assets properly. Nowadays, the process used to perform security checks and controls is often mistakenly associated with the vulnerability assessment. However, guaranteeing strong security should not just be associated to a mere protection of cyberassets, but rather should be extended to embrace people and processes. Vulnerability assessment tools are functional, but they only focus on the technical side of security. Instead, it is necessary to ensure that even the processes adopted and people involved are able to ensure an high level of security for the business assets. Similarly, it is not enough to ensure the protection of the perimeter of the corporate network from external attack, but rather must be protected even individual applications and internal processes.

Applications in particular need to be analysed in depth: *“[...] security-aware application design, dynamic and static application security testing, and runtime application self-protection combined with active context-aware and adaptive access controls are all needed in today’s dangerous digital world.”* [Gartner Trends]. Therefore, it is important to remark that every single component must be properly secured and protected as its failure could involve a failure of the entire service. This way, it is in principle possible to ensure that business and assets are properly protected against emerging threats that every year are targeting many organizations causing them considerable damage and losses of sensitive data.

2.4.1 DYNAMIC RISK MANAGEMENT

Nowadays, cyber risk management practices are adopted by the majority of large corporations to identify, analyse and manage cyber risks. A large number of methodologies, standards and tools have been developed to accommodate the particularities of different sectors and scenarios. However, these approaches are not a continuous process, but an activity repeated regularly over discrete and large time intervals.

These methodologies are valuable, if only because their application implies introspective efforts that help the organization to assess their situation and work towards its improvement. However, when it comes to dealing with the dynamic nature of technology and cyber threats, they become ineffective. Even if the intervals between risk assessments were smaller, they would still leave a window of opportunity where systems security could be compromised. The constant evolution of the threat landscape, the ever changing structure and behaviour of systems and networks, and the continuous appearance of new vulnerabilities render the results obtained from the application of these methodologies rapidly obsolete.

Another major weakness of current risk assessment and management methodologies is the inability to deal with various forms of uncertainty and, especially, lack of knowledge. Most approaches are generally very deficient when dealing with “unknowns” and do not provide an explicit means to do



so. It is true, however, that in many cases there are workarounds that in one way or another allow the consideration of “known unknowns”, i.e., entities (assets, threats, etc.) that we know that we do not know. A major problem, however, originates from “unknown unknowns”. For instance, knowing that one asset is vulnerable but not knowing the specific vulnerability is quite different from not knowing that the asset is vulnerable in the first place. Unknown unknowns constitute an important class of cyber security threats as they are, by definition, simply ignored by current risk assessments.

Dynamic risk management (DRM) is a novel concept where a continuous feedback of the system under observation is provided, monitoring attacks and adapting to different situations or events that may arise in real time [Poolsappasit, 2012].

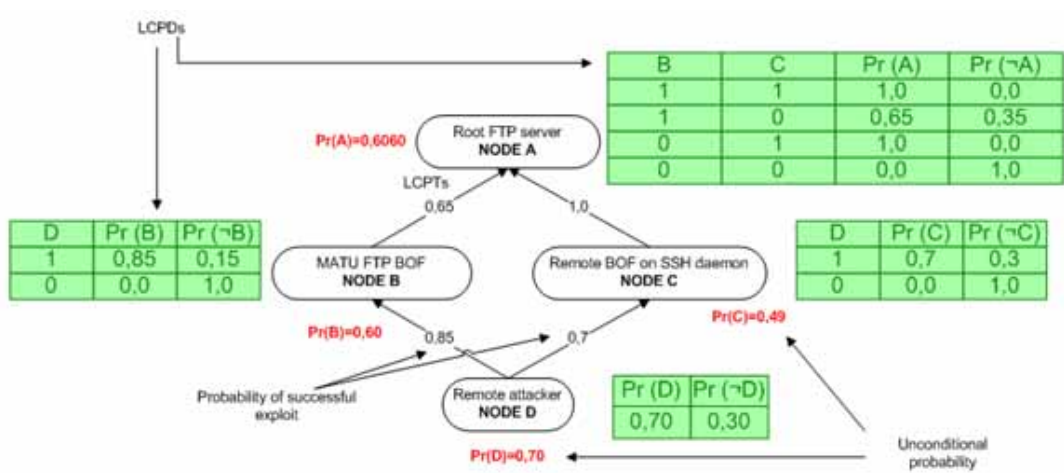


Figure 2. Bayesian Belief Networks used in Dynamic Risk Management Models

Under this new model, the human analyst should be leveraged for the few tasks that cannot be automated, such as the re-valuation of the assets. A heavy involvement of humans during the assessment and management of risks could otherwise sent us back to the undesirable situation raised by tradition risk management. Automation becomes a fundamental tool in the fight against cyber threats, and thus a critical component for effective risk management. In spite of this, automation poses new risks that have to be carefully balanced during the implementation of a DRM model. For example, constant changes in the organization can quickly generate blind spots not covered by automated systems.



Figure 3. Main standards involved in DRM

DRM presents promising properties to help in the dynamic detection and mitigation of risks and attacks. Some of the challenges addressed by a DRM solution are real-time performance, big data support, automation, scalability, adaptability or the capability to deal with uncertainty [NeoBlog].

2.5 OPEN SOFTWARE

Open Source, better Open Source Software (OSS – or Free OSS, FOSS also), is not exactly a ‘technology’, but rather a way to conceive Software development and software itself by releasing not only the (binary) executable component, but especially the complete source code of software; Furthermore, the original owner provides the users with the right to review und further develop the software, as well as study it for their own purpose. While the compiled version for end users could be also commercialized, the access to full source code has to be publicly accessible and free of charge. By this way everyone can download the source code of a specific software (i.e. OSS), study it and customizing it according to own needs and release the new version. But Open Source is also considered a ‘philosophy’ where concepts like open exchange, collaborative participation, transparency and community development are fully embraced and celebrated (also strongly recommended, but never imposed). Today many little, medium and big software houses and organizations make use of Open Source Software and this trend is on the rise. In this last case the most important reasons for its great success are its modifiability and the absence of commercial licenses (it is free of charge). [OSD].

According to [Blackducksoftware], the GNU General Public License (GPL) is the most popular open source license followed by the MIT License and the Apache License 2.0. While many open source licenses agree on the core principle of releasing the source code, there are several important distinctions to be made, For example, the GPL is a viral license, i.e. any modification of the code that was distributed under the GPL must be again licensed under the GPL. This is also called a “copyleft” license and is opposed to other open source licenses like the BSD license or the MIT license, which are also called “permissive free software licenses”.

2.6 OPEN HARDWARE

Open Source concepts can also be applied to computer hardware, thus obtaining the concept of so-called “Open Hardware” or “Open Source Hardware (OSHW)” [OSHWA, 2012]. In this case the design of all tangible artefacts (i.e. electrical, electronic, logical and/or architectural schemes) must be publically accessible. Also documentation including design files have to be released and well-publicized, licenses must not restrict modifications to the hardware or software and must not be specific to a product. Furthermore, no kind of discrimination against persons, groups and fields of endeavour, and others is allowed. If the licensed design requires software, embedded or otherwise, to operate properly and fulfil its essential functions, then the license may require interfaces sufficiently documented and an OSI-approved open source license.

Currently there exist several different open hardware licenses that generate some popularity among the scene:

- The TAPR Open Hardware License [TAPR] was specifically created to cater for open hardware projects by Tucson Amateur Packet Radio. The specification was heavily influenced by the GPL, but tried to incorporated demands specific to hardware [Ackermann, 2009].
- The CERN Open Hardware License (CERN OHL) created by CERN, which was created to provide for a collaborative framework for hardware development [Ayass, 2012].
- The Solderpad Hardware License [Solderpad], which is an adaption of the Apache 2.0 software license in order to make it more suitable for hardware projects



- The Balloon Open Hardware License, which is a non-copyleft license based on the MIT-license without much changes [P2PFoundation].
- The HDPL (Hardware Design Public License), which is inspired by the OSS GNU GPL [P2PFoundation].

Furthermore, many open hardware projects use one of the prominent open source licenses, even though these were originally made for software instead of hardware. Currently the main problem with all open hardware licenses is the difference in the application of copyright between hardware and software under certain jurisdictions. One popular example for the application of such a license is an open source 3D-Printable mobile robotic platform shown in [Gonzalez-Gomez, 2012]. Another even more popular case is the physical computing platform Arduino, which also follows an open source approach for their hardware components.

Another fundamental approach was the publication of the book “Open-Source Lab: How to Build Your Own Hardware and Reduce Research Costs” by Joshua M. Pearce through Elsevier, which provides a lot of instructions on building scientific instruments and laboratory hardware based on simple building blocks like Arduinos [Pearce, 2014].

2.7 FUTURE SECURITY AND PRIVACY INCIDENT MANAGEMENT

2.7.1 SECURITY INFORMATION AND EVENT MANAGEMENT

The term Security Information and Event Management (hereafter SIEM) stands for a set of tools and processes for managing IT security, as well as a set of IT best practices: Different inputs from various sources shall be normalized, deciphered and aggregated, including the problems inherent in the analysis of massive amounts of real time data. Therefore, Complex Event Processing (CEP) technologies have been devised in order to detect threats from the information gained, as well as maximizing the value of the supporting logs and increase the reliability of IT services.

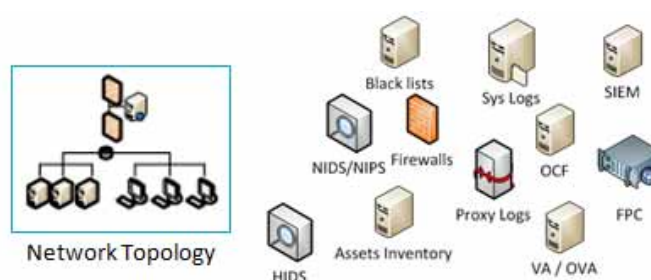


Figure 4. Some technologies to be orchestrated

“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.” [CAPITALProj]



2.7.2 SECURITY INCIDENT RESPONSE

The trend during the last years to incorporate incident response (IR) products and services into the arsenals of security teams can, according to Bruce Schneier [SchneierOnSecurity], be attributed to three fundamental reasons:

1. Companies and other owners have lost the control over their computing environment(s), often voluntarily by outsourcing data storage to the cloud, as well as by outsourcing the actual networks, thus making any kind of response more complex due to lack of control over large parts of the actual critical infrastructure.
2. The rise of increasingly sophisticated and complex attacks, especially considering so-called Advanced Persistent Threats (APTs) that were built with specific targets in mind, often for rather complex reasons, as well as using hacking as a means for making (geo-) politics between nations, including increasing collateral damage to unrelated networks.
3. The lack of investments by companies in protection and detection, although these are imperfect even under perfect circumstances.

Seen from a tactical level, according to Schneier, security is a combination of people, processes and technologies. While most detection systems rely heavily on technology, with some assistance of people and processes, detection is more evenly distributed among the three and response relies heavily on people with assistance by technologies and processes.

Schneier cites a statement by Cranor as key to successful IR "[...] *there are some tasks for which feasible, or cost effective, alternatives to humans are not available. In these cases, system designers should engineer their systems to support the humans in the loop, and maximize their chances of performing their security-critical functions successfully.*" deriving that the real need in security lies in developing technology that aids people, not supplanting them [SchneierOnSecurity].

2.8 PARADIGM SHIFT IN INDUSTRIAL CONTROL SYSTEMS

In this section, we concentrate on two main areas regarding paradigm shifts [WikiParadigmShift] in industrial control systems, namely (1) SCADA systems and (2) Resilient Control Systems.

2.8.1 PARADIGM SHIFT IN SCADA SYSTEMS

While many of the world's industrial control (SCADA) systems were built or designed at a time when the computing components of such critical infrastructure were not connected to the Internet, recent years saw some drastically changes when companies started to connect these devices and networks to their company networks, mainly in order to gain better control or to generate new products and services [WaterfallParadigmShift].

Based on this trend, an increasing amount of legacy systems, designed without the notion of security in mind, has been connected to the Internet, thus making industrial control systems a highly prioritized task throughout recent years. One new approach for perimeter protection of such systems is the concept of unidirectional gateways, i.e. gateways which only allow communication from one side to the other. This is mainly established by building hardware that physically only allows one direction, e.g., photo cells triggered by laser.



This is very different to more classical approaches, where a firewall filters types of traffic, predefined as being malicious, but still allows communication for most other traffic. Furthermore, since being a software component itself, firewalls are prone to attacks themselves, which is not possible for unidirectional gateways due to physical limitations.

2.8.2 PARADIGM SHIFT IN RESILIENT CONTROL SYSTEMS (RCS)

“A preeminent objective for corporate and government organizations is state awareness, a comprehensive understanding of security and safety for critical infrastructures, embedded within their industrial-based control systems. Asset owners as well as government are burdened to ensure they have a timely understanding of the status of their plant(s), to ensure efficient operations and public protection.” [INLPortal].

One of the main problems in historically developed control system lies in the fact that trust relationships between peers cannot be guaranteed and that the security of the communication cannot be assumed reasonably. Even more, a resilient control system design incorporates the role of a malicious actor, who is well-integrated in the environment and part of normal operation, in order to mitigate this threat [INLPortal].

These measures can be categorized as cyber and physical security, process efficiency and stability, and process compliancy, and provide the operating requirements that are monitored for state awareness and the actual definition of the state space.

Further needs include research into human system response, including not only malicious interactions, but also legit administrators, including the problems derived by highly distributed control systems.

“The move from reactive to proactive control of plants and mechanisms by which the evaluation and verification of designs is considered all the way from design through implementation stages of resilient control systems is enabled by this paradigm shift” [INLPortal].

2.9 INTRUSION MANAGEMENT SYSTEMS

In this section we want to describe the two main technologies that manage computer intrusions. Note that this kind of systems can be realized in hardware and/or in software (as application programs or firmware).

2.9.1 INTRUSION DETECTION SYSTEMS

“An intrusion detection system (IDS) monitors network traffic and monitors for suspicious activity and alerts the system or network administrator. In some cases the IDS may also respond to anomalous or malicious traffic by taking action such as blocking the user or source IP address from accessing the network” [NetSecurity].

There are several different strategies currently known and applied for the detection of suspicious traffic, as well as where these detection mechanisms are positioned in the infrastructure. Also the reaction on the detection can be different; while some systems only raise alerts, others are



configured to actively respond in order to, e.g., generate additional knowledge on the adversary. In the following, we give an overview of the most important strategies for intrusion detection systems.

NIDS

So-called Network Intrusion Detection Systems (NIDS) are installed within the network to monitor traffic to and from all devices inside the protected infrastructure, usually residing in specified nodes with a strategic value. Ideally, all inbound and outbound traffic should be scanned, still, this runs into the danger of creating bottlenecks in the infrastructure [NetSecurity]

HIDS

Contrary to NIDS, Host Intrusion Detection Systems (HIDS) monitor inbound and outbound events (e.g., API and system calls) of a specific device on which they are installed, to detect suspicious activities [NetSecurity].

Signature based-detection

Signature based IDS work quite similarly to traditional antivirus software, i.e., by scanning all packets that are encountered on the network for known signatures, i.e., fingerprints of known malicious threats. The main drawback of this approach lies in the fact that only known threats can be detected, which is especially problematic in the case of new attacks that have not been detected before. Furthermore, the update of the signature database typically needs some time after the new threat was first detected, leaving the system vulnerable in the meanwhile.

Anomaly based-detection

In contrast to signature based systems, anomaly based approaches generate a model of normal behaviour (e.g., network flows or sequence of system calls), which is assumed to be benign. This model serves as a baseline against which further events will be compared against. Any deviation from the normal behaviour is then flagged as anomalous, raising an alarm. The main strength of such approaches lies in their ability to detect previously-unseen and unknown attacks. Unfortunately, the catch is that false positives are generally quite high: anomalies are in fact considered to be instances of attacks, but they generally represent previously-unseen and unknown benign actions.

2.9.2 INTRUSION PREVENTION SYSTEMS

“An Intrusion Prevention System (IPS) is a network security/threat prevention technology that examines network traffic flows to detect and prevent vulnerability exploits. Vulnerability exploits usually come in the form of malicious inputs to a target application or service that attackers use to interrupt and gain control of an application or machine. Following a successful exploit, the attacker can disable the target application (resulting in a denial-of-service state), or can potentially access to all the rights and permissions available to the compromised application” [PaloAlto].

The main difference to Intrusion Detection Systems (IDSes) lies in the fact that the IDSes are typically passive systems with respect to the monitored traffic which reports findings. The IPS on the other hand is often combined with other systems and is placed directly in the communication path. The main target lies in analysing the traffic and reacting in case of suspicious traffic, including



measures like alarming administrators, dropping suspicious packets or even blocking connections altogether.

Since the IPS is applied in the direct communication path, it must work very effectively in order not to establish a bottleneck. Furthermore, in case of automated response measures the IPS must work as accurate as possible in order to avoid false positives [PaloAlto].

2.10 UBIQUITOUS / NOMADIC COMPUTING

2.10.1 UBIQUITOUS COMPUTING

When we talk about ubiquitous computing (also known pervasive computing) we mean the use of hardware and software technologies embedded into everyday objects and devices making them able to communicate by exchanging information. Mark Weiser is considered the father of ubiquitous computing. This new paradigm represents a profound evolution compared to desktop computing, because while in desktop computing it is used only one machine for a specific purpose, with ubiquitous computing devices are used while you are doing normal everyday activities, thus shifting the application of the IT technologies from the desktop to any other field: from houses to cars, from appliances to tools, etc. Alan Kay of Apple calls this the "Third Paradigm" in computing: *"Ubiquitous computing names the third wave in computing, just now beginning. First were mainframes, each shared by lots of people. Now we are in the personal computing era, person and machine staring uneasily at each other across the desktop. Next comes ubiquitous computing, or the age of calm technology, when technology recedes into the background of our lives."* [Weiser, 1995] Ubiquitous computing therefore it is also strongly different from the virtual reality, because while the virtual reality has the aim to place people in a reality generated by computers, ubiquitous computing has the purpose to put the computers inside the context of people's daily lives.

2.10.2 NOMADIC COMPUTING

The definition of the term "nomadic computing" is used to indicate the use of connectivity technologies able to connect a user to the Internet while it is moving from one place to another. This is particularly important because users need to continuously connectivity to the Internet to access their email and company data. The use of technologies for nomadic computing does just that, ensure access to the network regardless of the place, the transmission capacity and technologies used for the connection. There are different definitions for the term nomadic computing:

"According to the WiMax forum, nomadic stands for semimobile, which means that a minimum, the client mobile device is transportable to secondary fixed locations with no connection while in transit." [68]

While for the broader industry the term nomadic means mobile:

"Mobile computing takes place when portable computing devices interact in some fashion with a central information system. Users access the Internet and data on their home or work computers while away from the normal, fixed workplace." [Kindberg, 2001]



2.11 CONTACTLESS TRANSACTION

Contactless transaction/payment systems are credit and debit cards, key fobs, smartcards or other devices that use radio-frequency identification for making secure payments. The embedded chip and antenna enable consumers to wave their card or fob over a reader at the point of sale. Some suppliers claim that transactions can be almost twice as fast as a conventional cash, credit, or debit card purchase. The mass market introduction of contactless technology is an important event for the payments industry. Contactless payments are already providing benefits to consumers and retailers alike, in terms of higher levels of control and convenience for consumers and higher throughput for retailers.

2.11.1 NEAR FIELD COMMUNICATION FOR CONTACTLESS TRANSACTIONS

Mobile and contactless payments have been globally growing very fast over the last three years, both in figures and in pervasiveness and, at the end of 2013, they were representing 15% of the total transactions, whereas they are predicted to even overcome volumes generated by cards transactions within the next 10 years.

One of the main development from a technological point of view, which is having a deep impact on the way the payment transaction is conceived and executed, is undoubtedly the use of Near Field Communication, which, even if not initially designed for payments, may enable contactless operations to be directly authorized and accomplished by the user.

The evolution of NFC payments has been followed - and in some case anticipated - by both regulatory and standardization bodies, who setup a suitable framework to rule technical procedures and contexts of use. Some open issues have remained though, concerning security of operations accomplished through NFC, in terms of the possibility to preserve integrity and confidentiality of payments data and to prevent unauthorized interception, altering or interruption of payment operations.

According to Gartner [GartnerWWPT], a disappointing adoption of the NFC technology in 2012, together with an unclear strategic development of some high-profile services relying on that technology, are two main components which strongly affected its overall diffusion, bringing to a reduction with respect to what was initially forecasted for the total transaction value relying on NFC. In fact, as of today, market share accounts for a transaction value around the 3% of the total, which is almost the half of what was expected. Nevertheless, a new growth of interest and a consequent increase in its usage is foreseeable starting from 2016, in parallel with the consolidation of the mobile phones market and the wider diffusion of contactless systems.

2.11.2 NFC TECHNOLOGY OVERVIEW

NFC is the acronym of Near Field Communication and refers to a technology designed to enable short-distance, wireless, bi-directional connectivity between two devices. Such technology comes out as an extension of the standard ISO/IEC 14443 and consists of a combination of the interface of a smartcard and a reader in one only mobile device. It is a technology which has been available since several years, even though only recently it started to be commercialized on a wide scale.





In order to promote NFC potentialities and agree on standard ways to embed such technology in their mobile devices, some of the biggest players in the mobile market, Nokia, Philips and Sony, joined together in 2004, founding the NFC Forum, a not-for-profit association aimed at defining specifications for interoperability of devices and fostering the diffusion of NFC technology [NFCForum].

NFC-based chips have been successfully used in many applicative areas, but the most relevant one, which boosted many big players' interest and investment, is the one related to mobile payments, with specific reference to Mobile Proximity Payments, which are executed when physical proximity exists between the merchant's and the customer's devices.

From a functional point of view, NFC payments can be summarized in two steps:

- A payment device sends a message which is received by the NFC chip of the phone, which will display the amount to be paid and a request for authorization;
- Once the authorization is received, a reply is provided to the payment device, and the amount is directly charged on the user's bank account.

With respect to payments based on contactless cards, using NFC then represents a plus in that it integrates their characteristics with functionalities of mobile phone devices, such as the availability of a display to interact with the user and the availability of an internet connection via WiFi or GSM/UMTS. Additionally, NFC allows to read RFID tags and to interact with other NFC devices, being able to integrate value added services using the chip's functionalities of authentication and communication.

This way, a mobile device which supports the NFC technology may integrate or even substitute the traditional payment card and can be regarded as an "electronic wallet" where to store different cards – just to cite some examples: credit cards, prepaid cards, loyalty cards, transport cards, and so forth.

And it is relevant to notice that NFC technology can be used also as a support to those services which are not directly linked to enabling payment transactions, but as a device for user identification. Just to cite examples, a NFC-enabled mobile phone can work as a badge for access control or as a tool for ticketing services.

Another field where NFC has been successfully used is that of additional security provided to other devices. Just to cite a couple of examples, a smartphone might be used to unlock a PC, using a user

profile stored in that mobile, or to enable, via its physical presence, some functionalities, such as the home banking.

As said, NFC-based devices are growing in figures and in diffusion on the global scale, but still, they are currently covering less than a half of the whole market of mobile devices. In order to enable NFC-based services also on those devices who are not natively supporting the use of NFC, suitable plug-ins have been introduced into the market, which provide smartphones with contactless capabilities.

2.12 TRUST AND IDENTITY

In a highly and still increasingly internet-connected world, where private and public organizations, citizens, potential cyber attackers and victims communicate through a technological network, issues like Trust and/or Identity are of greatest importance. That's because every 'subject', manually or at various level of automation, need to trust the communication target, but it can be also needed the trust on communication path. As also stated by Forrester, these issues get a rethink. In fact they do not even apply to data transmitted on a network, and the question that can arise is: who or what can we trust? These concepts are going to be completely re-invented. [DiSalvo]

Authentication technologies

2.12.1 ONE TIME PASSWORD (OTP)

OTP devices are able to generate a numeric code that changes every time it is used or as the time passes. The OTP code is generated using a secure algorithm and the device is synchronized with a server that is able to check if a code supplied by a user is generated using the OTP device.



Figure 5. Key Ring form OTP token



Figure 6. Smartcard form OTP token

2.12.2 PERSONAL CARD READER

PCR devices are OTP devices that are able to “sign” a transaction using a challenge/response mechanism. They can be coupled with a smartcard and protected with PINs to increase the security level.



Figure 7. Personal Card Reader

2.12.3 “ON-CARD” CHALLENGE-RESPONSE DEVICES

This kind of authentication devices are embedded on a smartcard equipped with an alphanumeric display and a micro-keyboard. Users can interact with the card and use it as a simple OTP device or a Personal Card Reader implementing challenge-response mechanisms.

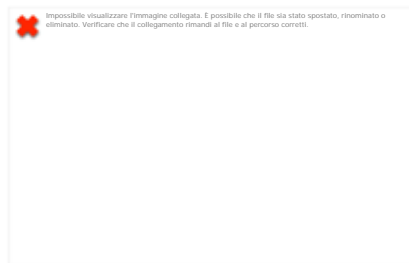


Figure 8. Challenge-Response mechanism implemented on-card

2.12.4 ONE-TIME PASSWORD VIA SMS

The GSM Network can be used as an alternative communication channel to send users a dynamic authentication factor or to confirm payment transactions via an OTP code sent in an SMS message.

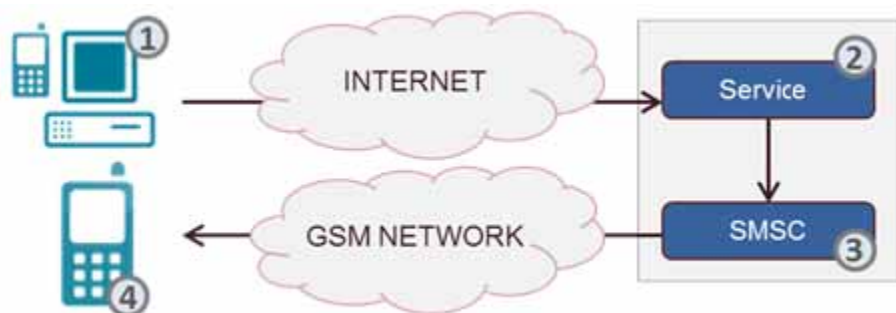


Figure 9. One-Time Password via SMS mechanism

2.12.5 CERTIFICATE-BASED AUTHENTICATION

A digital certificate can be installed on mobile devices into secure storage areas in order to implement strong-authentication mechanisms. Several security products on the market adopted this strategy enabling devices to be used as a second authentication factor in a transparent way for users.



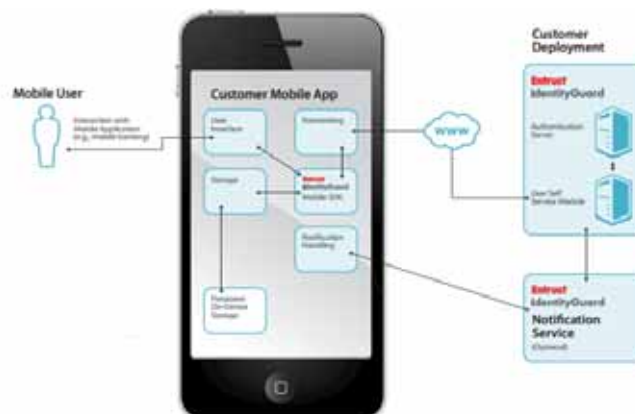


Figure 10. Example: logical architecture of the Entrust IdentityGuard Mobile SDK

2.12.6 MOBILE ONE-TIME PASSWORD (OTP)

On mobile platforms “virtual” OTP generators are available. This applications offers the same functionalities as the hardware tokens while keeping the user private key in the secure internal storage areas. After using a PIN code to unlock the application, an OTP code is generated.

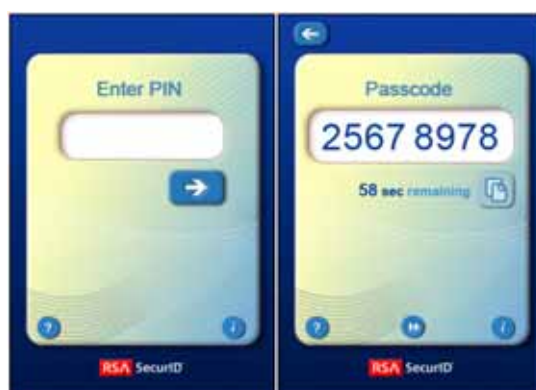


Figure 11. Example Mobile OTP application

2.12.7 MOBILE TRANSACTION DATA SIGNING

A more sophisticated mobile app may implement Challenge/Response mechanisms using Transaction Data Signing (TDS) techniques to sign payment transactions.

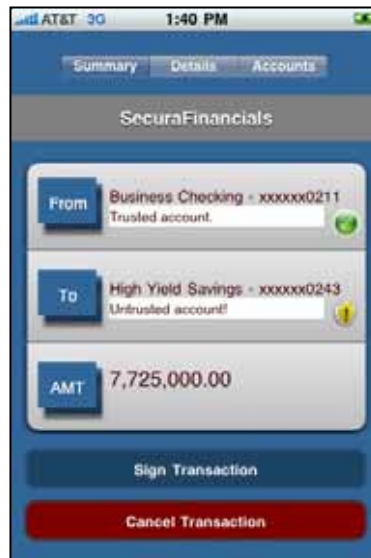


Figure 12. Example transaction signature via challenge-response mechanism

2.12.8 VOICE RECOGNITION

The voice of an individual is unique; thanks to a number of variable factors that makes the voice timbre usable as an authentication factor. Currently several commercial authentication solutions are present on the market even for the mobile platforms.



Figure 13. Logical schema of an authentication process via voice recognition

2.12.9 FACE RECOGNITION

Using the embedded camera, mobile devices may authenticate users focusing the users' face and comparing the image with another one previously acquired.



Figure 14. Screenshot of a mobile application using face-recognition

2.12.10 IRIS RECOGNITION

Several mobile applications are available on the market implementing users' iris recognition as an authentication factor, by the way they are still not as mature as other biometric authentication techniques, because infra-red cameras should be used to acquire the iris "texture" in order to get the necessary image details.

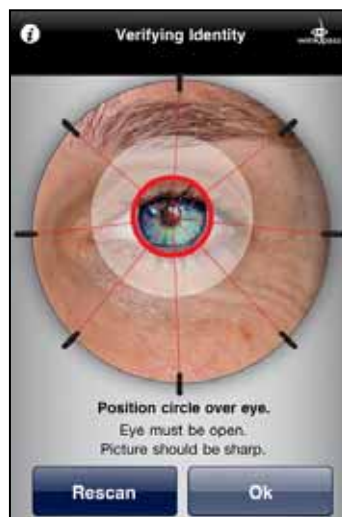


Figure 15. Example of an iris-recognition based authentication application

2.12.11 FINGERPRINT RECOGNITION

Users strong authentication via fingerprint scanning are already implemented on mass-market mobile devices and are mature and reliable solutions.



Figure 16. Fingerprint scanning on an Apple iPhone device

2.12.12 PATTERN BASED RECOGNITION

“Semantic” tasks can’t be easily automated or replicated and may introduce an higher security level for the authentication mechanisms on mobile platforms. An interesting implementation of this security mechanism is the Pattern-based recognition where a user have to reproduce a pre-recorded path on the screen to authenticate.



Figure 17. Example of pattern-based unlock screen

2.12.13 IMAGE BASED AUTHENTICATION

Another example of semantic task based authentication is the image-based recognition where users are requested to identify an idea, a concept, or to select a group of images according to a pre-recorded order.



Figure 18. Example mobile application for image-based authentication

2.12.14 COMPARATIVE ANALYSIS

In order to compare the different solutions for a strong authentication, we defined an analysis model based on the following features:

		Approach							
		Traditional			Multiplatform	Mobile			
		OTP	Challenge - Response	TDS ¹²	Certificate	STK ²⁰	Biometric	Advanced App	Telephony
Features in comparison	Security level								
	Secure provisioning						-		
	Usability								
	Easy to carry								
	Easy to distribute								
	Easy to upgrade								
	Easy to decouple								
	Secure notification								

	Feature non present
	Feature implemented, still not mature
	Feature implemented, intermediate maturity level
	Feature implemented, good maturity level, still not distinctive compared to other solutions
	Feature implemented, very good maturity level, a reference point

Figure 19. Comparative analysis

3.1 SMART CITIES

For further information see Appendix A: High Level Scenarios section 4.1

The new paradigm of cities is based on the need to respond to the new challenges that have arisen in recent years based on the new model of city urbanization, based on the rise and impact that these new needs and the consequences on the current management model.

Cities have historically played a major role in developing opportunities, and today, this role is even greater, as recent studies by the United Nations and World Bank, estimating that 80% of global GDP is generated by the cities. The synergies that are generated in cities, for cultural, social reasons, and attraction, creates an employment development space tremendously favourable to innovation and job creation of high added value.

The management of existing metropolis is increasingly difficult, and the demand for services is progressively higher, just like the quality that is expected of them. All forecasts indicate that the growth of cities continues inexorably coming to:

- By 2030, an estimated 60% of the world population will live in urban areas.
- Every day nearly 180,000 people are added to the urban population.
- 75% of energy consumption is estimated on urban areas
- As also 80% of greenhouse gas emissions

Thus, it is necessary to define a new generation approach to deal with this new paradigm and confront these necessities by giving new responses.

3.1.1 SMART CITIES STATE OF THE ART

The smart city concept has reached a point of hatching. There are many cities throughout the world focusing their investment models based on smart actions. In many cases these actions are based on isolated solutions in terms of energy efficiency or improvements in the transportation network solutions. However, just as there are many actions that do in terms of citizen participation, transparency or service's accountability.

We can therefore identify three models of smart actions clearly differentiated: The New Brand City (infrastructure-based), The City of Sensors (based on the M2M concept) and The Smart Interoperability City Approach (based on a platform interoperability). Each of these three scenarios has a different view, as an approach of what should be a smart city:

The first one (The Brand New City) is only possible in scenarios where you are creating a city from scratch, or only applicable to a new residential area of the city under construction. Starting with a clean state is easier to create a city with the conditions one may want for a city of the future. At the same time as it is linked to an urban concept, attracting people and future residents lies in the quality of services available and the model of smart cities has high appeal on it. These cities can therefore focus their model in a complex, advanced telecommunications infrastructure network and



other urban infrastructure, which allow the city to adapt more easily to the requirements of present and future.

On the other hand, our second approach (The City of Sensors), is based on these cities where the creation of new areas is more complicated or nonexistent, and where the smart needs are based on data collection. It is a model based on sensing of cities in order to know what is happening in your city and thus make decisions based on real time data. In turn, these city models usually have a large number of isolated smart actions (As containers with capacitive sensors, traffic sensors, air quality meters, etc).

Finally, the third model (The Smart Interoperability City Approach) is focused on urban management from a central vision. In this scenario, the city has a middleware that is able to read information from their smart services, network of sensors, open data sources and other devices such as mobile phones, etc., in order to unify all the information into a central platform, allowing decisions based on all available information, not just in one service isolated information. This approach focuses on the interdependencies that each service has with other city services, as planning and knowledge of the state of others, enables better management, better use of data and higher protection in terms of resilience.

3.1.2 CYBERSECURITY AND ITS ROLE ON SMART CITIES

Within the world of Smart Cities, security plays a key role not only by securing safe communications but also by achieving a high level of data protection.

Taking into account the approach that city management is taking in the smart cities, the security is meant to be one of the big issues to assure the efficiency and result of the new system. The Smart Interoperability City Approach is nowadays the procedure leading the path for smart cities. And as a brain who manage the city, coordinates infrastructure and interacts with different services provided by many operators and used by millions of citizens needs to assure the security of its data, its communications and be able to prevent hacking actions against it.

Data itself is a business, so privacy the users become highly important. It is necessary to implement mechanisms that protect users against misuse from data consumers. Communications are also an important factor, as an attack to a smart infrastructure can collapse the city and create important problems to its citizens.

We are introducing communications to the city infrastructure and bringing access to the objects to a network composed by nearly every single element of the city.

The Smart City concept is revolutionizing the way cities manage their services and the way in which citizens interact with the administration and with their own city. Thus, it is necessary a holistic view of the city and its services. This is where comes in the Urban Platform concept.

The urban platform aims to improve the services offered by the city, from one central intelligence engine to be able to exchange information from heterogeneous sources among several services and to manage it from an integrated point of view.



Such platform would have a middleware to enable interoperability of multiple systems, providing a semantic interoperable platform which allows real-world information available to applications Smart (Internet of Things) with a focus on Big Data, Cloud-capable, Open source, multi-language and agnostic communications.

This holistic approach to smart cities was born with a spirit of integration, and hence the main role of a urban platform, but also with the vocation of expansion beyond the limits of a city, growing into its metropolitan area, including the incidence of aspects such as mobility, waste management, water management, etc., which affects more services and citizens beyond the strict area of the city.

Yet, it is known the need of evolution towards intelligent systems and service provisioning at the ends of the network. These decentralized systems delegate the authority for decision-making at lower levels, without requiring the validation of higher level entities. Distributed systems consist of many entities that work together, and users are shown as a single coherent system.

No matter if at the end we face a centralized or distributed architecture, what is absolutely true is that as the proliferation of IoT deployments, the diversity and number of threats that seek to exploit vulnerabilities present in Internet-connected devices will grow. We will have to deal with estimated billions of objects that interact with each other and with other entities such as individuals or virtual entities. All these interactions should ensure somehow protecting the information and services offered by the different actors and limiting the number of incidents that may affect the entire network. However, protecting the IoT is a complex task because the number of potential threats grows rapidly in a context of overall connectivity and accessibility. Threats and types of attacks are numerous, including attacks on communication channels for data theft, denial of service, manufacturing and impersonation, operate services on a non- authorized, etc.

Attack models that can be used against these types of networks are independent of either the architecture they have is centralized or distributed [Román, 2013]. However, by the very nature of them, an attacker could control part of the network but it is not possible to control the entire system. More likely attack models are [Babar, 2010]:

- Denial of service: in addition to depleting traditional resources of the service providers and network bandwidth, wireless infrastructure of data acquisition networks is also a target.
- Physical damage this attack is typical of attackers who have no technical knowledge but can damage the physical device or at least the hardware module that enables virtualization of it.
- Eavesdropping: attackers can go into the channels of communication to extract data from the information flow. Any internal attacker who gains access to a particular infrastructure could extract information circulating within that infrastructure.
- Nodes capture: as the devices are physically located in a certain environment, rather than destroy, an attacker could try to extract the information they contain. Objectives of this attack could also be other infrastructure to store information, such as processing entities or data storage.

3.1.3 CONCLUDING REMARKS

In this section we have observed the different elements involved in the process of conversion to a Smart City. In this case, the approach is given by a central solution that acts as a platform or



operating system of the city. An idea like this has already been adopted by the city of Barcelona. Then we have shown that either in a centralized or distributed approach, it is of special relevance the security of the urban platform, its availability as well as the integrity of communications and often the confidentiality of personal information (i.e., network security).

3.2 INTERNET OF THINGS/QUANTIFIED SELF

For further information see Appendix A: High Level Scenarios section 4.2

The Internet of Things (IoT) is probably one of the most important new technological paradigms of our days. IoT can be considered as the first real evolution of the Internet and being a new technological paradigm, it has the potential to change the way people live, work and think. What makes up the IoT is everything that is real, tangible and is able to use the latest technology to connect to the Internet. This creates a new virtual network composed by new devices and entities that will improve our life quality: *“From energy grids and traffic, to medical and financial decision-making processes, to the very texture and nature of our daily life”* [IoT_EU]. However, despite its enormous potential, IoT has also raised a number of paradoxes due to the fact that the same technologies on which it is based can dramatically increase its complexity and the overall difficulty of management.

3.2.1 QUANTIFIED SELF

In recent years, the concept of collecting and analyzing data has moved from being mainly used in business, to a much more personal level. People are now tracking every facet of their lives with the aid of technology. This, in essence, sums up what the quantified self movement is and what it stands for [Ballano, 2014].

The Body Area Network (BAN) made of wearable sensors, is an application area that exists since few years and has extensively researched through EU projects (e.g. WASP project, IST-034963 and many others). Despite this, its applications outside the research area were not significant until the recent years. Normal people were not happily using BAN sensors in their everyday lives mainly due to some common critics:

- sensors are not really usable and well designed for everyday usage;
- sensors are not well integrated into an unique system or middleware,
- sensors are not precise enough for clinical applications, especially those targeted for the mass-market;

On the other hand, Figure 20 reports a list of the possible signals that can be measured using a BAN of wearable sensors. The number of signals that can be used with such sensors is quite wide and creates a good connection with the increasing applications of mobile biometry (see section 3.3)



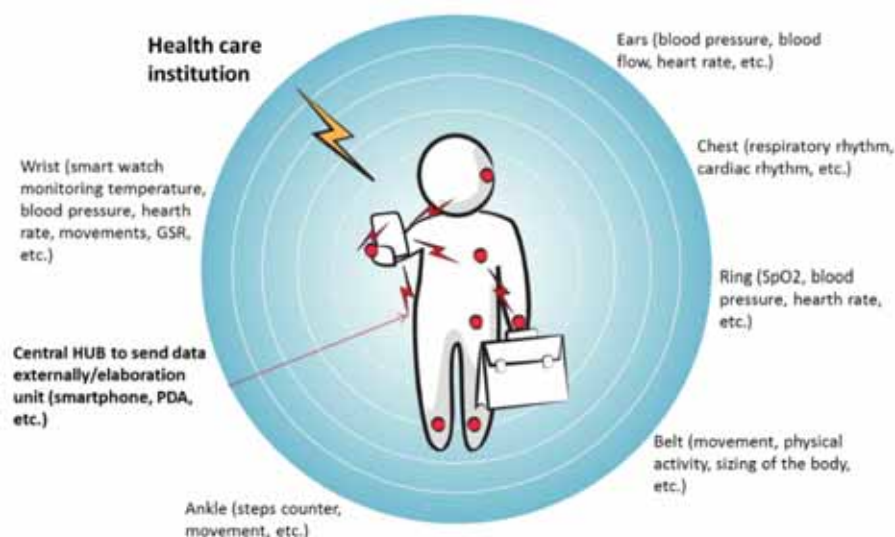


Figure 20. The list of possible sensors that can be measure on a Body Area Network (BAN)

In parallel, as reported in Figure 21, the differentiation of products follows the clear identification of users' preferences and the clustering of the sensors according to the market usage trends: wrist bracelets are among the most used wearable products, followed by arm, leg and body sensors.

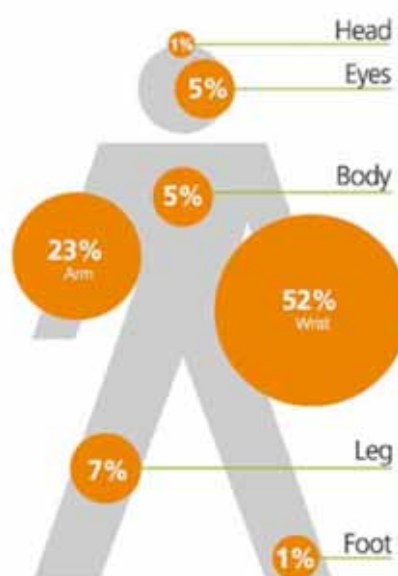


Figure 21. Distribution of the sensors on the body, according to "WearableThis" infographic data (<https://www.pinterest.com/pin/82401868156853162/>)

Summing up the real essence of the wearable technologies is well summarized in the following sentence:

"The implications and uses of wearable technology are far reaching and can influence the fields of health and medicine, fitness, aging, disabilities, education, transportation, enterprise, finance, gaming and music. The goal of wearable technologies in each of these fields will be to smoothly incorporate functional, portable electronics and computers into individuals' daily lives" [WearableMag, 2013].

Speaking of Digital Health and personalized health services, the Self-tracking, Seamless Engagement and Personal Efficiency improvement are the new frontier and the Personalized Big-Data Spaces are the data counterpart supporting such a vision [Kalakota, 2013]. The Personal Big-Data space is the virtual data space composed by all the data sensed by the internet of things sensors, either directly worn by the seniors (e.g., as a multisensory bracelet) or installed in their houses (for example). The list of instrumented environments from which these data are coming is everyday longer, including smartcars, smart offices, etc.

The increased importance of PBDS is a revolution that started with the introduction of a great number of wearable and unobtrusive well-designed and integrated sensors on the mass-market (for example integrated into a unique fashion bracelet). Once, the measurement of a big number of biomedical data was not easily feasible with affordable and yet usable and well-designed sensors. Thanks to the evolution of this market segment, the PBDSs are nowadays a central element of any personal healthcare systems, more than it was in the past. The development of Assisted Living systems is one of the evolutionary aspects that the healthcare system is facing since few years. *"Moving to the Humans is the new wave"* [CEFRIEL, 2010] A long-term radical change of perspective happened in the health services since few years that goes under the name of "Patient Ecosystem". It consists in the evolution from the simple hospital care to a network of services for patients provided in home environments, mobile contexts through different channels and new technologies and homes.

Inside the structure of a modern patient ecosystem (source PRECIOUS project), we can distinguish four phases:

1. Risk factor data collection through an heterogeneous collection of biometric data, performed in the trials
2. Data processing supported by trials data
3. Analysis and modelling of data for the evaluation of lifestyle trends and the risk analysis for frequent fallers problem,
4. Feedback and responses which will be the base of the novel awareness methodologies whose aim in general is the injection of behavioural changes



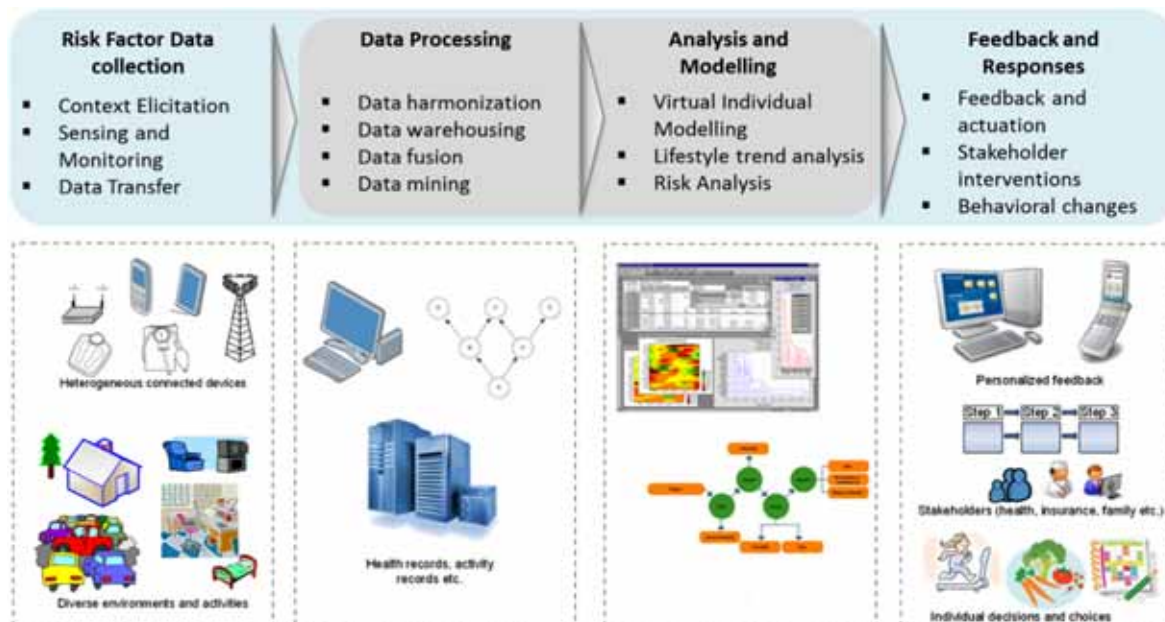


Figure 22. Reference system for Lifestyle Management and Diseases Prevention (source: PRECIOUS project)

This type of approach is being actively researched since few years, but just recently, the market shown to be ready for a wider adoption, due to the increasing market of wearable devices and also the appearance of different widespread ecosystems: specifically Apple Healthkit and Google Fit.

The phenomenon of quantified self hence, is not only a matter of over-usage of biometric wearable systems, but also gets with it a fundamental change in the health services and it is a core part of the mHealth revolution.

3.3 MOBILE BIOMETRY

For further information see Appendix A: High Level Scenarios section o

Thanks to the wide adoption of smartphones and wearable terminals, the low cost biometry is increasing considerably its market impact. Many affordable sensors are appearing on the market embedded into the most modern mobile terminals as well as into the wearable devices. Compared to classical biometry, this new trend creates a completely different application area because usually its typical application is in a heterogeneous context and in external environments. In general these days we record the evolution of the so-called “Mobile Biometry” as a new branch of biometry whose characteristics are:

1. Tight integration with mobile terminals such as smartphones or wearable Internet of things devices
2. Low cost of sensors
3. Typical usage for personal authentication either locally or for remote services (e.g., m-banking) in heterogeneous contexts. [Gelb, 2013] [Hosseini, 2012] (The first paper surveys 160 cases where biometric identification has been used for economic, political, and social purposes in developing countries, the second one m-surveys 121 banks in the world which use biometrics in their operations)



4. Data fusion and integration of different biometric data

All these aspects can be summarized into the modern definition of the biometric applications:

"A biometric is a physiological or behavioural characteristic of a human being that can distinguish one person from another and that theoretically can be used for identification or verification of identity."

Where, beside the classical physiological measures (Iris, Fingerprints, Hand, Retinal and Face recognition), we find the behavioural aspects (Voice, Typing pattern, Signature, Context, Mood ...).

"A biometric that is based on a behavioural trait of an individual. Examples of behavioural biometrics includes speech patterns, signatures and keystrokes. Contrast with physical biometric".

Figure 23 reports the corresponding evolution of the authentication methods as a function of the asset value that is being protected and the corresponding authentication level. The combined biometry and the behavioural are reported as the most secure methods nowadays available for protecting important assets and, thanks to the large availability of the smartphones and wearable terminals, also foreseen to become the most widespread in the near future.

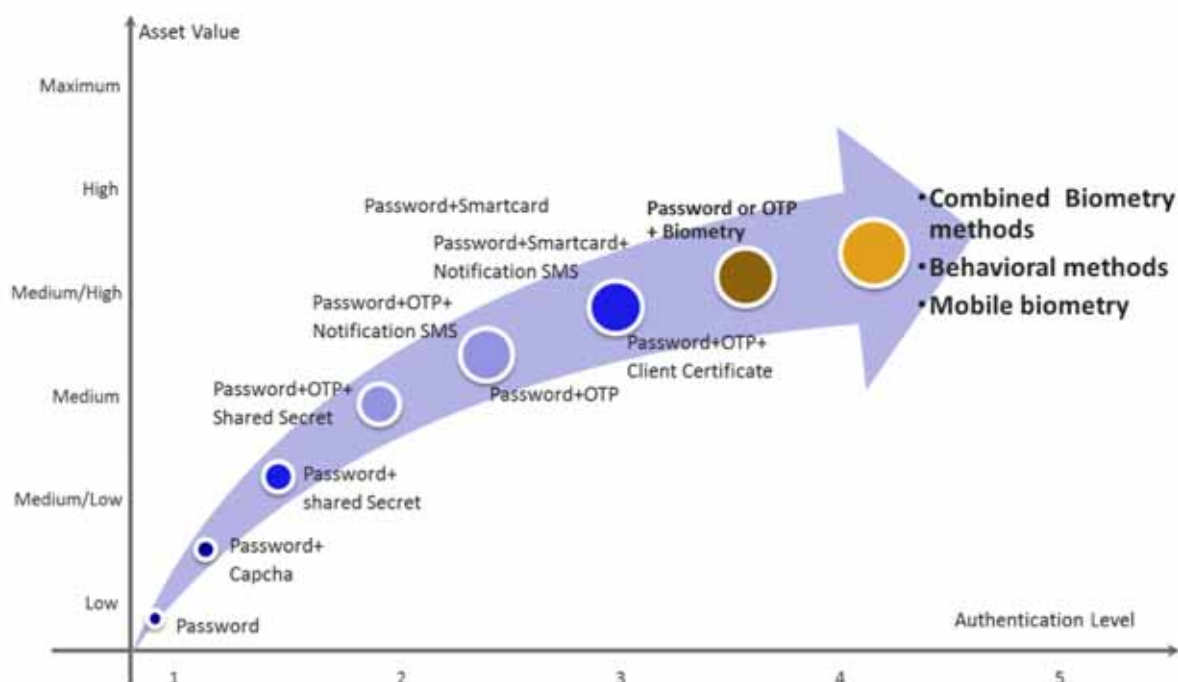


Figure 23 - evolution of the authentication methods compared to the value of the asset being protected

Above bullets are all contributing to the general weakness/problems of mobile biometry: the low cost of sensors and the general application into heterogeneous contexts lead to a poor quality of the biometric sample (e.g. acquisition under the sun light of the face through the camera of the smartphone). This general poor quality of data, which usually would lead to a non-negligible error rate (high FAR and FRR indexes), is somehow compensated by the larger number of sensors present on the terminals. These terminals allow for a multi-factorial acquisition of the biometric data: fingerprint, voice, face, typing patterns etc. All these data are nowadays combined into algorithms

on-board or remotely available to infer behavioural patterns. This new trend in biometry leads to a new flourish of behavioural based application and authentication methods.

Figure 24 reports the overall view of the **MoBio**, the combination of different biometry methods with behavioural patterns.

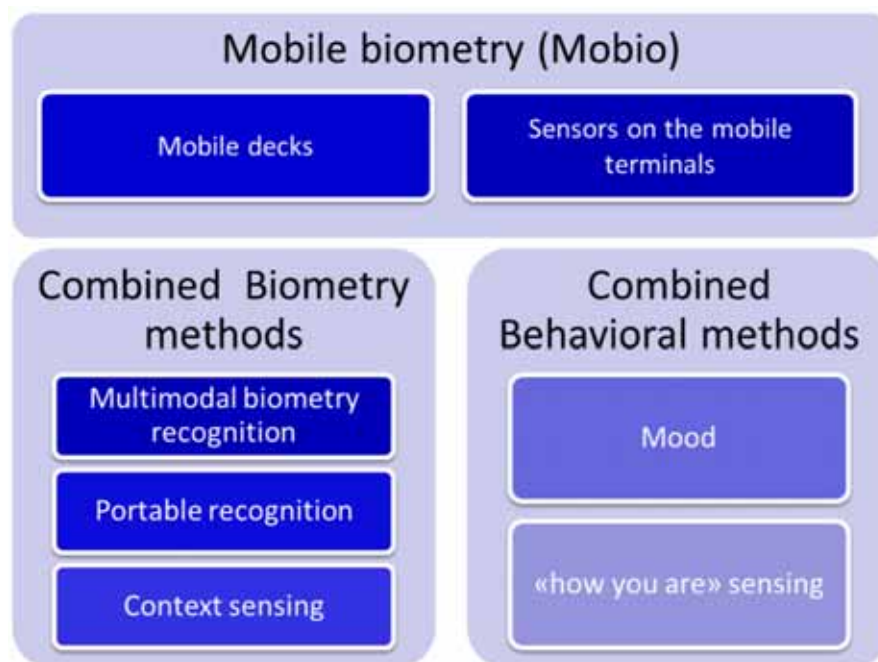


Figure 24 – the modern classification of the biometric methods and the leading role of mobile biometry

Biometric authentication methods are rapidly moving to **mobile authentication channels**. This new trend implies new problems and advantages. Summing up, the problems tied to this evolution are:

- Environmental
 - open-air authentication (e.g. sunlight, wind)
 - low quality acquisition media (e.g. low quality cameras or mic)
- Low network bandwidth

Which are balanced by several new opportunities:

- Integration of sensors (e.g. GPS, accelerometer, context analysis)
- Combined Biometry methods (e.g. voice, fingerprint, face). Direct biometric authentication methods are asymptotically improving. Single methods reliability is not good enough for mass-adoption and the mobile terminals offer different biometric channels. This leads to combining different biometry method with context information.
- Combined Behavioral methods (e.g. “whenever you are”, “how are you”). Due to the asymptotic improvement of the single biometric methods we observed the above mentioned combination of different sensors. Among these there are also some second level biosignals, inferred from the physical data, such as mood sensing and tracking of behavioural and mood

to improve authentication and track the real identity of the person behind a terminal: multiple factors are combined to score the likelihood that a user is, in fact, who he or she claims to be online [BehavioSec][AdmitOne].

By the security point of view, the interesting new application is that the context and all the sensors are integrated into the authentication process.

In recent years, the evolution of the Identification as a Service (IDaaS) helped this trend compensating the limited computational resources of mobile terminals. As a matter of facts, the complexity of the algorithms became too complex, due to the integration of the different sensors and the compensation of environmental noise.

IDaaS are software products that do advanced biometrics just using hardware sensors on the terminals. [CVMetrics] [PasswordBank].

Figure 25 shows the overall schematization of MoBio and underlines pros and cons.

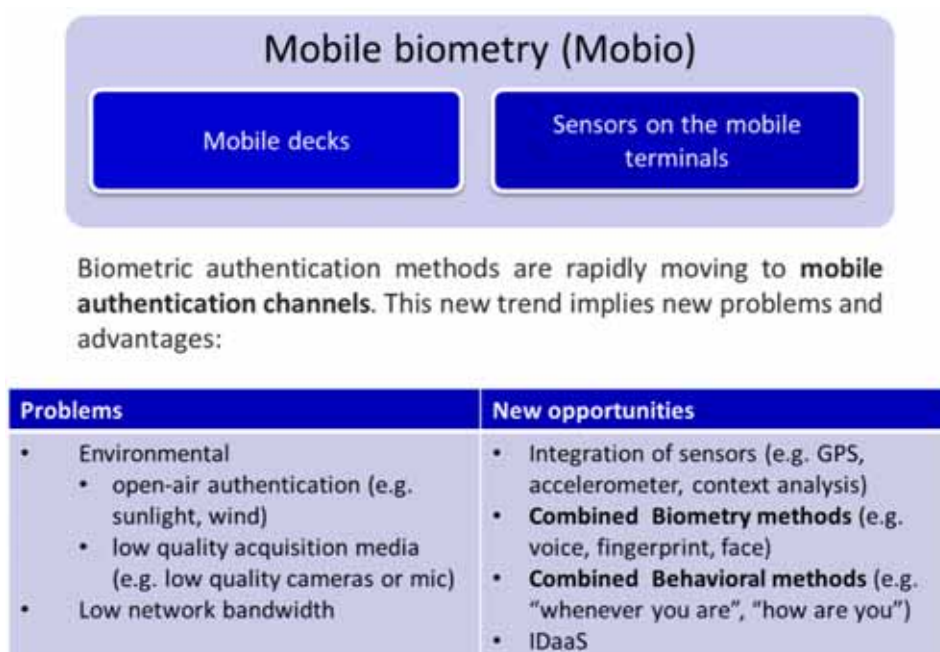


Figure 25 – Opportunities and problems of the MoBio

Figure 26 shows a larger scenario where the mobile biometry integrates with other data sources. As a matter of facts, the mobile biometry evolution intersects with other big trends such as mobile health and the **personalized big-data spaces** because it shares with these other scenarios the same need of measuring multiple biometric data. In this wider scenario the data coming from the wearable (users state) and the on-device sensors (system state and world state) contribute to a more precise context sensing together with other types of data (situational state) [Schmidt, 2014]. The application of mobile biometry for security mainly ties to new authentication methods, usually called no-passwords authentication, where the system recognizes the user and its behaviour and grant access to important assets only after it has enough confidence that the user is who he/she claims to be.

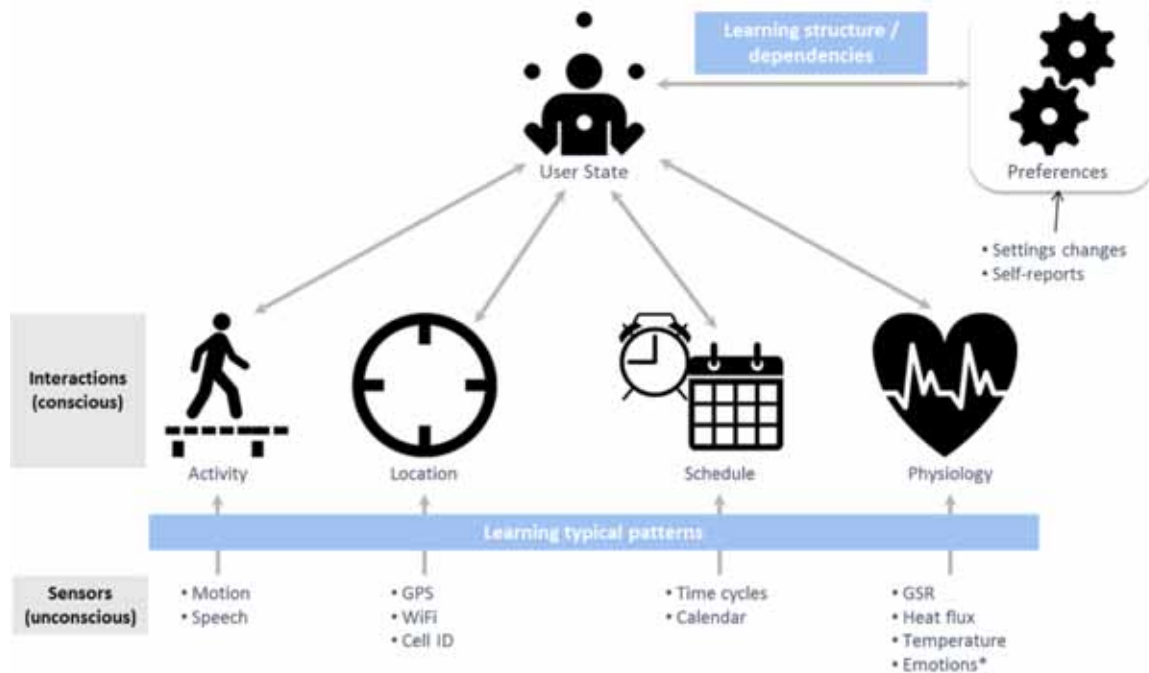


Figure 26 –Integration of MoBio with context aware systems and integration of different data sources.

3.4 UNMANNED SYSTEMS

For further information see Appendix A: High Level Scenarios section 4.4

As reported in [WorldScientific] “An unmanned system is a machine or device that is equipped with necessary data processing units, sensors, automatic control, and communications systems and is capable of performing missions autonomously without human intervention. Unmanned systems include unmanned aircraft, ground robots, underwater explorers, satellites, and other unconventional structures.”

Unmanned systems (US) is a general concept that comprises a wide array of specific types, such as unmanned ground vehicle (UGV), unmanned aircraft system (UAS), autonomous underwater vehicle (AUV), unmanned aerial vehicle (UAV), remotely piloted aircraft systems (RPAS), unmanned surface vehicle (USV), unmanned undersea vehicle (UUV) or unmanned spacecraft (USC).

Unmanned systems are being used both for military and for civil tasks such as reconnaissance operations, fire extinction, surveillance or delivery of objects in commercial transactions. The main benefit of these systems is that they are extremely suitable to avoiding tedious task or to perform dangerous operations, eliminating the risk that these tasks may pose to human lives [Lewis, 2004]. As a consequence, the use of these platforms is consolidating at a steady pace. Different market studies anticipate an explosive growth of the use of US for different markets and applications. There is a well-defined market segment for defense applications and another potential huge segment of civil US with multiple applications in other sectors.

It is expected that these markets and applications will not emerge simultaneously but experience will permeate between different sectors as US are increasingly used. Government users are expected to be the first adopters within the civil market, based on knowledge of past and ongoing activities.



The figure below presents a classification of possible users within the civil-government market:



Figure 27. Classification of possible users

During the last decade, unmanned aircraft systems (UAS) have become the fastest growing sector in the aerospace industry, with growth rates of up to 20%. This makes UAS a success story of US technology. Current perspectives are that this trend will be at least maintained or most likely increased over the coming years. This growth has been restricted largely to the military systems and operations, which limits applications to a reduced number of scenarios.

In recent years, several organizations have carried out a number of initiatives (some of them still ongoing) aimed at exploring the real benefits that the UAS can bring to the civil market, and as a result, it is generally agreed that those benefits range from the evolution of existing products and services by optimizing the capabilities delivered and cost incurred, to the implementation of completely new services which cannot be achieved by using current manned systems. A big percentage of these services are envisaged to be delivered by using small UAS, which has brought the attention of the industry and the European authorities to provide a short-term solution to insert this small UAS into the European airspace.

One of the most prominent examples of UAS is the RPAS, which are UAS that cannot operate out of line of sight and at altitudes where a person on the ground must readily see them. The next Figure shows the RPAS market growth for the forthcoming years by vertical markets.



Figure 28. European Civil and Commercial RPAS Market

In the particular case of RPAS, Airborne surveillance capability offered by RPAS aircrafts can provide a differential added value in citizen safety and security, infrastructure protection and disaster management scenarios. Thanks to their greater agility, increased persistence and reaction capacity, RPAS can also significantly extend the intelligence-gathering capabilities (e.g. situation awareness) in rough or inaccessible terrain, such as mountainous regions and also at sea beyond the coastal horizon, providing explicit identification of possible threats. This will allow users having this surveillance information on a more frequent, reliable and cost-efficient basis.

RPAS aircrafts offer excellent flight characteristics and robustness in rough conditions and require little support base infrastructure. In its simplest configuration they can be operated by just a single person as responsible of the mission and of the flight remote control of the aerial vehicle and by another person taking care of the payload installed (e.g. EO/IR, SAR Radar, LIDAR, etc.).

In response to this promising market trend and outstanding capabilities, a huge effort is being performed in both Europe and the United States to develop the necessary standards and regulations to integrate RPAS into the airspace in a safe and efficient manner. RPAS have still a number of challenges to overcome such as incorporating airborne standards into their development, developing “see-and-be-seen” (sense and avoid) technology, and competing with existing manned aircraft capability for their business. Aspects as limited operational range, RF allocations for control links, privacy concerns and meeting security and regulatory requirements need to be taken into account.

Such vehicles use primarily GPS receivers for positioning and guidance. Thus, there is a growing concern about the impact on the operation that could come from attacks, intentional or not, against the civil navigation signals, for example by spoofing or jamming. Such attacks have been extensively studied from a theoretical point of view, and news involving real attacks is becoming increasingly common.

RPAS run even the risk of being hijacked and used as weapons against other airspace users or targets on the ground. This could be achieved by means of electronic attacks (e.g. jamming or spoofing of data links or satellite navigation systems) causing serious hazards to air safety. A spoofing attack attempts to deceive the GPS receiver by broadcasting fake GPS signals. These signals may be modified as to cause the receiver, and hence the RPAS, to think to be located at a different location



or time. On the other hand, a jamming attack can interrupt / block the GPS signals and thus make them non-operational for the use by the vehicle.

3.5 SMART TRANSPORT (AUTOMOTIVE)

For further information see Appendix A: High Level Scenarios section 4.5

The Transport Challenge is allocated a budget of €6 339 million for the period 2014-2020 and will contribute to four key objectives, each supported by specific activities [H2020_EUC].

“Transport is on the brink of a new era of “smart mobility” where infrastructure, transport means, travellers and goods will be increasingly interconnected to achieve optimised door-to-door mobility, higher safety, less environmental impact and lower operations costs. In order to achieve efficiency at system-level, targeted efforts are needed to develop and validate new solutions that can be rapidly deployed, notably on corridors and in urban areas. They will address transport means and infrastructure and integrate them into a user friendly European transport system of smart connected mobility and logistics. Research and innovation on equipment and systems for vehicles, aircraft and vessels will make them smarter, more automated, cleaner and quieter, while reducing the use of fossil fuels. Research and innovation on smart infrastructure solutions is necessary to deploy innovative traffic management and information systems, advanced traveller services, efficient logistics, construction and maintenance technologies.” [APRE].

The EU has devised a strategy for integration of the EU transport area, towards the creation of an effective transport system that is resource-efficient, competitive and environment-friendly. According to the 2011 EU White Paper on Transport Strategy, the European Commission: *“adopted a roadmap of 40 concrete initiatives for the next decade to build a competitive transport system that will increase mobility, remove major barriers in key areas and fuel growth and employment. At the same time, the proposals will dramatically reduce Europe's dependence on imported oil and cut carbon emissions in transport by 60% by 2050.” [EC_WhitePa].*

By 2050, key goals will include:

- The drastic reduction of conventionally-fuelled cars in cities,
- 40% use of sustainable low carbon fuels in aviation,
- at least 40% cut in carbon emissions from shipping.
- A 50% shift of medium distance intercity passenger and freight journeys from road to rail and waterborne transport.

The emergence of advanced satellite navigation is a major enabling technology that supports the development of Intelligent Transport Systems towards achieving the goals set by the EU Strategy. A multitude of transit agencies to offer trip planning services either through their own website or through Google Transit. An apparent trend in new trip planners is that they provide aggregated information from a number of different transit agencies. Multimodal trip planners that feature both driving and public transit appear to be more common internationally, particularly in Europe where several Multimodal trip planners are available as the result of European Projects such as OPTI-TRANS and START.



The development of the General Transit Feed Specification (GTFS) by Google, has increased the availability of transit data, especially since GTFS is open source and available to any interested entity. Though not competing directly feature-for-feature, GTFS has been substantially more widely-adopted than the alternative Transit Communications Interface Profiles (TCIP) standard developed by the American Public Transport Association (APTA) and the Freight Transport Association (FTA). The rapid adoption of GTFS over TCIP is largely due to its relative ease in describing, implementing, and maintaining the data feed. Specialized tools that enable small transit agencies to enter, export and host the transit data needed to put their transit information on Google Transit quickly emerged (e.g., Transit IDEA project), following the success of the GTFS schema.

Furthermore, the introduction of the OpenTripPlanner as Open Source software provides the opportunity for everyone to build on this tool in order to create a customized trip planner. OpenTripPlanner uses royalty-free geographical data provided by OpenStreetMaps and it is able to import GTFS formatted data.

New trends in Multimodal transportation advisor systems include the provision of interoperability with non - typical transportation means (such as Taxis and car pooling systems) and personalized or special-purpose journey planners, by implementing Semantic Web technology combined with Geographic Information Systems in order to offer personalized services based on user preferences and temporal data. An ontology-based approach allows to link, structure and share data in order to obtain a personalized result based on user preferences in a timely fashion, utilizing real time data and optimizing the final outcome (Itiner@ project) [H2o2o_EUC].

The aim of Europe is clearly to foster the evolution of the smartcars market. Despite this long-term target there are still some critical issues that is worth to consider especially concerning information security aspects. The automotive is expected to increasingly see the adoption of Context aware systems and immersive interfaces (e.g. augmented reality) where the IT complexity is disappearing. This poses new threats and approaches to security which is largely to be investigated.

To help clarifying the context, the picture below represents the interactions of the basic elements that interact within Smartcar scenario

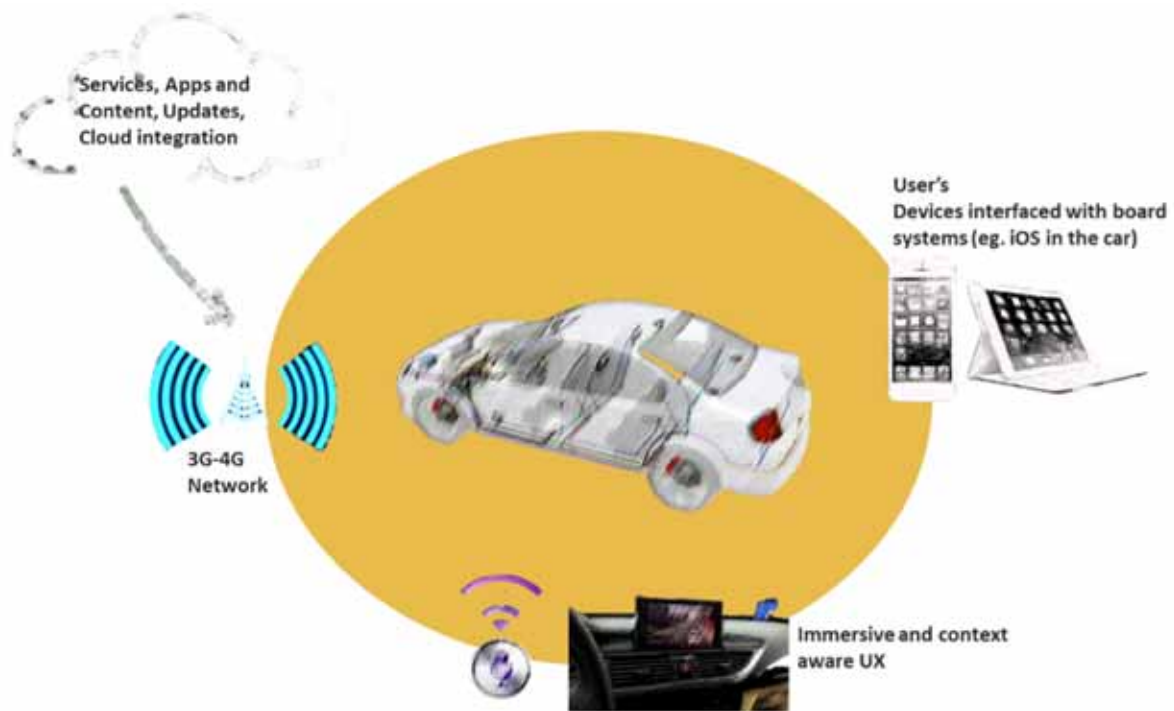


Figure 29. Smartcard connections scenario

Modern cars are increasingly becoming complex IT systems and are moreover always connected. This exposes these systems to all the security problems already known for online systems (malware, DoS, attacks). The software and IT architectures must be developed from scratch using a proper approach because of the peculiar aspects of the car industry and because the safety and security in this context are mixed together. In almost any modern software system, exposed to external menaces the Secure Software Development Lifecycle (SSDL) is a stable and well-known best practice, which has still largely not been adopted in the automotive world. One reasonable solution is to re-think them with a trusted platform approach, like Apple is also doing with their “iOS in the car” system (the iOS in the car funding concept is that it is a fully trusted platform).

Like any other complex IT system, also in-car software needs to be updated. Nowadays used solutions are either OTA or tokens (e.g. USB sticks or pen-drives), but whatever solution it is used, there are specific security problems that must be solved. A wrong or malicious update of the onboard systems could lead to serious problems, malfunctioning and most of all safety breakdowns.

Any communication channel in complex IT services must be properly secured, this means proof of the source and the destination, privacy of the channel and data integrity. All these requirements can and must be embodied in the way the car communicates with external data sources, to prevent leaks or damages. Modern solutions derived from mobile applications, can be adopted in automotive world.

Automotive electronic control units (ECUs) control a broad range of functionalities including brake, powertrains, lighting, door lock, entertainment etc. The capability to distribute SW updates on the field and over-the-air will become critical for both quality and security performances. ECUs are interconnected by common wired networks and usually by CAN busses. While this architecture proved to be efficient in terms of performances and costs, it opened the door to a novel kind of potential attacks with a potential impact on security.



For example, performing over-the-air updates on car ECUs open a new flaw for security aspects. In fact it has been already demonstrated that modern cars can be hacked since they are now mini networks where both crucial and less crucial ECUs are all connected to each other (via Controller Area Network). They can also be hacked via the usage of connected mobile devices.

The following list has the aim to sum up the main critical aspects related to smartcars information security

- Existing standards are not really tested against real threats and attacks, often no real assessment have been done on the existing protocols,
- The market is neither really uniform nor standardized and each producer uses its own proprietary solutions to improve the overall smartcar security [Bilton, 2015].
- The appearance on the market of new complete ecosystems (e.g., Google in the car, iOS car) poses new problems to the real security of smartcars
- Autonomous driving is coming on the market
- Several new attacks have been exploited and demonstrated for cars nowadays on the market
- Safety and security and cybercrime are colliding in this particular area of business: cybercrime activities could easily lead to safety disruptions/problems.
- Activity aims to support automotive industries (OEMs, supplier) to protect and improve their products [Khandelwal, 2015].

3.6 LOCATION BASED SERVICES

For further information see Appendix A: High Level Scenarios section 4.6

Central to the concept of Context-Aware Computing, is the availability of positioning data both in indoor and outdoor environments, enabling a variety of novel Location-Based Services (LBS) [Schmidt, 2001]. The advantages of LBS can be leveraged to offer real-time navigation information to the user and can be used within the context of efficient transport, logistics and asset tracking, emergency response, location-based advertising etc. Through the accurate estimation of position data and the design of intelligent services based upon them, LBS aim to improve our interaction with the physical world.

Mobile location-based services are based on locating the cell phone of a mobile user, by means of the cellular network infrastructure (e.g. GSM [Varshavsky, 2006] or CDMA localization [Caffery, 1998]) or by Global Navigation Satellite Systems (GNSS). The Global Positioning System (GPS) [Groves, 2013] is the most well known example of GNSS, mostly due to the integration of GPS receivers in modern Smartphones. GPS has been developed and is currently being maintained by the United States Armed Forces. The Russian GLONASS (“Globalnaya Navigatsionnaya Sputnikovaya Sistema”)[GLONASS] is another alternative to GPS currently in operation. Two additional GNSS systems are currently being developed and are expected to be fully operational within the next years, namely the European Galileo system and the Chinese COMPASS [ESA, 2011][CSNO, 2011].

Indoor location-based services are usually provided by a separate, dedicated system, which requires the existence of specialized infrastructure in the area wherein the users move and interact with each other. Dedicated infrastructure in indoor areas is necessary, as mobile LBS are not as accurate in an indoor space.



The following figure illustrates a high-level overview of the architecture of a location estimation system.

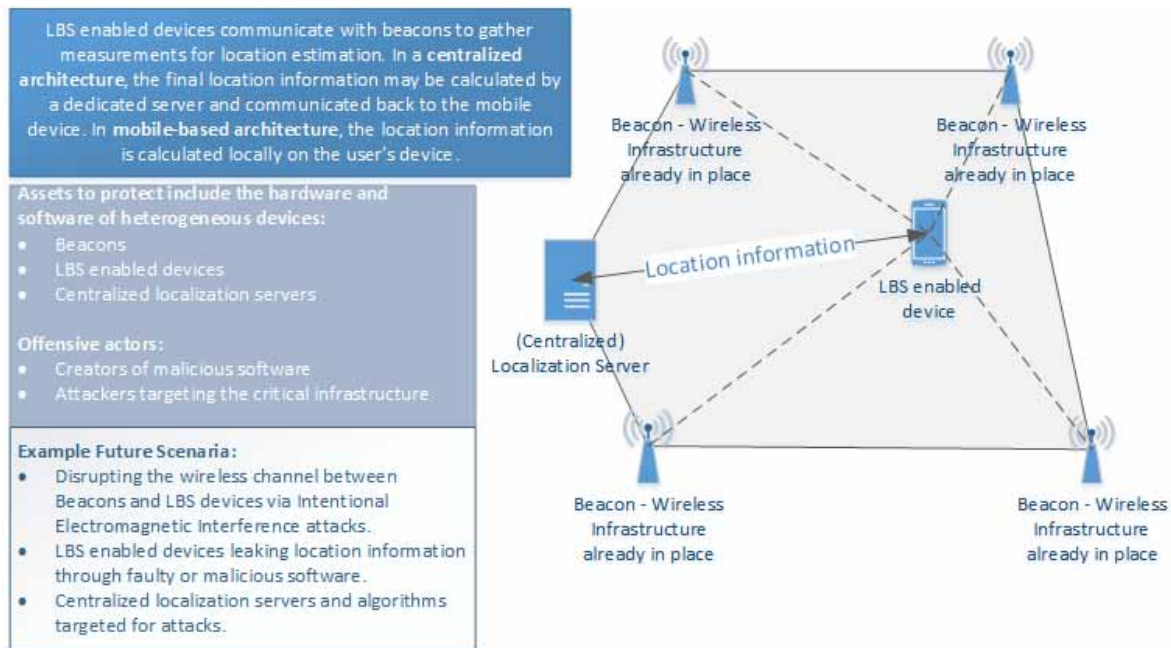


Figure 30. High-level overview of a location estimation system architecture

Fixed-infrastructure beacons are set up in an area wherein location based services are required. Examples of fixed infrastructure beacons are the GPS satellites, WiFi routers that are set up in a campus to provide an indoor service, cell towers etc. Mobile devices may be specialized handsets, Smartphones etc. that are carried by the user. Mobile devices communicate with the infrastructure beacons in order to generate measurements used to infer their position. Measurements refer to characteristics of the wireless signal, such the reported Time of Arrival, Signal Strength, Direction of Arrival etc. The implementation of localization algorithm defines the kind of measurement that needs to be collected.

A location estimation system can feature centralized or mobile-based localization architecture. A **centralized** architecture is particularly useful in asset tracking and emergency response, as a central dedicated server is used to estimate the position information. A **mobile-based** architecture means that the location information will be calculated locally, on the user's handset and is usually preferred when there is user demand for privacy or large scalability.

In the case of LBS, there are multiple assets to protect, including the software and hardware of the related components (the beacons, the mobile LBS enabled devices, centralized localization servers etc.) The protection of the wireless channel against intentional electromagnetic interference attacks is an additional issue that tends to be overlooked. Privacy concerns also arise since the location data of a user in many cases need to be protected.

For example, cellular network operators are required to set centralized localization services for the purposes of emergency response. In this case, privacy and security concerns were identified early on and led to a variety of government mandates and regulations that ensure the protection of location information as personal data. Faulty or malicious software on a user's mobile device, however, can lead to leaks of location information and compromise the privacy and security of the user.



With the ever-increasing number of LBS-enabled Smartphones and considering society's growing reliance on LBS, it becomes clear that positioning systems and their individual components should be hardened against cyber attacks.

3.7 SOCIAL NETWORKS

For further information see Appendix A: High Level Scenarios section 4.7

Social network is a term that has achieved great popularity today. Although the term was coined in 1954 by J. A. Barnes, today social networks represent a phenomenon particularly interesting to analyze. Social networks are networks made up of people, linked by relationships that unite them. Most people are linked by a relationship if they interact daily but also sporadically, if they know each other or share common interests.

Social networks are based on the so-called 'Social Media', i.e. computer-mediated tools that let individuals the creation, manipulation and sharing of information of any kind (such as pictures, videos, links, opinions and so on) inside networks of virtual communities. Being a 'technological trend', Social Networks are not a new kind of technology because they are not a technology itself. The main underlying technology is the well known version 2.0 of World Wide Web, that is Web 2.0 (or Dynamic Web), but Semantic Web technologies (as in Web 3.0) are also used to represent, track, store and elaborate all the different kinds and lots of links between people, with the aim, always more often, to obtain individual's profiles. But social media depend also on mobile technologies to highly increase individual interactions and manage entire communities. The communication paradigm to understand here is that the transmission system model is not 'monologic' (i.e. one single source to one or multiple targets) as in traditional media, but it is 'dialogic' (i.e. multiple sources to multiple receivers). As Murthy Dhiraj said, *"Social media has been broadly defined to refer to 'the many relatively inexpensive and widely accessible electronic tools that enable anyone to publish and access information, collaborate on a common effort, or build relationships'"*.

Social interactions can also be described by the so-called 'peer effect' studies, where a peer group is defined as a social group (or a primary group) of people with similar or same interests (like in 'homophily'), knowledge, social status and age.

3.7.1 IMPACTS AND STATE OF THE ART

The impact that social networks had on our society is very strong as it has affected the economy [Jackson, 2011], the exchange of information, the search for new jobs, the introduction of new products and technologies, etc. Social networks are thus a particularly interesting field of study in various disciplines ranging from economics, technological innovations and cultural events.

The study of networks from an economical point of view contemplates the following two important aspects: understanding how economics is involved in social network structures; the fact that modern economic tools are very useful to analyze network influence.

Social networks also influenced (and are still influencing) labour market very much: in last years they became an important information pipe to access jobs, and this is considered an evidence for anyone. As observed by Myers and Shultz, a relevant percentage (62%) of the interviewees have



found about their first job through a social contact, and this kind of trend is not specific to a particular industrial sector, but it is typical.

But social networks play an important role in other fields, also, as learning, information diffusion, political/ ethical opinion and so on [Cropf, 2007].

A social network, because of its intrinsic nature, is also used as vehicle of information; it surely enables information (true or false) dissemination among ‘connected’ people. Characteristics like this one can have (and usually have) implications on human decisions, so they can influence people decision making. Moreover people’s friendships exist on a basis of similarity, and this can be called ‘homophily’, so an individual is friend of another if (and maybe only if) this last shares something with him/her. The shared ‘thing’, or trait’, can result in the purchase of a product. According to ‘Social Media Marketing Industry Report 2014’ social media are considered important by 92% of marketers for their business; blogging will be inserted in future plans by 68% of marketers; original content (in written form) is most important for social media marketing for 58% of marketers; 89% of marketers are looking for the best tactics on how to attract and obtain audience.

3.7.2 CYBER SECURITY RISKS ASSOCIATED WITH SOCIAL NETWORKS

As said, social networks can really and easily influence masses and/or individuals; moreover they can constitute a large part of an organization’s business. These facts surely can raise criminal and terroristic intentions. In effect social networking sites are a prime target for cyber criminals. Maybe the simplest attacks are spam and hoaxes executed by sending links to social contacts (i.e. on Facebook, Twitter, LinkedIn, etc). A form of hoax can be the obfuscation, or shortening, of URLs on social websites as well as on e-mail messages.

A threat for an organization could consist of what an employee might disclose through the use of social networks.

According to the Cisco 2013 Annual Security Report, online threats are mostly concentrated on mass audience sites, including the still discussed social media; the report showed that online advertisements are 182 times more likely to deliver malicious content than pornography sites, just for example. There are also reported, in Global Risks 2013 Eight Edition, results on the risk of rapid dissemination of false information. There have been several incidents where false information exchanged over internet produced serious consequences on people’s life.

Moreover cybercriminals have been using social engineering techniques based on social media to prepare and execute attacks against either users or organizations. In this kind of new approaches FBI also has been involved. Personal and sensitive user data have been stolen. In the (recent) past mass e-mail letters with misspelled messages were used, but nowadays criminals make use of social networks in combination with common and well-known social engineering techniques to achieve their aims. Today, defence against a typical social engineering attack is very difficult because of human / psychological factors. As Frank Nagle (senior consultant at MANDIANT and an investigator on a striking real case) said, “Employees in these social engineering attacks are really on the front lines. When email is really targeted, it is tough to come up with technical means so you need to rely on employees to be educated and on alert for those types of things.”



3.7.3 CONCLUSIONS

A key concept here could then be the (eventual) ‘influence’ on an individual’s behaviour by that one of his / her social contact, in other words the mutual correlation, strong or weak, among social networks’ individuals. Research on this last topic is still open.

However, to properly study the dynamics of social learning, experimental analyzes on collected data have to be done, as proposed, for example, by Conley and Udry. Another approach involves the use of structured predictive models.

Findings like discussed ones make understand better this complex and large social phenomenon, thus making thinking over different human behaviour areas such as ethics, politics, education, (cyber) security, psychology and more, therefore not only economics or marketing.

For the depicted peculiarities of such a trend (maybe a really ‘social trend’), social networks are also criticized; some critical aspects may include disparity, reliability and relevance of information exchanged, privacy issues and effects on interpersonal relationships.

3.8 BYOD

For further information see Appendix A: High Level Scenarios section 4.8

The term BYOD refers to the corporate policies that allow its employees to use their personal devices (Smartphones, tablets and PCs) to do their jobs, accessing through these to the business data and systems.

In the 2015 and future years, technology is expected to keep up with business growth. Employees are more and more free to choose the type of the device and operating system to use for work, as well as they require the capability for fast and smart delivery of content and information. A strong example is the projected uptake of tablets: there is a growing consumer expectation as the device became widely used within large and small business, as well across the public administration.

Tablets provide portability and a much easier way of use than traditional laptop, and this, combined with a major interest and demand for high speed access to information anytime and anywhere, is expected to drive large adoption in all the business areas through the 2015.

3.8.1 BYOD STATE OF THE ART

In a recent survey it is estimated that that 200 million users of 360 million users will be using their own personal devices for work. More than 85% of Malaysians use their personal devices in the workplace but only 26% of them are provided with sufficient support from enterprise’s IT department. This is also a consequence of the “consumerization” of the IT devices and services that change the way ICT support the business operations. It is to be considered the following approaches for BYOD:

1. give the enterprise device to the employee;
2. add the owned employee’s device to the enterprise device;
3. replacing the employee’s owned device to enterprise devices.

The most important thing to consider is to provide effective solutions by which the employee can enjoy the IT services not just limited to enterprise device and working hours. On the contrary, it should allow anything concerning both work and private tasks, anywhere with internet or WLAN.

The benefits from the adoption of BYOD could be:

1. boosting productivity;
2. cost reduction;
3. an improved employee's morale.

Employees, especially the youngest, are very happy to work on social network interactively while the companies can provide more value-added ICT services to employees without allocate extra budget for this expenditure.

BYOD has been lately put beside another alternative paradigm: COPE Corporate Owned Personal Equipment. COPE is often traded as a solution for most of the BYOD problems, first of all the fact that being the terminal a property of the enterprise it is not possible for the owner to install everything and policy enforcement is easier. However, this alternative approach does not add any extra security because it rather open the doors to more dangerous situation. Companies usually adopt COPE instead of BYOD thinking it's more secure but these terminals are often obsolete or low level and un-patched even if the patches exist because of practical difficulties to distribute patches to all the employees (except if the company adopted a Mobile Application Management –MAM– solution). As a matter of facts COPE terminals are in several cases used as featurephones, phones without any extra application installed and with not updated OSes. F-Secure lately [AppleInsider] underlined that one of the leading trends of infection is precisely to exploit the featurephones, also thanks to the hundreds of exploitable Android bugs.

3.8.2 BYOD AND CYBERSECURITY ISSUES AND CHALLENGES

A survey by SANS reveals that 56% of respondents did not have a policy or any rules regarding to mobile devices. In addition, during mobile application installation or execution, the user is normally required to grant some permission, such as location-based services or phonebook or any other type of notifications. The so called “DAC”(Discretionary Access Control), in other word, the control of resources and services suffers from numerous security vulnerabilities. These vulnerabilities are, in the most of cases, eclipsed by the benefit of the app itself (flexibility, customizability, and so on..). In the recent years, companies have shown more and more increased tolerance and interest for employees in the use of their own mobile devices at work, with the consequence that employees use mobile devices to access confidential information. The problem is the link between the business rules and the rules of access of the DAC. Many third-party apps could expose company confidential resources to a risk. University's researches have proposed various models to improve the mechanism of policies on the mobile devices. For instance, on android phones, AURASIUM is a prototype that enforces some predefined policies. Some companies have developed their own solution to this security problem, such as Apple (www.apple.com/ipad/business/it/byod.html), Samsung (www.samsung.com/global/business/mobile/solution/security/samsung-knox), Symantec (www.symantec.com/). These solutions support the BYOD paradigm. Other solution, such as Samsung Knox, consist of and isolated environment for corporate apps while most of them provide a Mobile



Device Management (MDM) service that block or, in some cases, reset the device that violates the security policy. Those policies, unfortunately, are often based on vague concepts.

For an effective support of the BYOD paradigm, application markets should specify security policies spanning multiple apps, checking whether an apps complies with a given security policy and ensure the app never violates it.

BYOD security can be ensured through the use of specific requirements that must be met before employees can connect their devices to enterprise systems. Among these prerequisites are: verify network access through the use of appropriate strong passwords, prohibit the installation of specific applications that can be dangerous and ensure that all data stored on the devices are properly encrypted and protected. This way can be avoided that the company's data be stolen causing a leak of sensitive and confidential data For access and permission issues, malware such as key logger and cyber attacks greatly increase the potential for unauthorized access.

3.8.3 CONCLUSIONS

If the trend of companies is to shift their focus to the virtual and the "consumerization" of IT, it is inevitable that the BYOD becomes more and more convenient and also a robust solution to the requirements of the ICT agenda. They cannot be neglected and the cost for the solutions must not be greater than the benefits of BYOD. To be adopted BYOD must converge towards a single framework that encompasses the individual solutions analyzed. For this purpose should also be considered the involvement and participation of employees so that they are satisfied the requirements of both business competitiveness but also the demands of personnel who use the devices.

3.9 VIRTUALIZATION

For further information see Appendix A: High Level Scenarios section 4.9

'Virtualization' is a buzzword used to describe a trendy technology, so the term itself depicts well a current trend. In the ICT era every real computing resource, hardware or software, can be virtualized: it is therefore possible to create a non-real version of any specific computing resource ad use it place of the real one. A virtualization framework takes the real resource(s) and gives user a sort of representation of it, providing also a dedicated execution environment. This way you can use 'logical' resources instead of physical ones (hidden by virtualization framework) but you do not notice any difference. So you can have virtualization at various levels: application, operating system, server, storage, devices and so on.

Virtualization is also referred to as 'Green IT', for it helps to reduce hardware and network facilities, thus allowing energy consumption.

3.9.1 IMPACTS AND STATE OF THE ART

In 2013 there were really lots of virtualization technologies that gained a large part of software on desktops. But one of the greatest impacts will be probably on data centres. In fact virtualization can be considered an IT constant in driving the change for a data centre.



The list of attractive impacts or benefits is really long and involve better testing, faster re-deployments and easier backups, just to mention some. New virtualization technologies are coming to markets every day. One innovation in such a sense is the Virtual Storage Area Network (VSAN) and detached storage, which can increase flexibility in a data centre but also gives a greater automation level.

Another notable effect will be evident on reduction of corporate power and cooling expenses.

All this just discussed is only a first generation of future virtualization; a second generation technology will scale up in a better way, so to obtain multiple virtual servers sharing a single operating system license. Moreover virtualization works best with detached storage. This implies a large increase in network traffic, so organizations that want to adopt and implement storage detachment will need strong network management.

Virtualization has given a positive impact on security, also. In fact virtualization improves security because makes it more fluid and, mainly, context-aware. In a data centre that uses virtualization, security can be more made automatic.

3.9.2 CYBER SECURITY RISKS ASSOCIATED WITH VIRTUALIZATION

First of all, existing physical security can't protect virtual system that is systems equipped with a sort of virtualization technology. The reason is simple: physical security devices are not suited to protect virtual infrastructures (such as virtualized data centres and private and hybrid clouds) because of their specific design. Such security controls depend on physical devices that are deployed on data centre's perimeter or on 'physical' networks.

Therefore can arise some challenges but also threats, as follows:

- Physical security devices do not see the virtual network structure
- The hypervisor (i.e. the virtualization manager component) becomes a new threat surface
- No accessing roles: there is only one virtual administrator with all powers
- Machines become files: good for mobility and rapid change, but an opportunity for theft

3.9.3 CONCLUSIONS

Virtualization technology can really scale up and revolutionize many companies' technological infrastructure, assets and, therefore, business. High attention must be surely paid on design the entire solution, but mostly on new security challenges. In fact it is well known that a (cyber) criminal makes use of latest available technologies, so a new challenge in cybersecurity must consider new attack surfaces and foresee new and different kinds of protection.

3.10 CLOUD COMPUTING

For further information see Appendix A: High Level Scenarios section 4.10

The new paradigm of cloud computing is born due to an increasing demand to use new kind of services that can exploit the full potential offered by the Internet and its new technologies. The introduction of cloud computing introduce numerous possibilities to design and create a whole new

range of innovative services: in fact new opportunities can be identified and exploited at the benefit of both the customer and the provider. Among all the new IT trends cloud computing represents one of the major innovation, especially in the way of how services are provided to users. Hardware, platforms and software applications are provided on-demand allocating to users exactly the amount of resources that they need, nothing more and nothing less. This ensure to achieve a great flexibility that goes directly to meet the real needs of the user who has requested it. Moreover all the provided services follow a Pay-as-you-Go policy, which ensure that the user pay for only what his actually using.

The base technique used for cloud computing services is virtualization, by which logical resources are abstracted from the physical resources that are managed directly by the cloud provider. These resources are shared according to a multi tenancy approach by which using the same hardware resources with the same operating system, several software instances are allocated and finally assigned to each individual user, creating in this way an isolated environment for each one. This technique allows to reuse the same hardware resources, thus limiting the overall cost for cloud providers and simplifying at the same time the management of the provided services. Finally, considering that all cloud services are provided through the Internet, an user can access them from anywhere without restrictions, using also the various types of mobile devices commonly available in the market.

3.10.1 ADAPTION TO THE NEW PARADIGM

Thanks to its potential benefits, cloud computing is recording an increasing interest in several organizations, which see in the cloud services an useful mean to increase their productivity while reducing at the same time their costs of use. For example, businesses no longer need to buy, maintain and update a full and complete back-end IT infrastructure. All these tasks are administered directly by the cloud provider itself, which is responsible for ensuring also a rapid and efficient service to its customers. The adoption of cloud services is definitely set to grow considering their strong benefits which are extremely convenient both for the company and for the individual users.

However despite all these benefits, many companies still choose not to rely on cloud services due to some problems that hinder the adoption of these new services. First, users necessarily need of an internet connection without which they cannot access their data and services. Possible outages must also be taken into account because, although many cloud providers have a high rate of availability, they can always experience a service interruption, thereby hindering services access to all its customers. Another important problem is the loss of data control: when a company wants to entrust its data to a cloud provider, inevitably loses also its direct and exclusive control. Therefore it is necessary to put a great trust in the chosen cloud providers considering that company and users are entrusting their personal and sensitive data. Finally there is one of the major problem that hampers the adoption of cloud computing services: security against possible cyber attacks.

3.10.2 CYBERSECURITY AND ITS ROLE ON CLOUD COMPUTING

Although cloud providers have always used the best possible protection against cyber attacks, hackers or other malicious users could succeed to overcome the imposed defences breaking into the internal network perimeter of a cloud provider. This can cause a serious damage threatening the availability, integrity and confidentiality of the stored data. It should be noted that if an attacker is

able to attack successfully a cloud providers he would have access to a huge amount of sensitive and confidential data of several users, held within the data centre managed by the cloud provider.

The excessive concentration of data in the cloud data centre makes a cloud provider an interesting target for cyber criminals, who from time to time find new ways to successfully attack it. Among all the common cyber threat we can highlights the following ones [Sabahi, 2011], [Jansen, 2011]:

- Cloud service used as attack vector: an attacker could use a cloud service to host a malicious script or application from which could start further attacks directed to the cloud itself or against other hosts. At this point, considering that the attack is coming from the cloud, it could use a great amount of computing power at which the attacker may not have access otherwise.
- Account hijacking: even in the cloud this threat is more alive than ever. An attacker could use the different methods of exploitation to hack user's account and access its data and its services. User's privacy therefore can be threaten simply using phishing, sending spoofed emails to the user, password guessing or a great number of other common hacking tactics.
- DDoS attacks: using the rapid elasticity of resources provided by cloud providers an attacker could allocate many instances from which to start its DDoS attacks. This attack is extremely powerful and especially difficult to prevent and mitigate as it is able to flood the target using a huge quantity of unwanted traffic which can prevent the proper functioning of the attacked service.
- Malicious Insider: if the user's or company data is not encrypted before being transmitted to the cloud provider, the internal employees who work within the data centre could have the full access to information and private data.
- Shared resources: although hypervisors are designed to manage and isolate individual instances that are allocated to the users, attackers may found vulnerability in them that allows to overcome the isolation and allow attackers to come into contact with the private resources of the other users.

3.10.3 CONCLUSIONS

Cloud computing has enormous potential and it seems that its adoption will grow rapidly in the coming years. The benefits that it is able to provide are significant and represent a strong evolution of the traditional IT services. Advantages such as rapid elasticity, the possibility to allocate resources on demand, costs reduction, increased accessibility to personal data and services from all over the world represent a really important technological innovation. However, as described above, despite all the potential benefits, there are many causes that hinder the adoption of cloud computing services. The cyber attacks represent especially a constant danger which constantly threatening the users' privacy and security of the various services offered. The decision to use or not use cloud services is therefore an important choice for both the company and the end user, which must be taken according to the actual degree of confidence that they have towards the cloud providers who wish to entrust their sensitive and private data.

3.11 AUTO TAGGING

For further information see Appendix A: High Level Scenarios section 4.11

The term "auto-tagging" or "automated tagging" describes techniques for applying tags, short annotations, to objects on the net that add metadata to said objects. Currently the popularity lies on artificial intelligence based approaches applying methods of machine learning, deriving the metadata automatically from other sources, but also ontology based approaches exist, where all elements are tagged with respect to entries in a database.

The automation is done in order to be able to tag large amounts of data and without human intervention, i.e. the algorithms categorize the data and add metadata based on their own premises. One very prominent example for auto-tagging is done in [Stone, 2008], where he authors personal data gathered from Facebook in order to automatically tag users on photos with their name. While potentially useful, this kind of research opens up privacy problems, especially considering persons who never gave their consent to be tagged on photos.

But also other forms of automated tagging have been devised in the past, often for tagging multimedia files, but also in order to get a better understanding of written text. Especially emotions are very interesting when automatically mining environments like e.g. web 2.0 networks, as detecting sentiment and emotion is very important to understand the real meaning of texts. This also holds true for even shorter messages, where the real meaning is often hidden by special language and emoticons, like Twitter. While tagging of multimedia entries or in order to gather emotions is a rather recent field, automated categorization is much older and very much related to auto-tagging.

3.11.1 STATE OF THE ART

Like many applications of machine learning, auto-tagging is currently undergoing a big trend in the scientific community, as well as in the industry and the wider adaptation of these techniques in various areas. As [Hedden, 2013] highlights, there exist several different approaches, where automated version get the upper hand in current research, maybe due to the fact that large amounts of data are getting available, e.g. through open-data initiatives, but also due to people sharing an increasing amount of personal data on the web. Automated methods excel at a very large number of documents and provide much greater speed in indexing. Still, there are currently limits in what kind of files can be tagged, furthermore, many methods for automated tagging either need a taxonomy or reasonable training sets.

The automated detection of sentiment and emotion in texts, especially considering Social Networks and the Web 2.0, has been tackled too in the past, e.g. by [Francisco, 2006], where the authors explore the possibilities of automated tagging with respect to the detection of emotion and subsequent classification of messages.

Automated tagging is often seen as an application of machine learning, so the whole field of development in this area can be related to the definition of tagging techniques. This is especially true in the area of BigData-analysis, where questions regarding the attribution of metadata due to wrong classification, but also privacy considerations regarding the results of aggregations come into play.



3.11.2 CYBER SECURITY RISKS ASSOCIATED WITH AUTO-TAGGING

The main impact of auto-tagging for common users is in the form of getting categorized by information collecting entities on the web, whether they are intelligence agencies or other individuals. Automated categorization of users based on private data can especially be used during more advanced phishing attacks, where the attacker gains access to either a "friend" of the individuals on a social network and harvests the interests of the individuals, or by simply crawling the web for information on people and assigning them to actual personal profiles. In the case of phishing, some approaches then send specifically targeted phishing messages in order to make the target install either a malware that generates a backdoor, or in order to automatically generate more information from the target [Huber, 2011]. Automated harvesting and enrichment of personal data is especially important in the case of so-called spear phishing, where the attacker does not attempt to phish a large amount of people using techniques as generic as possible, but tries to carefully craft phishing attacks specifically targeting a single person or a small group.

Especially considering the amount of private data that is out in the Internet, auto-tagging techniques can drastically reduce privacy of individuals by making the different information particles combinable. This can also result in false attribution of tags to persons and profiles which may lead to very inconvenient situations and opens up a market for blackmail and related instances of cybercrime. A criminal could also threaten to put out information on the web, so that individuals get tagged with specific meta information that is unfortunate or, in some jurisdictions, even dangerous for them.

Another possible problem for user security lies in the fact that with the amount of information out in the wild, identity theft becomes increasingly possible. While this area is especially trending in the US due to the weakness of using the SSN (Social Security Number) as means for identification, recent developments in the area of e-government may lead to a considerable amount of identity theft in Europe too.

Here one main research question could be, how the methods of auto-tagging could be extended in order to allow for the clearer identification of identity theft, i.e. whether auto-tagging could provide a means for defence against this kind of crime. The same holds true for phishing detection – given good algorithms for the identification of phishing attacks based on auto-tagging (tagging mails and messaged as phishing attacks with a very low false positive rate) could be the solution to an ever-increasing problem in cybercrime.

3.11.3 CONCLUSIONS

While auto-tagging is a very useful technique to “make sense of the web”, i.e. to attribute metadata to unstructured data, thus generating meta structures that can be harnessed in order to exploit these vast amounts of data produces every day by various individuals, there is a potential for abuse with these techniques. As all techniques that give the possibility to combine seemingly unrelated data and generate knowledge on the result, there are very pressing privacy issues, especially during the unsolicited application of such techniques on person data. Especially in the area of phishing, this opens up many new perspectives for the automatisisation of high-level spear phishing, i.e. processes of cybercrime that currently needed quite a large amount of time to launch good attacks will become much more easy and accessible to non-determined cybercriminals. Furthermore, the combination of



information particles may lead to the disclosure of undesired information, opening up new ways of exploiting this during blackmail scenarios. In the case of aggregated data, much more research is needed in methods to guarantee the right to be forgotten as stated by the European Court. Furthermore, auto-tagging can be seen as a neutral techniques that would also allow the development of new techniques for thwarting large scale spear phishing attacks.

3.12 SMART GRIDS

For further information see Appendix A: High Level Scenarios section 4.12

Smart grids are complex systems designed to deliver energy to consumers in a cost-effective, adaptive and flexible manner based on consumption and energy production information. It is therefore a modern approach to energy storage and transport where information management about behaviours of suppliers and consumers plays a central role to improve the efficiency, reliability, cost and sustainability of the overall system.

Smart grid approach has a set of differentiating factors compared to other forms of energy grids. First, they are more reliable, improving fault detection and implementing self-healing mechanisms of certain components of the grid. This feature makes smart grid more resilient against attacks, either they be physical or cyber. Reliability also refers to the capacity to divert current along different possible paths from source to destination, avoiding power outage problems.

Another factor is the capability to receive power from a destination if it generates more power than it consumes (eg. A local sub-network). This is call bidirectional energy flows.

One of the most prominent factors of smart grids is demand-side management, by which the overall efficiency is improved and power price reduced thanks to less redundancy in transmission and distribution lines and a greater utilization of generators.

The flexibility of the smart grids permits the integration of highly variable energy production sources, such as renewable energy sources (e.g. wind power, solar power), without the need to add more energy storage.

Last factor of relevance is the way now consumers and suppliers relate to each other, having the possibility to accommodate power price in a flexible and more sophisticated manner depending on specific consumer behaviours and preferences. Users typically use different means of telecommunication networks, helping the retrieval, transfer and collection of data from deployed sensors (e.g. smart meters) to remote control systems and, eventually, the processing and management by administrators.

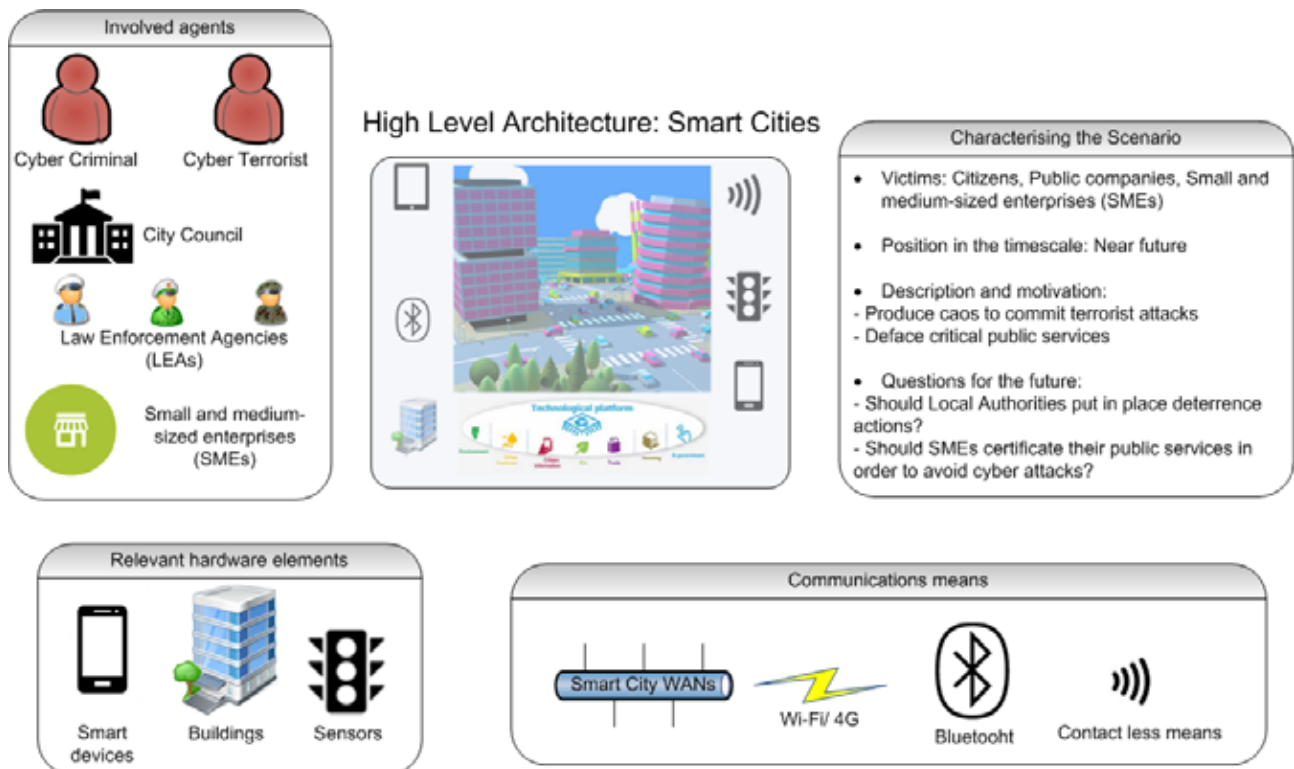
The smart grid is considered by the European Commission a critical infrastructure, since energy grids (of whatever form), and, ultimately, energy, is fundamental for the well-functioning of the society and economy.

ENISA presented in December 2013 a profound analysis of threats, vulnerabilities, exposures, and risk to the smart grid [ENISA, 2013]. Main threats discovered where natural disaster, damage/loss of IT assets, Outages, Nefarious activity/Abuse, Deliberate physical attacks, Unintentional data damage, Failures/Malfunction, Evesdropping/Interception/Hijacking, and Legal. While some of the

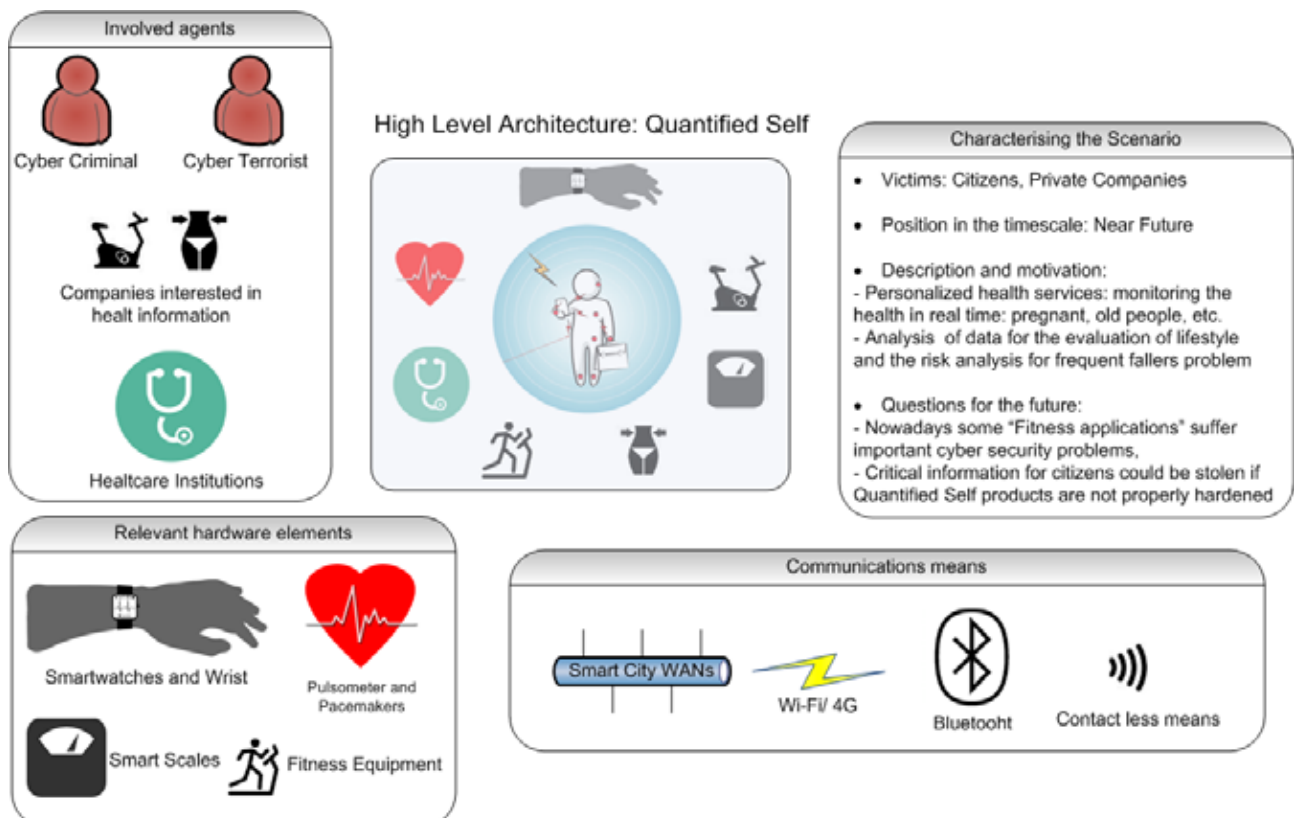


threats correspond to unintentional and/or non-human cause, there are others that and may be directly related to cyber-crime and cyber-terrorism acts.

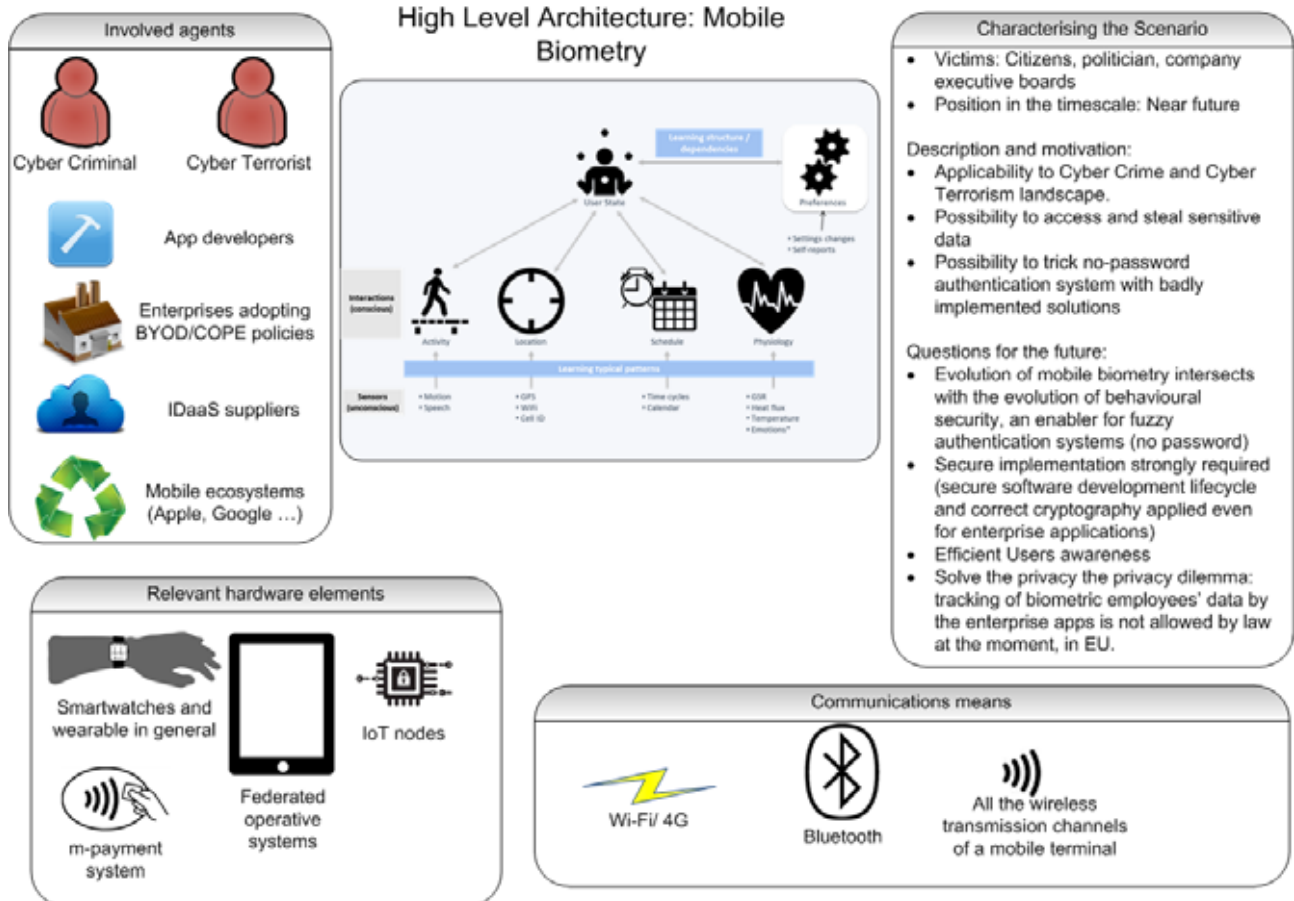
4.1 SMART CITIES



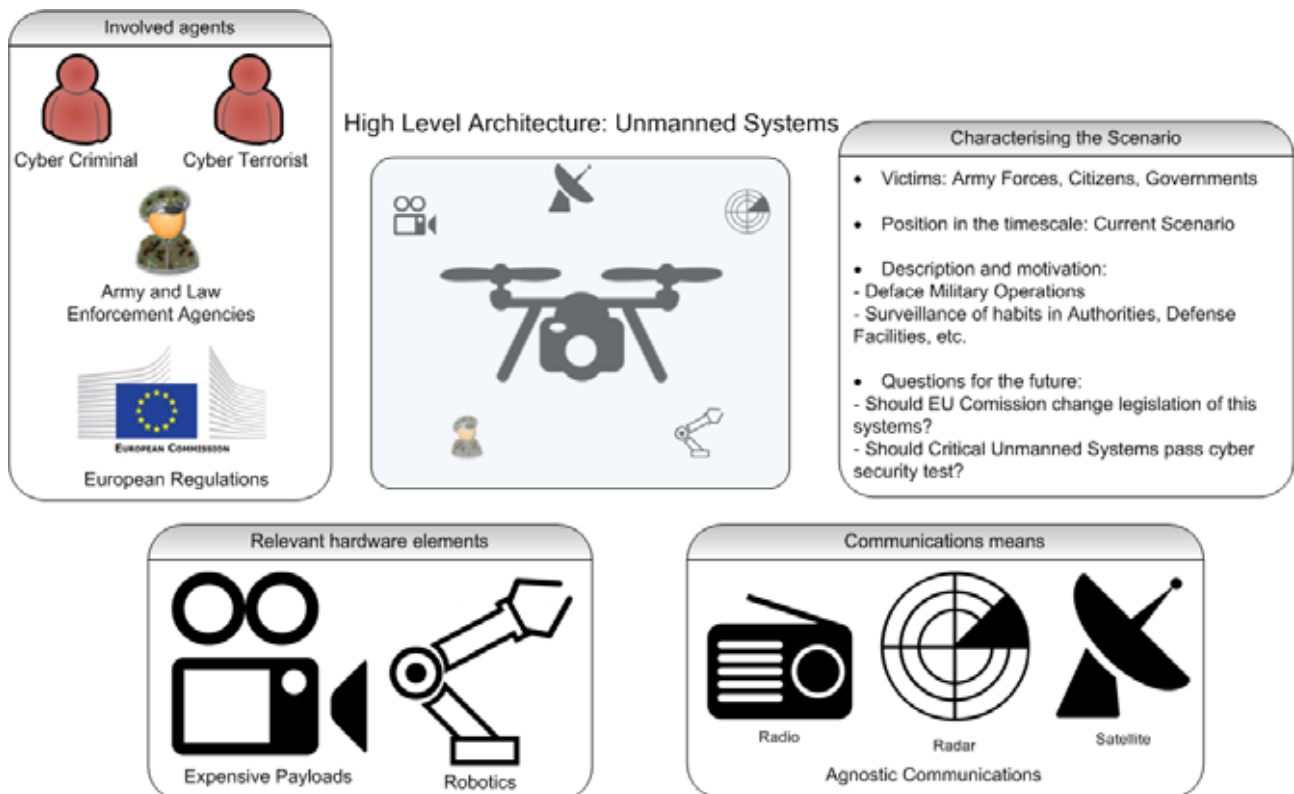
4.2 INTERNET OF THINGS/QUANTIFIED SELF



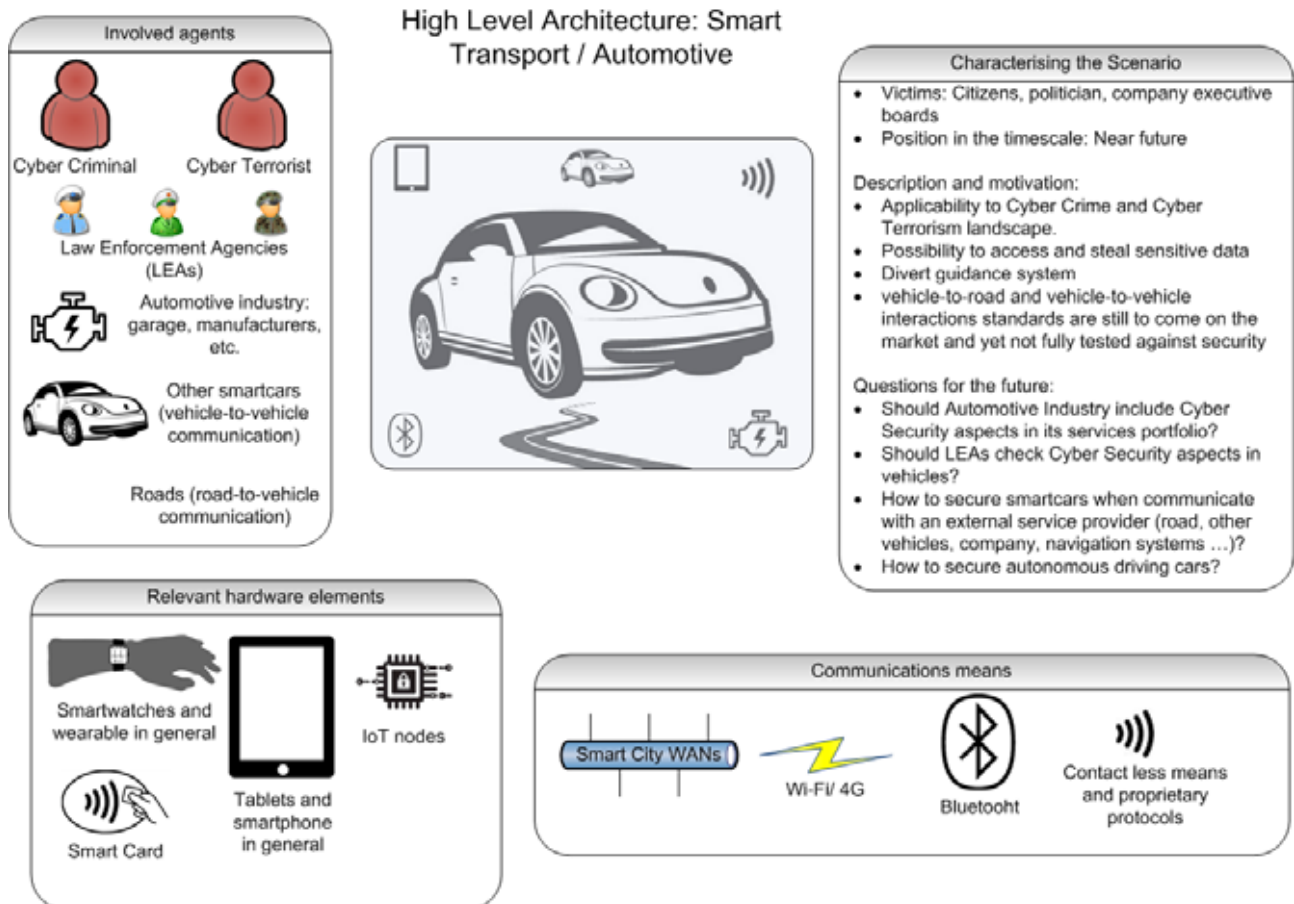
4.3 MOBILE BIOMETRY



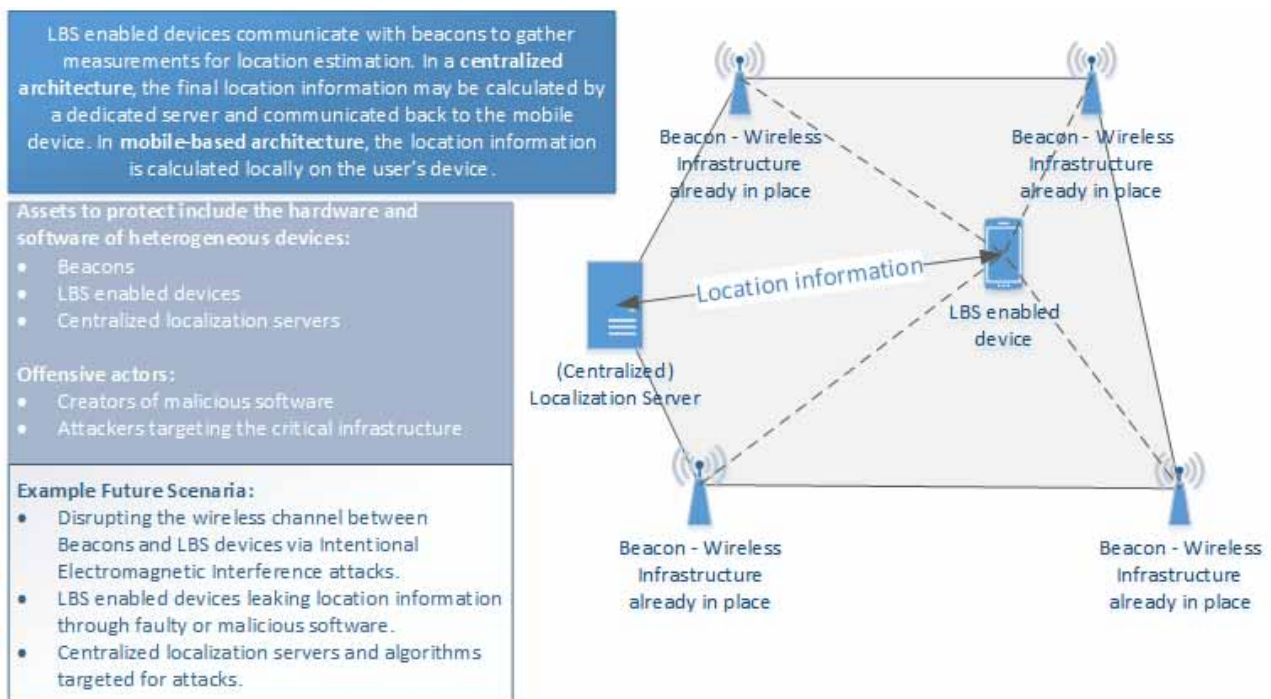
4.4 UNMANNED SYSTEMS



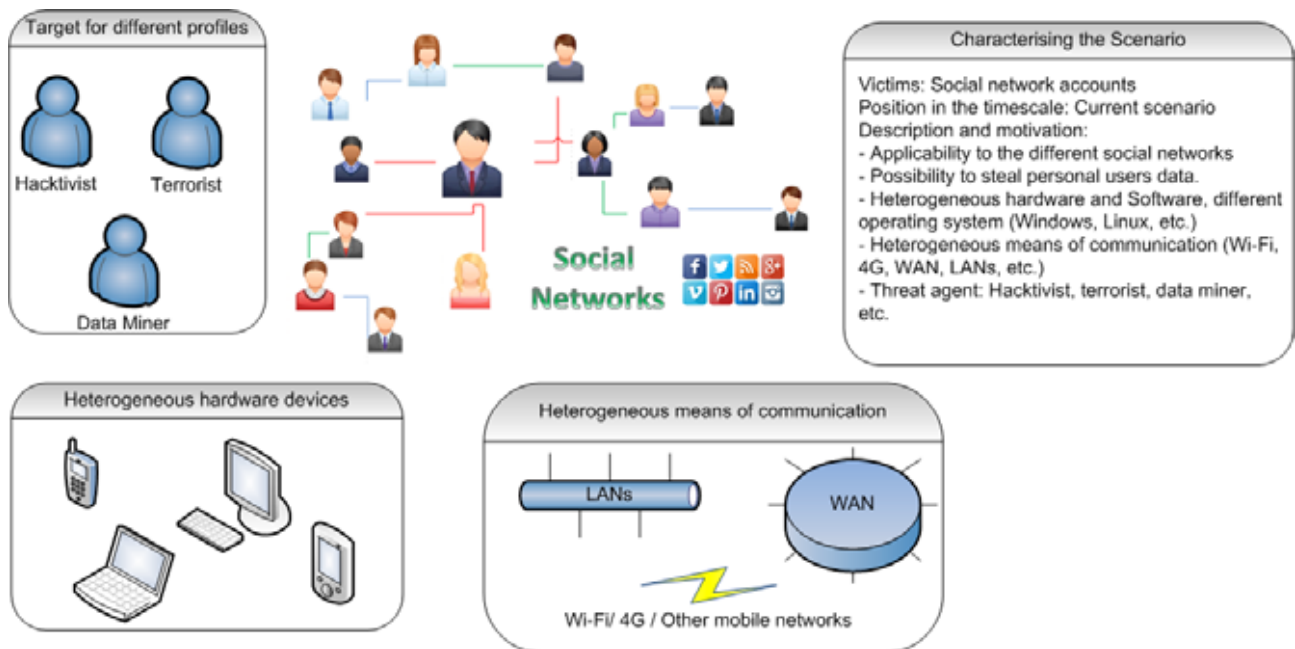
4.5 SMART TRANSPORT (AUTOMOTIVE)



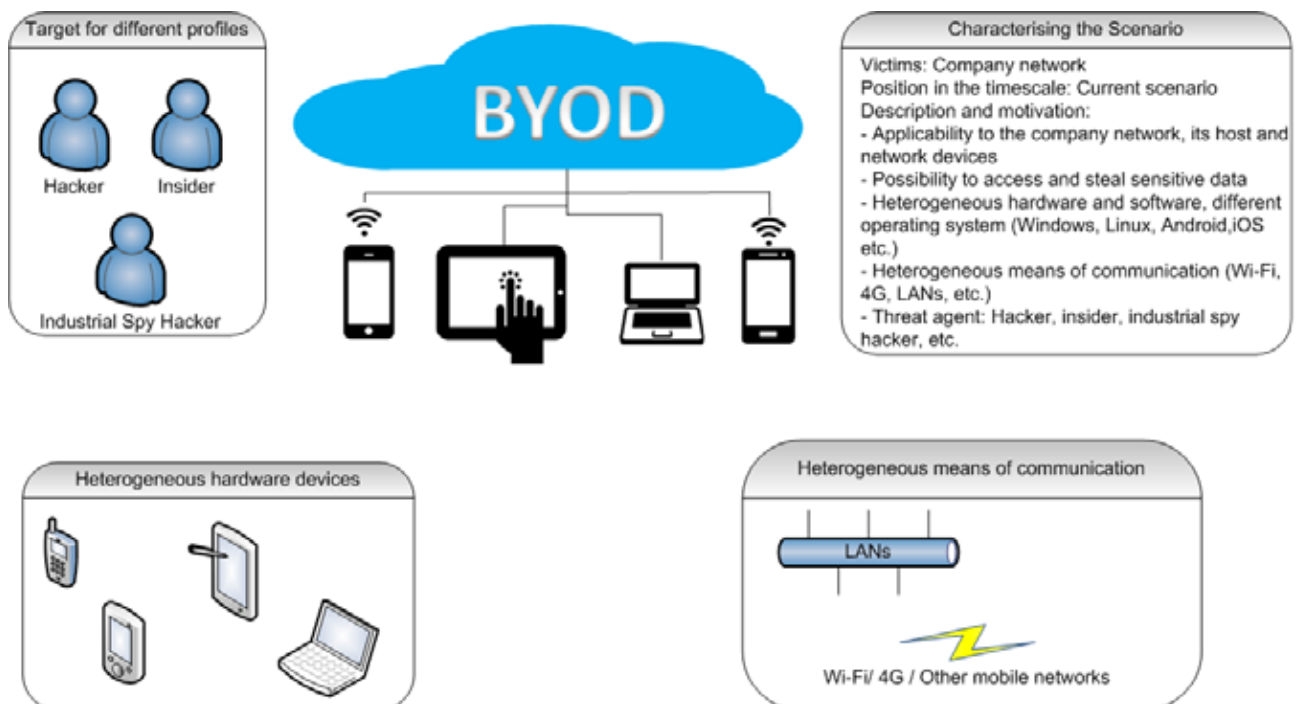
4.6 LOCATION BASED SERVICES



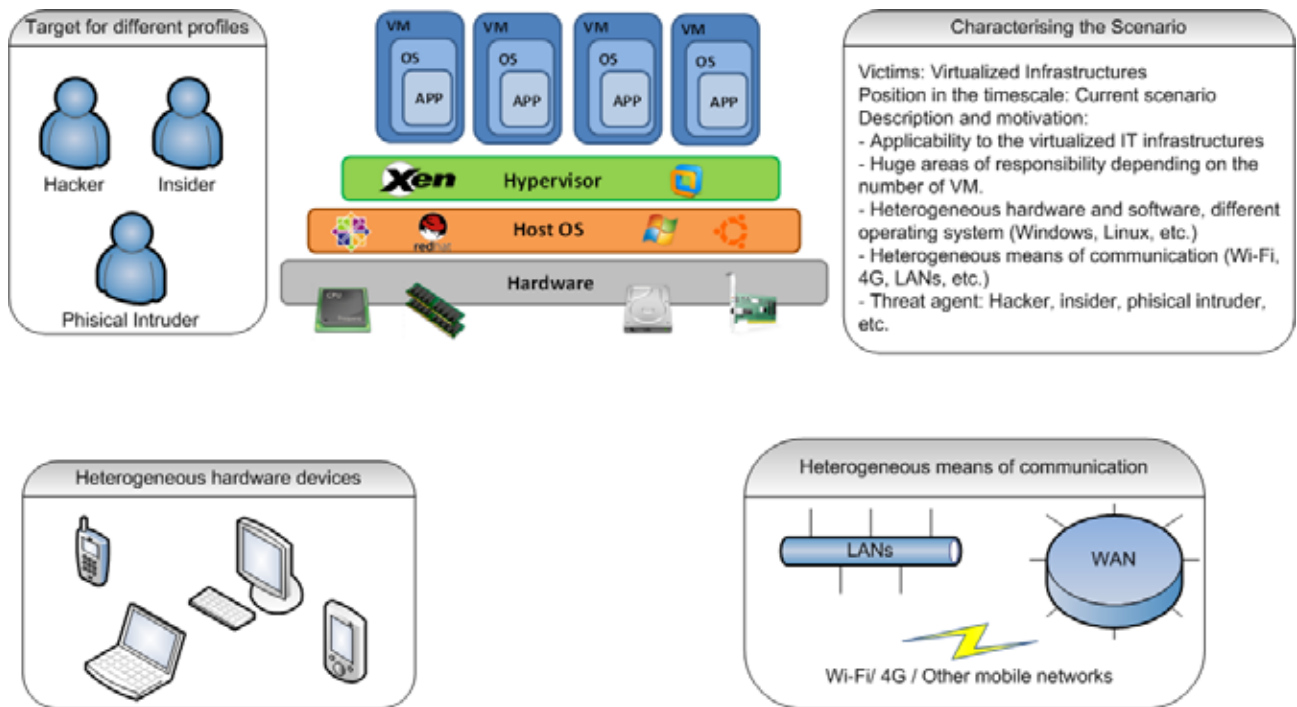
4.7 SOCIAL NETWORKS



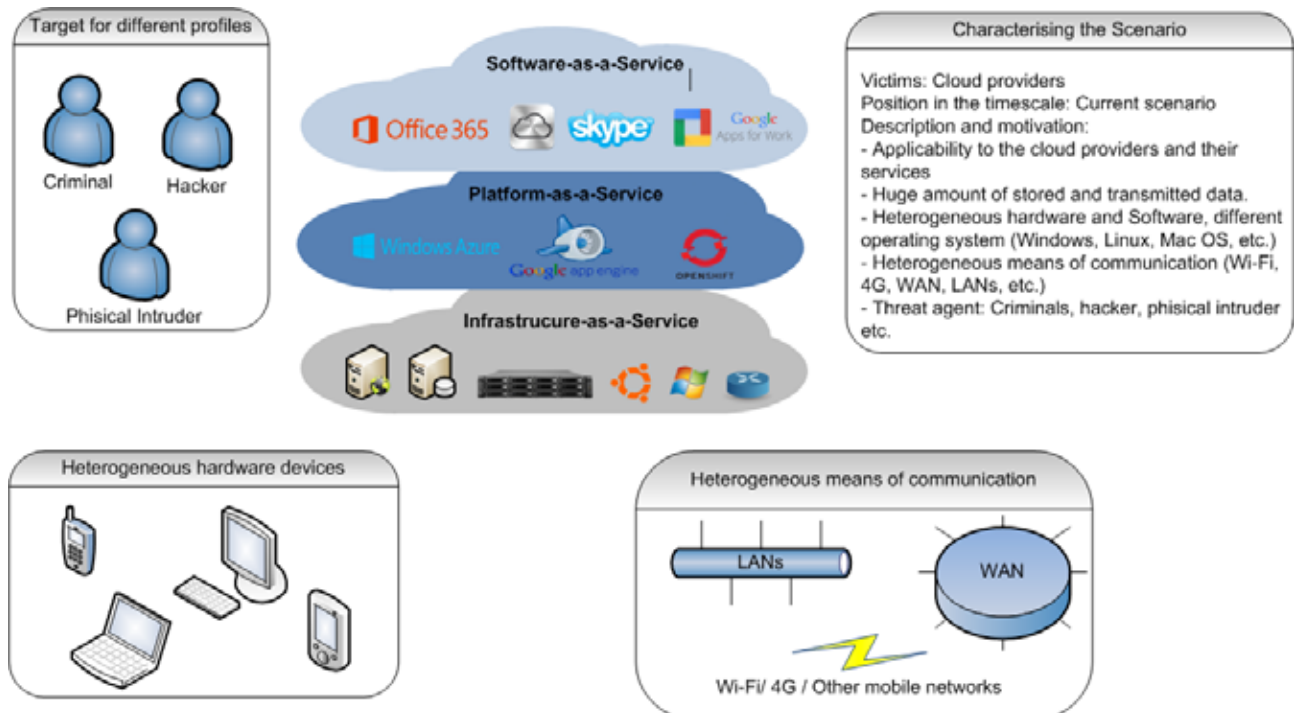
4.8 BYOD



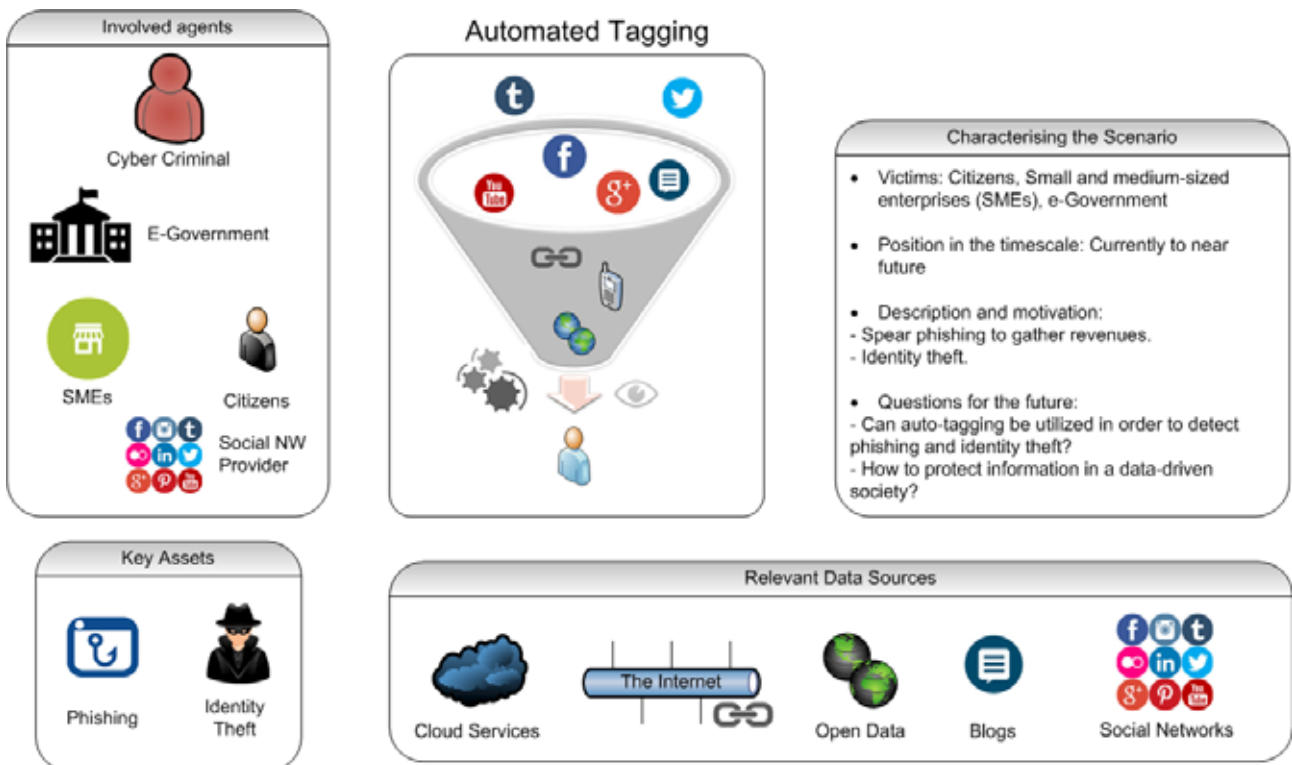
4.9 VIRTUALIZATION



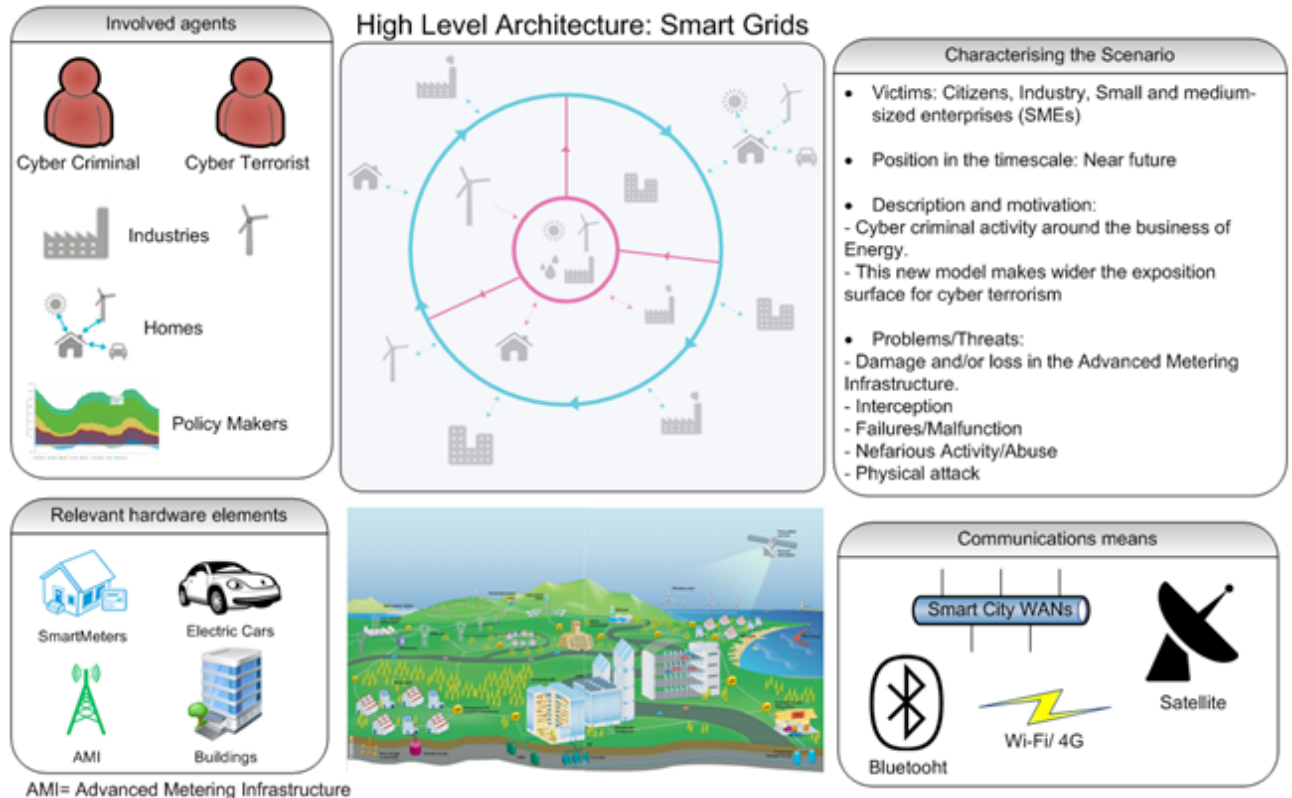
4.10 CLOUD COMPUTING



4.11 AUTO TAGGING



4.12 SMART GRIDS



Nowadays cyber security goes mainstream. The cyber risk landscape is evolving rapidly in a multitude of areas and the total number of data breaches and cyber attacks increase every year. The top three industries affected are Public, Information and Financial Services but no industry is immune to security failures. Financial or Reputation lost and brand damage consequences of cyber attacks are a fast-growing concern among business [MANDIANT, 2015].

IT threats in cyber attacks are multi layered. Usually the multi-layered approach to security is split in these layers: network layer, application layer, device layer, physical layer and the human layer. They involve a huge number of involved components and terminals are heterogeneous: Personal Computers, Mobile Devices, Network Devices and Industrial Hardware. However it is important to recognize the difference between external and internal threats. In external threats an adversary attempt to penetrate computer systems from outside the company's network whereas internal threats happen inside. Many internal data breach instances come from an authorized individual.

Figure 31 represents another way to describe the real essence of security and cybercrime today. Ultimately there are two types of exploits: one relates to humans the other to machines. Technical exploits and human exploits are actually both exploits of a unique information space where an asset exists. Being the risk management all about evaluating the probability/risk of a threat exploiting a vulnerability into an assets, this enlarged concept of information space opens the door to an holistic risk evaluation methodology (humans + machines) and an integrated cybercrime strategy (where attacker attack the information space in general thus humans and machines). That is what is happening nowadays. Depending on where the exploits happen the solutions are totally different because “wetware” and “hardware” do not work in the same ways.

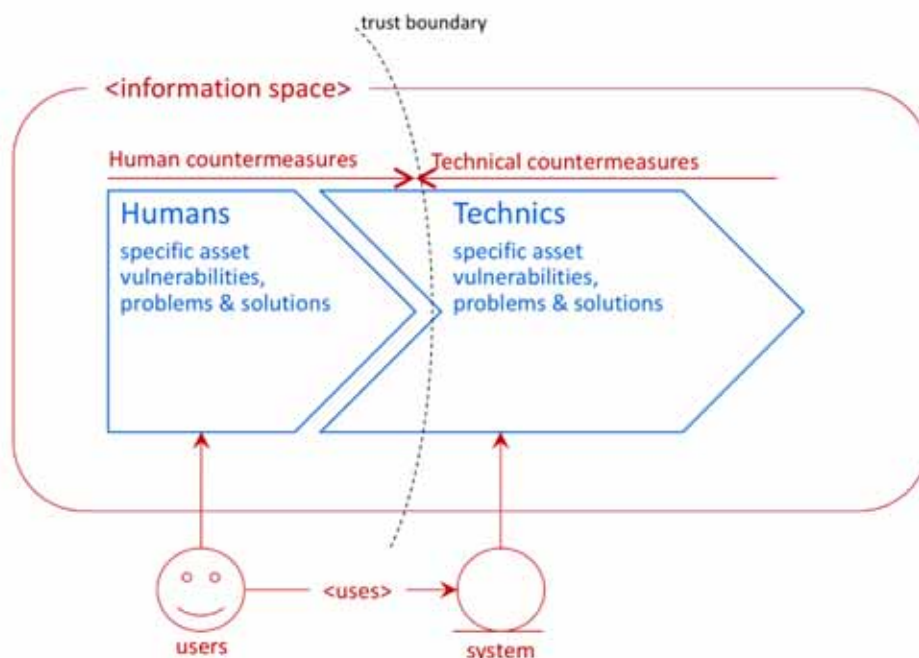


Figure 31. Assets exists into an information space that needs to be totally protected

In the last few years a large-scale security breaches have highlighted a new class of security threat: APTs. “Advanced Persistent Threat (APT) is defined by ENISA as a group with both the capability



and the intent to persistently and effectively target a specific entity” [ENISA, 2014]. Social Engineering, SQL injection, Viruses, Worms, Spyware and other form of Malware are all vectors that security professionals encounter every day in their work. Organizations in the years made some improvement but attackers may have been inside their network for months before being detected.

Nonetheless nowadays the APT schema is not anymore so “advanced” because cyber criminals got instruments and methods to face this new opportunities. Performing APT attacks is becoming extremely simple; it mainly means having a business (devilish) plan. The cyber crime completed a transition started few years ago from geek-driven to business-driven attacks [Frumento, 2014].

Many companies are now using cloud-based services to store sensitive data. The major security challenge is that the owner of the data may not have control of where data are located. Cryptographic approaches and the use of policy rules must be considered. Furthermore, tablets and mobile internet usage is increasing every day and for this reason attackers are shifting their targets to Android and IOS platform. Organizations will be forced to reconsider their mobile security strategy.

Industrial Control Systems (ICS) are not generally targeted by mainstream attackers. They attackers are motivated, well-funded and may even be a state-sponsored organization. Most of the attacks are executed using expressly developed malware and the aim might be both steal financial and exploration data. In many cases these attacks can be part of a larger cyber-warfare strategy. Disclosure in ICS and SCADA system is not present due to the nature of the infrastructure itself.



6.1 REFERENCES

- APRE. (n.d.). Agency for the Promotion of European Research - Bandi. Retrieved 27 May 2015, from <http://www.apre.it/5524>
- Ackermann, J. (2009). Toward Open Source Hardware. Retrieved from https://www.tapir.org/Ackermann_Open_Source_Hardware_Article_2009.pdf
- AdmitOne. (n.d.). Identity Assurance as a Service: AdmitOne Security. Retrieved 27 May 2015, from <http://www.admitonesecurity.com>
- ApacheHadoop. (n.d.). Welcome to Apache™ Hadoop®! Retrieved 27 May 2015, from <https://hadoop.apache.org/>
- Ayass, M., & Serrano, J. (2012). The CERN Open Hardware Licence. *International Free and Open Source Software Law Review*, 71–78. <http://doi.org/10.5033/iffoslr.v4i1.65>
- Babar, S., Mahalle, P., Stango, A., Prasad, N., & Prasad, R. (2010). Proposed Security Model and Threat Taxonomy for the Internet of Things (IoT). *Recent Trends in Network Security and Applications*, 420–429. http://doi.org/10.1007/978-3-642-14478-3_42
- Ballano Barcena, M., Wueest, C., & Lau, H. (2014). How Safe is Your Quantified Self.
- BehavioSec. (n.d.). The token you can't forget. Retrieved 27 May 2015, from <http://www.behaviosec.com>
- Big-Project. (n.d.). Welcome to BIG - Big Data Public Private Forum! | BIG - Big Data Public Private Forum. Retrieved 27 May 2015, from <http://www.big-project.eu/>
- Bilton, N. (2015, April 15). Keeping Your Car Safe From Electronic Thieves. *The New York Times*. Retrieved from http://www.nytimes.com/2015/04/16/style/keeping-your-car-safe-from-electronic-thieves.html?smid=tw-nytstyles&_r=2
- Blackducksoftware. (n.d.). Top 20 Open Source Licenses | Black Duck. Retrieved 28 May 2015, from <https://www.blackducksoftware.com/resources/data/top-20-open-source-licenses>
- Brumley, N., Poosankam, P., Song, D., and Zheng, J. (2008). Automatic Patch-Based Exploit Generation is Possible: Techniques and Implications. In *Proceedings of the 2008 IEEE Symposium on Security and Privacy (SP '08)*. IEEE Computer Society, Washington, DC, USA, 143–157. DOI=10.1109/SP.2008.17 <http://dx.doi.org/10.1109/SP.2008.17>
- CEFRIEL. (2010, December 14). Patient Ecosystem: come innovare l'erogazione di servizi ai malati. Retrieved 27 May 2015, from <http://www.cefriel.com/2010/12/patient-ecosystem-come-innovare-l'erogazione-di-servizi-ai-malati/>
- CSNO. (2011). Beidou Navigation Satellite System Signal in Space Interface Control Document.



- CaPITALProj. (n.d.). 2. Future Security and Privacy Incident Management. Retrieved 27 May 2015, from http://capital.atosresearch.eu/emerg_area2
- Caffery, J. J., & Stuber, G. L. (1998). Overview of radiolocation in CDMA cellular systems. *IEEE Communications Magazine*, 36(4), 38-45. <http://doi.org/10.1109/35.667411>
- Cardenas, A. A., Manadhata, P. K., & Rajan, S. P. (2013). Big Data Analytics for Security. *IEEE Security & Privacy*, 11(6), 74-76. <http://doi.org/10.1109/msp.2013.138>
- Cloud, W. (2015, May 25). Cloud computing. In Wikipedia. Wikipedia. Retrieved from http://en.wikipedia.org/wiki/Cloud_computing
- Cropf, R. A. (2007). The wealth of networks. How social production transforms markets and freedom: by Yochai Benkler. *Social Science Computer Review*. <http://doi.org/10.1177/0894439307301373>
- CvMetrics. (n.d.). Reduce Cyber Threats with Behavioral Biometric Security. Retrieved 27 May 2015, from <http://www.intensityanalytics.com>
- DiSalvo, D. (n.d.). 'Trust' And 'Identity' Get A Rethink - In Photos: Forrester: Top Technology Trends For 2014 And Beyond. *Forbes*. *Forbes*. Retrieved from <http://www.forbes.com/pictures/ehjh45lih/7-trust-and-identity-get-a-rethink/>
- Dosi, G. (1982). Technological paradigms and technological trajectories. *Research Policy*, 11(3), 147-162. [http://doi.org/10.1016/0048-7333\(82\)90016-6](http://doi.org/10.1016/0048-7333(82)90016-6)
- EC_WhitePa. (n.d.). White paper 2011. Retrieved 27 May 2015, from http://ec.europa.eu/transport/themes/strategies/2011_white_paper_en.htm
- ENISA. (2013). Smart Grid Threat Landscape and Good Practice Guide. ENISA.
- ENISA. (2014). Advanced persistent threat incident handling.
- ESA. (2011). Galileo Fact Sheet.
- Europe, B. (n.d.). Big Data Europe® Empowering Communities with Data Technologies. Retrieved 27 May 2015, from <http://www.big-data-europe.eu/>
- Francisco, V., & Gervás, P. (2006). Exploring the Compositionality of Emotions in Text: Word Emotions, Sentence Emotions and Automated Tagging. In *AAAI, Workshop on Computational Aesthetics: Artificial Intelligence Approaches to Beauty and Happiness*.
- Frumento, E. and Puricelli, R. (2014) 'An innovative and comprehensive framework for Social Vulnerability Assessment', *DeepSec 2014*. Wien, 19 November 2014. *Proceedings: Magdeburger Journal zur Sicherheitsforschung*. Available at: http://www.sicherheitsforschung-magdeburg.de/uploads/journal/MJS_033_Frumento_Assessment.pdf
- GLONASS. (n.d.). Information analytical centre of GLONASS and GPS controlling. Retrieved 28 May 2015, from <http://www.glonass-center.ru/en/>

- Gartner Trends. (n.d.). Gartner Identifies the Top 10 Strategic Technology Trends for 2015. Retrieved 27 May 2015, from <http://www.gartner.com/newsroom/id/2867917>
- GartnerWWPT. (n.d.). Gartner Says Worldwide Mobile Payment Transaction Value to Surpass \$235 Billion in 2013. Retrieved 28 May 2015, from <http://www.gartner.com/newsroom/id/2504915>
- Gelb, A., & Clark, J. (2013, January). Identification for Development: The Biometrics Revolution. Retrieved 27 May 2015, from http://www.cgdev.org/sites/default/files/1426862_file_Biometric_ID_for_Development.pdf
- Gonzalez-Gomez, J., Valero-Gomez, A., Prieto-Moreno, A., & Abderrahim, M. (2012). A New Open Source 3D-Printable Mobile Robotic Platform for Education. *Advances in Autonomous Mini Robots*, 49–62. http://doi.org/10.1007/978-3-642-27482-4_8
- Groves, P. D. (2013). *Understanding GPS: Principles and Applications* (Artech House Mobile Communications Series). (E. D. Kaplan & C. J. Hegarty, Eds.) (2nd ed.). Boston, MA: Artech House Publishers.
- H2020_EUC. (n.d.). Smart, Green and Integrated Transport - Horizon 2020 - European Commission. Retrieved 27 May 2015, from <http://ec.europa.eu/programmes/horizon2020/en/h2020-section/smart-green-and-integrated-transport>
- Hedden, H. (2013, October 1). Taxonomies for Auto-Tagging Unstructured Content. Retrieved 28 May 2015, from http://www.hedden-information.com/Taxonomies_for_Auto-Tagging_Unstructured_Content.pdf
- Hosseini, S. S., & Mohammadi, S. (2012). Review Banking on Biometric in the World's Banks and Introducing a Biometric Model for Iran's Banking System. *Journal of Basic and Applied Scientific Research*, 2(9).
- Huber, M., Mulazzani, M., Weippl, E., Kitzler, G., & Goluch, S. (2011). Friend-in-the-Middle Attacks: Exploiting Social Networking Sites for Spam. *IEEE Internet Computing*, 15(3), 28–34. <http://doi.org/10.1109/mic.2011.24>
- InLPortal. (n.d.). Grand Challenge. Retrieved 27 May 2015, from https://inlportal.inl.gov/portal/server.pt/community/distinctive_signature__icis/315/grand_challenge
- IoT_EU. (n.d.). Questions for IoT. Retrieved 27 May 2015, from <http://www.theinternetofthings.eu/questions-iot>
- Jackson, M. O. (2011). An Overview of Social Networks and Economic Applications. *Handbook of Social Economics*, 511–585. <http://doi.org/10.1016/b978-0-444-53187-2.00012-7>
- Jansen, W. A. (2011). Cloud Hooks: Security and Privacy Issues in Cloud Computing. 2011 44th Hawaii International Conference on System Sciences. <http://doi.org/10.1109/hicss.2011.103>



- Kalakota, R. (2013, August 12). Quantified Self, Ubiquitous Self Tracking = Wearable Analytics | Business Analytics 3.0 on WordPress.com. Retrieved 27 May 2015, from <https://practicalanalytics.wordpress.com/2013/08/12/predictive-search-wearable-computing/>
- Khandelwal, S. (2015, January 21). Two Million Cars Using Wireless Insurance Dongle Vulnerable to Hacking. Retrieved 27 May 2015, from <http://thehackernews.com/2015/01/progressive-snapshot-device-hacking-car.html>
- Kindberg, T., & Barton, J. (2001). A Web-based nomadic computing system. *Computer Networks*, 35(4), 443-456. [http://doi.org/10.1016/S1389-1286\(00\)00181-X](http://doi.org/10.1016/S1389-1286(00)00181-X)
- Lewis, P. J., Torrie, M. R., & Omilon, P. M. (2004). Applications suitable for unmanned and autonomous missions utilizing the Tactical Amphibious Ground Support (TAGS) platform. *Unmanned Ground Vehicle Technology VI*. <http://doi.org/10.1117/12.547452>
- MANDIANT. (2015). M-Trends® 2015: A VIEW FROM THE FRONT LINES. Retrieved from <https://www2.fireeye.com/rs/fireeye/images/rpt-m-trends-2015.pdf>
- Madan, B. B., & Banik, M. (2014). Attack tolerant architecture for big data file systems. *ACM SIGMETRICS Performance Evaluation Review*, 41(4), 65-69. <http://doi.org/10.1145/2627534.2627556>
- Manyika, J. (2011). *Big Data The Next Frontier for Innovation, Competition & Productivity*. S.I.: McKinsey & Company.
- NIST Privacy. (n.d.). NIST Privacy Engineering Objectives Risk Model Discussion Deck. Retrieved 27 May 2015, from http://www.nist.gov/itl/csd/upload/nist_privacy_engr_objectives_risk_model_discussion_deck.pdf
- NeoBlog. (n.d.). Dealing with 'cyberuncertainty'. Part II | Indra. Retrieved 27 May 2015, from <http://www.indracompany.com/en/sostenibilidad-e-innovacion/neo/blog/articulo/dealing-cyberuncertainty-part-ii>
- NetSecurity. (n.d.). Everything You Need to Know about Intrusion Detection Systems (IDS). Retrieved 27 May 2015, from <http://netsecurity.about.com/cs/hackertools/a/aa030504.htm>
- NfcForum. (n.d.). NFC Forum. Retrieved 28 May 2015, from <http://www.nfc-forum.org>
- OSD. (n.d.). The Open Source Definition | Open Source Initiative. Retrieved 28 May 2015, from <http://opensource.org/osd>
- OSHWA. (2012, May 26). Open Hardware Definition. Retrieved 28 May 2015, from <http://www.oshwa.org/definition/>
- P2PFoundation. (n.d.). Open Hardware Licenses. Retrieved 28 May 2015, from http://p2pfoundation.net/Open_Hardware_Licenses



- PaloAlto. (n.d.). What is an intrusion prevention system? Retrieved 27 May 2015, from <https://www.paloaltonetworks.com/resources/learning-center/what-is-an-intrusion-prevention-system-ips.html>
- PasswordBank. (n.d.). Retrieved 27 May 2015, from <http://www.passwordbank.com/idaas/>
- Pearce, J. (2014). Open-source lab: how to build your own hardware and reduce research costs. United States: Elsevier Science.
- Poolsappasit, N., Dewri, R., & Ray, I. (2012). Dynamic Security Risk Management Using Bayesian Attack Graphs. *IEEE Transactions on Dependable and Secure Computing*, 9(1), 61–74. <http://doi.org/10.1109/tdsc.2011.34>
- Roman, R., Zhou, J., & Lopez, J. (2013). On the features and challenges of security and privacy in distributed internet of things. *Computer Networks*, 57(10), 2266–2279. <http://doi.org/10.1016/j.comnet.2012.12.018>
- Sabahi, F. (2011). Cloud computing security threats and responses. 2011 IEEE 3rd International Conference on Communication Software and Networks. <http://doi.org/10.1109/iccsn.2011.6014715>
- Schmidt, A. (2014). Context-Aware Computing: Context-Awareness, Context-Aware User Interfaces, and Implicit Interaction. Retrieved 27 May 2015, from https://www.interaction-design.org/encyclopedia/context-aware_computing.html
- Schmidt, A., & Van Laerhoven, K. (2001). How to build smart appliances? *IEEE Personal Communications*, 8(4), 66–71. <http://doi.org/10.1109/98.944006>
- SchneierOnSecurity. (n.d.). The Future of Incident Response - Schneier on Security. Retrieved 27 May 2015, from https://www.schneier.com/blog/archives/2014/11/the_future_of_i.html
- Solderpad. (n.d.). Solderpad Licenses. Retrieved 28 May 2015, from <http://solderpad.org/licenses/>
- Stone, Z., Zickler, T., & Darrell, T. (2008). Autotagging Facebook: Social network context improves photo annotation. 2008 IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops. <http://doi.org/10.1109/cvprw.2008.4562956>
- TAPR. (n.d.). The TAPR Open Hardware License. Retrieved 28 May 2015, from <http://www.tapr.org/ohl.html>
- Tene, O., & Polonetsky, J. (2012, February 2). Privacy in the Age of Big Data. Retrieved 26 May 2015, from <https://www.stanfordlawreview.org/online/privacy-paradox/big-data>
- Varshavsky, A. (2006). Are GSM Phones THE Solution for Localization? Seventh IEEE Workshop on Mobile Computing Systems & Applications (WMCSA'06). <http://doi.org/10.1109/wmcsa.2006.2>
- WaterfallParadigmShift. (n.d.). Paradigm shift in SCADA security «Waterfall Security Solutions. Retrieved 27 May 2015, from <http://www.waterfall-security.com/paradigm-shift-in-scada-security/>



- WearableMag. (2013, October 18). Wearable Technology and Wearable Devices: Everything You Need to Know. Retrieved 27 May 2015, from <http://www.wearabledevices.com/what-is-a-wearable-device/>
- Weiser, M. (1995). The Computer for the 21st Century. Readings in Human-Computer Interaction, 933-940. <http://doi.org/10.1016/b978-0-08-051574-8.50097-2>
- WikiParadigmShift. (2015, May 8). Paradigm shift. In Wikipedia. Wikipedia. Retrieved from http://en.wikipedia.org/wiki/Paradigm_shift
- WorldScientific. (n.d.). Unmanned Systems. Retrieved 27 May 2015, from <http://www.worldscientific.com/worldscinet/us>
- Yan, J. (n.d.). Big Data, Bigger Opportunities - Data.gov's roles: Promote, lead, contribute, and collaborate in the era of big data. Retrieved 26 May 2015, from <http://www.meritalk.com/pdfs/bdx/bdx-whitepaper-090413.pdf>
- Yen, T.-F., Oprea, A., Onarlioglu, K., Leetham, T., Robertson, W., Juels, A., & Kirda, E. (2013). Beehive: Large-Scale Log Analysis for Detecting Suspicious Activity in Enterprise Networks. Proceedings of the 29th Annual Computer Security Applications Conference on - ACSAC '13. <http://doi.org/10.1145/2523649.2523670>

6.2 BIBLIOGRAPHY

- Armando, A., Costa, G., Verderame, L., & Merlo, A. (2014). Securing the 'Bring Your Own Device' Paradigm. Computer, 47(6), 48-56. <http://doi.org/10.1109/mc.2014.164>
- Barham, P., Dragovic, B., Fraser, K., Hand, S., Harris, T., Ho, A., ... Warfield, A. (2003). Xen and the art of virtualization. ACM SIGOPS Operating Systems Review, 37(5). <http://doi.org/10.1145/1165389.945462>
- Eslahi, M., Naseri, M. V., Hashim, undefined H., Tahir, N. M., & Saad, E. H. M. (2014). BYOD: Current state and security challenges. 2014 IEEE Symposium on Computer Applications and Industrial Electronics (ISCAIE). <http://doi.org/10.1109/iscaie.2014.7010235>
- Miller, K. W., Voas, J., & Hurlburt, G. F. (2012). BYOD: Security and Privacy Considerations. IT Professional, 14(5), 53-55. <http://doi.org/10.1109/mitp.2012.93>
- Smith, J. E., & Nair, R. (2005). The architecture of virtual machines. Computer, 38(5), 32-38. <http://doi.org/10.1109/mc.2005.173>
- Uhlig, R., Neiger, G., Rodgers, D., Santoni, A. L., Martins, F. C. M., Anderson, A. V., ... Smith, L. (2005). Intel virtualization technology. Computer, 38(5), 48-56. <http://doi.org/10.1109/mc.2005.163>



- End of Document -

