Security Risks of Machine-to-Machine Communications

2 authors:

Esmeralda Kadëna
Óbudai Egyetem
26 PUBLICATIONS 35 CITATIONS
SEE PROFILE

Kerti András
Óbudai Egyetem
2 PUBLICATIONS 19 CITATIONS
SEE PROFILE

Esmeralda Kadena, Andras Kerti: Security Risks of Machine-to-Machine Communications

Abstract

Machine-to-Machine (M2M) systems and technologies currently have a huge focus in the field of Information and Communication Technology (ICT). It is estimated that they will be developed in various sectors of the industry at a rapid pace. The main problem is security, more and more devices will be connected to the Internet in which critical business processes depend and in the same time the risks to applications increase.

This article attempts to put forward approaches which would address these risks. To develop this work I am concentrated in three research questions: "How secure are the data and the information on these systems and technologies?", "Which are the main challenges that came from M2M?" and "How can risks be addressed?".

Keywords: *Machine-to-Machine; Communication; Security; Risks.*

Introduction

First of all definition is very important. M2M has several different meanings: it stands for Mobile-to-Mobile, Machine-to-Machine, Machine-to-Man (or vice-versa), Machine-to-Mobile (or vice-versa) (Galetic, Bojic, Kusek, Jezic, & Desic, 2011). Here I will use it in the context of Machine-to-Machine communication. The communication of M2M is set up between two or more entities and there is no need of direct human intervention (Singtel, 2012) (3GPP , 2008).

There are several actors in such environment such as computers, mobile phones, tablets, but also a broad range of sensors, actuators, pieces of industrial and medical equipment, and too many of other everyday devices (Watson, Piette, Sezgen, &

Motegi, 2004), (Emmerson, 2010). The concept of the underlying communication network that allows bidirectional exchange of information between these devices, it is another important aspect of M2M communication. It can be seen from its longer acronym M2 (CN2) M that stands for Machine-to-(Communication-Network-to)-Machine (Boswarthick, Elloumi, & Hersent, 2012). M2M systems find applications in different areas such as home and industry automation (ETSI, 2012), connected consumer (ETSI, 2013), smart metering (ETSI, 2010), healthcare (ETSI, 2013), smart traffic (ETSI, 2013), and countless others. Through this wide variety of possible uses, M2M communication helps to achieve the vision of connected things - Internet of Things (IoT) (Atzori, Iera, & Morabito, 2010), a world where it is thought that ubiquitous and intelligent applications contribute to a better, practical and safer world.

It is concluded that the number of these connected devices is rapidly growing. According to Cisco Internet Business Solutions Group (IBSG), 25 billion devices were connected to the Internet on 2015 and 50 billion will be by 2020 (Evans, 2011). Ericsson declare that their vision of more than 50 billion connected devices by 2020 may seem a bit ambitious today, but with the right approach, it is within reach (ERICSSON, 2011). Is it clear that we are faced with a rapid growth and due to this, the concept of M2M communication is becoming more and more significant. But interaction between devices based on different access network technologies (i.e. mobile: 2G/3G/4G, Wi-Fi, Bluetooth), using different platforms and data models is still very limited. The idea consists on connecting a large number of different devices communicating through different technologies, so to create a heterogeneous environment. In order to enable connection of heterogeneous devices, globally accepted standards have to be used and developed new ones to achieve ubiquitous connectivity and security.

M2M background

M2M Architecture

Even though every specific deployment of M2M is unique, exist four fundamentals stages for the most M2M based applications (ETSI, 2013):

- Collection of data;
- Transmission of data through a communication network;
- Assessment of data;
- Response to the available information.

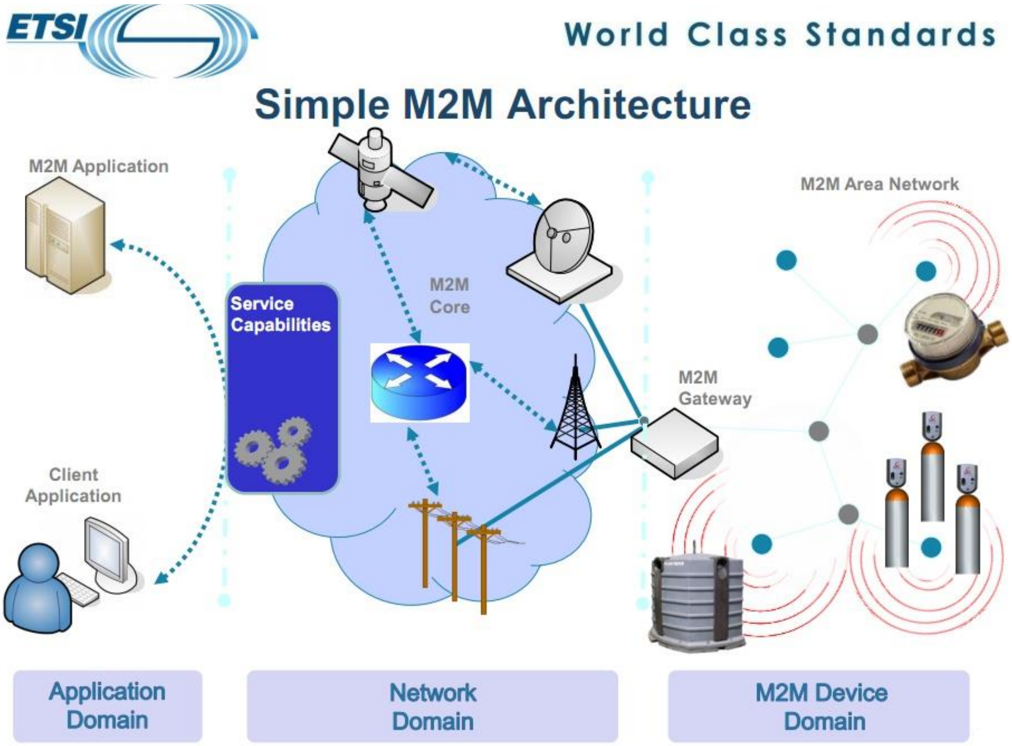

Figure 1: Basic M2M architecture

In the Figure 1 it is shown the M2M basic architecture. M2M devices reply to requests for data contained within them or transmit the data automatically. Devices can be of different kinds like temperature sensors, motion detectors, level indicators, etc. To enable the transmission of the data the machine (if it is sufficiently complex) can use the module of the M2M device as its modem. Nevertheless, if the monitored machine is made of switches and simple circuits and is not capable to point out a sufficiently intelligent behaviour, then it is given the role of slave and is controlled by the M2M module.

M2M devices may compose an M2M area network, which can be realized as, e.g. a Bluetooth based personal area network of body sensors (Boswarthick, Elloumi, & Hersent, 2012). M2M gateway provides interconnection of M2M devices and forwards collected data from them to communications network.

The communication between M2M gateway and M2M end-user application or server is realized via communications network such as cellular network, telephone lines and communication satellites (Boswarthick, Elloumi, & Hersent, 2012). The advantage of cellular data services is the ability to send frequently large amounts of data. This means of data transfer is usually most convenient as telephone lines require implementation that can be rather complicated, and satellite transmissions, which are of particular use in remote monitoring over large distances, are commonly very cost and energy-inefficient.

Finally, when data reach an M2M application, they can be analyzed, reported and acted upon by a software agent or a process, depending on the specific system design.

M2M Use Cases

- Traffic Cameras

Traffic cameras with cellular connectivity may be installed in locations such as motorway overpasses or remote stretches of roadway. Cameras may also require simultaneous secure local WLAN connectivity to the next camera down the road, e.g., when measuring average speed.

- Metering

Almost every house and office building has a gas, water, and electricity meter that measures the use of these utilities. When it comes to measuring the usage, the process is time inefficient and, therefore, a costly affair. Automatic meter reading is the technology of automatically collecting data from energy meters, and transferring that data to a central database for analysis and/or billing. Additionally, as the adoption of smart metering technologies grows, the need to monitor usage on a real-time basis becomes more and more compelling as a business case to optimize use of a smart grid for both energy usage, and for individual households to contribute to the electrical grid.

- Vending Machines

Vending machines are an efficient and cost-effective method of distributing retail goods and it's important that the service provider keep track of stock levels, and whether the machines are working properly. Vending machines are subject to regular attacks on their contents. This increases the threat to other items of value in the machine, as well as to the collection of electronic payments. Additionally, in some advanced applications, there is a desire to push multimedia marketing to displays in the vending machines. Vending machine connectivity may come from a variety of connectivity options within the customer premises.

- Asset/Cargo Tracking

A remote asset/cargo tracking system allows owners or users of equipment to, for instance, monitor critical parameters, perform remote commands, or monitor movements. Asset and cargo tracking will often require that the M2M device be placed in areas where physical access is difficult. Such placements would be part of a service provider's attempt to protect it from the environment, and to resist theft and tampering of the M2M device. This placement, together with the fact that the M2M device may be mobile, can make it difficult and costly to physically access the M2M device.

Challenges and security in M2M

Recently, an immense attention has been lavished on M2M communications. But with comfort and convenience came some security risks. The Internet of Things can turn into the Internet of Troubles. Any device that has network connectivity is exposed to attacks, directly over the network or indirectly from an application. Here the main focus is on data collected by devices and then processed by applications. These data might include personal information that is always of value to data and identity thieves/hackers. Devices and application of IoT are also in the center of attention of people who are involved with cyber warfare, cyber espionage, hacktivism, and even terrorism. Which is more a cyber-attack has the potential to damage physical services and infrastructure and it is intelligible that it might even take lives.

In June 2010, a highly sophisticated and unique computer worm called Stuxnet came to the world's media attention. Stuxnet was designed to target only specific software controls that are used at an Iranian nuclear plant. It used zero-day vulnerabilities in Microsoft Windows to propagate across the nuclear plant's network and to scan for the presence of Siemens Step7 software (Naraine, 2010). The Stuxnet malware successfully compromised the Siemens application and issued instructions to rapidly increase and decrease the velocity of the spinning centrifuges, which caused vibrations that led to the centrifuges tearing apart. Between November 2009 and January 2010, it is estimated that over 1000 centrifuges were destroyed by the Stuxnet malware, setting back the Iranian nuclear program significantly (Zetter, 2014). The Stuxnet malware demonstrates that connected machines in the physical world can be damaged by compromising the connected application that controls them.

Based on a study by IOActive was found “a host” of vulnerabilities in sensors (used to monitor metrics such as temperature and pipeline pressure) that leave them open to radio-borne attacks from as far as 40 miles away (Kirk, 2013). The main concern is that if is abused by an attacker it could cause life loss. The researchers said that sensors from three major wireless automation system vendors, which communicate in the 900 MHz and 2.4 GHz bands, had a number of problems. For example, they found some families of sensors shipped with identical cryptographic keys. It means that several companies may be using devices that all share the same keys, putting them at a greater risk of attack if a key is compromised.

According to Michael Lee report in 2013, there is a need to protect the integrity of M2M communications (Lee, 2013). One particularly troublesome issue is that sensors generally run on limited batteries. The goal of a distributed denial of service (DDoS)[1] attack is to take the device out of service by forcing it to field all of the incoming requests. This will be done even more quickly if the demand kills the sensor's battery.

On the other side even when the M2M system is free of Malware some other problems with regard to security seem to happen. Markus Breitbach has presented a case study for the use of M2M in a networked security camera installation as an example of the value of the technology (Breitbach, 2013). An M2M-based surveillance solution saves security professionals from the consuming and often incomplete task of manually evaluating data and images captured by networked cameras. With M2M-enabled devices loaded with software, these smarter cameras can analyze images and process relevant data and can even contact security professionals over a mobile network by sending a text message to alert in a security intrusion event.

[1] A distributed denial-of-service (DDoS) attack is an attack in which multiple compromised computer systems attack a target, such as a server, website or other network resource, and cause a denial of service for users of the targeted resource (Rouse, 2013).

The two issues, of course, are different: One deals with the security of M2M itself, the other with how the technology can be harnessed for security applications. The bottom line, though, is that both suggest the deep connection of M2M with everyday activities. M2M will be a key to maintaining security or, if misused, disrupting it. These outcomes, good and bad, will happen without human intervention. Great care must be taken to directly design and deploy this technology.

Security threats

M2M devices have unique characteristics and deployment (3GPP , 2008). M2M devices are typically required to be small, low cost, inexpensive, able to operate unattended by humans for extended periods of time, and to communicate over the wireless WAN or WLAN. M2M devices are typically deployed without having to require much direct human intervention and, after deployment, they tend to require remote management of their functionality. The flexibility in terms of subscription management is also required.

These requirements introduce a number of unique security vulnerabilities for the M2M devices and the wireless communication networks over which they communicate. These security vulnerabilities are described in the following categories:

- Physical Attacks

May include insertion of valid authentication tokens into a manipulated device, inserting and/or booting with fraudulent or modified software (“re-flashing”), and environmental/side channel attacks, both before and after in-field deployment. These possibilities then require trusted “validation” of the integrity of the M2M device’s software and data, including authentication tokens.

- Compromise of Credentials

Comprising brute force attacks on tokens and (weak) authentication algorithms, physical intrusion, or side-channel attacks, as well as malicious cloning of authentication tokens residing on the Machine Communication Identity Module (MCIM).

- Configuration Attacks

Such as fraudulent software update/configuration changes, misconfiguration by the owner, subscriber or user, misconfiguration or compromise of the access control lists.

- Protocol Attacks on the Device

These attacks are made against the device. For example here can be mentioned, man-in-the middle attacks upon first network access, denial-of service (DoS) attacks, compromising a device by exploiting weaknesses of active network services, and attacks on OAM and its traffic.

- Attacks on the Core Network

Here are included the main threats to the mobile network operator (MNO): Impersonation of devices, traffic tunneling between impersonated devices, leak of configuration of the firewall in the modem/router/gateways, DoS attacks against the core network. Here can also be included the change of the device's authorized physical location in an unauthorized or attacks on the radio access network, using a deceptive device.

- User Data and Identity Privacy Attacks

Include secretly listening to other user's or device's data sent over the UTRAN[2] or E-UTRAN[3]; camouflaging as other user/subscriber's device; user's network ID or other confidential data revealed to unauthorized third parties, etc. Some of the

[2] The Universal Mobile Telecommunications System Terrestrial Radio Access Network (UTRAN) is the fixed network infrastructure that contains the facilities for the transmission to and from the mobile users over radio (Telecom ABC, 2015).

[3] E-UTRAN (Evolved UTRAN) is the network architecture defined for the E-UTRA radio interface as a part of 3GPP LTE physical layer specification (ECEE, 2013).

vulnerabilities with focus on the subscription aspects of the M2M devices have also been identified in (3GPP, 2009).

Addressing security risks

As it was mentioned above, while connectivity is convenient, it can also makes a device vulnerable. A hacker could be after data, ID, gain access to the power grid or simply searching targets of opportunity. In a fully connected environment, even a seemingly low-value device such as a light bulb can be used as a bridge into more critical systems and data.

To address the potential security risks/threats, is very important to have an understanding that what makes a system secure enough. Security is a chain thus all the links must be secured. First of all deep analysis should be made. In the table below I have summarized the main points that organizations and (or) individuals can take in consider:

RISK ANALYSIS
Attack Probability
Cost of attack
Potential Damage

Table 1: Risk Analysis

⇕

DEFENSE ANALYSIS
Detection possible?
Prevention possible?
Cost of prevention?

Table 2: Defense Analysis

EECatalog declares that for Korstanje, the solution consists on a multi-layered architecture as it is shown on Figure 2, built on a foundation of trusted hardware (Hayes, 2015). Rejecting unauthorized access to that hardware base is critical, but assuming that the system is designed in the right way, safety and security are inherent within each layer.

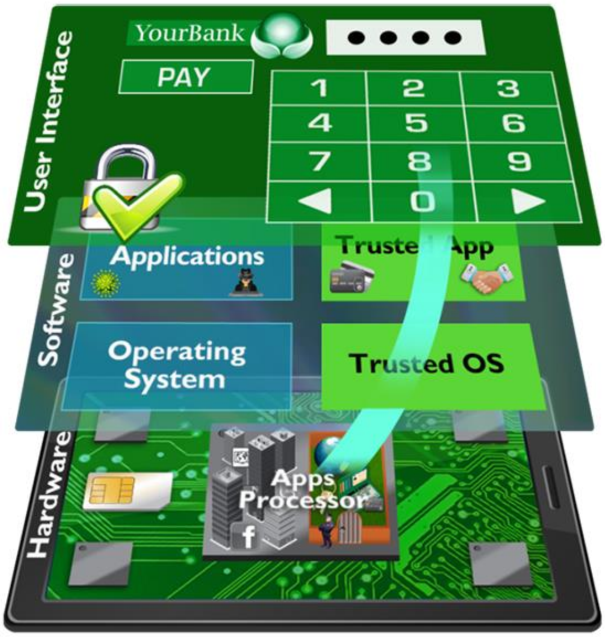

Figure 2: A multi-layer system

Design engineers have to find all the bugs in a system during development, while the attackers only have to find one. In a multi-layered system an attacker has to go through many layers to make the break but breaking through one does not damage the others. Based on (Boswarthick, Elloumi, & Hersent, 2012), below are presented the basics for creating a secure system.

Trusted environment

To establish trust relationships in distributed systems, the systems must contain security elements and capabilities which are essential to create the trust boundaries. These components include methods to extend the trust boundaries and convey trust to an external entity. This kind of environment provides hardware security measures and a root of trust in order to construct systems which merge characteristics of trust and enforcement. It is an entity, logically separated within M2M device and contains all the necessary resources and functions to provide a trustworthy environment for the execution of software and storage of sensitive data. The trusted environment ensure isolation of software and data that are stored by separating them from the M2M device in order to protect them from unauthorized access. To protect the system behavior, the trusted environment provides hardware security trust measures.
To secure operations, root of trust is essential. It secures the internal system operation and can expose properties or system's identity to external entities. Based on root of trust, the trusted environment is protected by a secure process which provide this environment to reach the state of trustworthy. This process includes all components and programs that are executed during the system boot, and can be extended to the operating system and software, thus expanding the trust boundary provided by the root of trust.

A model for this extension process is the verification of every new component when it is loaded, by measuring its integrity at the time of its initialization. Through this method every component, its state and configuration are uniquely identified. Then the measurement result is stored and integrity is protected by the trusted environment. Moreover this measurement can be compared with reference values and is hand of the verification entity to decide if this new component should be included in the extended trust boundary. As verification is intended to take place locally, it relies on the assumption that the trusted environment is in a predefined state after a completed verification process. On the other hand, validation requires that a reporting entity transfers the verification results to an external party. Then the external validator can assess the device's system state. Through validation, the predictability of the trusted environment's functions is made observable and as a consequence, trustworthy. What is more this environment can provide protected functions for the M2M device authentication towards the operator's network. This can be reached by storing the authentication data inside the trusted environment.

- **Requirements, Functionality and Interfaces**

To perform security-related functions, the trusted environment must provide cryptographic capabilities. These include:

- Symmetric and asymmetric encryption and decryption;
- Hash value calculation and verification;
- Random number generation;
- Digital signature generation and verification.

In addition, the secure storage for keys, credentials, and authentication data must be provided by the trusted environment. The storage area can be inside or outside the environment but security is protected by the trusted environment. Furthermore, the trusted environment should be able to set secure channels for the communication with other parts inside the M2M device. The interfaces which are needed to realize this communication are initialized in the secure start-up process, integrity is protected by the trusted environment, and so are supposed to operate correctly. There are two categories of interfaces that can be distinguished.

1. Protected interfaces

This interfaces ensure integrity protection and/or confidentiality of the data carried across them. This can be attained by the use of security protocols or hardware interfaces. If security protocols are used, further functionality such as authentication of the entity with which the TRE communicates, and message authentication and/or confidentiality, can be provided.

2. Unprotected interfaces

Facilitate communication between the trusted environment and the M2M device's general resources. Here M2M device is not supposed to be secured against tampering and/or eavesdropping. Nevertheless, these unprotected interfaces can give access to data which is cryptographically protected by the trusted environment for instance when the trusted environment is in possession of pertinent key material, and cryptographically secures data stored in unsecure memory. Even unprotected interfaces can benefit from other security measures such as making the interface available only after the trusted environment checks the code of its counterpart resource across the interface, for example during a secure boot-up of the M2M device. Figure 3 presents the components and interfaces of the trusted environment in a M2M device (Boswarthick, Elloumi, & Hersent, 2012).

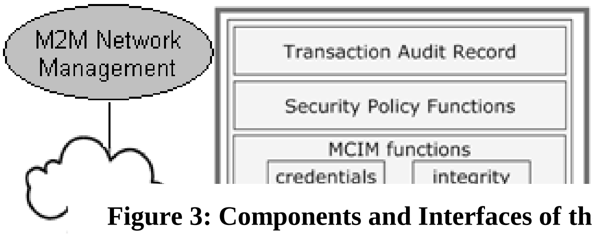

Figure 3: Components and Interfaces of the trusted environment in a M2M Device

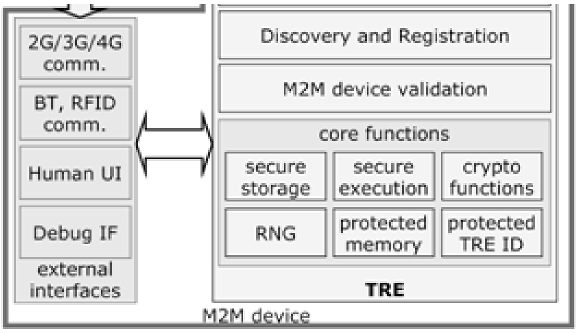

Figure 4: Components and Interfaces of the trusted environment in a M2M Device

Verification

Security is of the essence in the technological problem described above, and aims to satisfying two concrete protection goals:

- Ensuring that M2M device can reach and operate in a secure state without network connectivity, locally.
- Enabling establishment of assurance, locally and remotely, on the state of the M2M device, to assess its security properties and so trustworthy operation.

With validation we can understand the ability to technically assess the state of a system for all security-relevant properties. The argument for dedicated technical means to validate if a M2M device is applicable to its whole lifecycle, from manufacture to initial deployment (validation for installation verification), maintenance (validation for diagnosis and success verification), through to validation of correct configuration change.

Methods of system validating in its operational phase differ from pre-deployment testing and certification, or formal security proofs on a design. They lead into the realm of trusted systems and trusted computing. Here are defined three main variants. Taking in consider closed systems like smart cards, autonomous validation is their respective model. This model arrive at a secure state simply by local means and do not communicate to the exterior state information. On the other extreme stands remote validation, which was specified as remote attestation from the Trusted Computing Group. Basically, an open system only reports state information in a secure way in this second option. A wide spectrum of other variants consist on between the ranges marked by these extremes. This spectrum is called (not a single method) semi-autonomous validation (SAV). There exists just one concrete example, namely, what the TCG’s Mobile Phone Working Group has specified as secure boot (TCG, 2008), at least on the level of technical specifications.

Standardized system needed

M2M involves several sectors such as the smart home, smart power grid, electronic medical care, intelligent buildings, and intelligent transportation, etc., and each of them comes with varied and complex standards. What is more, standards of the industry are different from country to country. From the standard organizations related to communications point of view, the international ones are: 3GPP, IEEE, ETSI, ITU and IETF and also local ones in China: CCSA and CESI. All of them are researching and developing M2M related standards.

Due to expansion of M2M communication globally there is a need to have success. Therefore M2M needs a common framework on which all services and devices can interoperate and scale, and be widely available, with maximum achievable efficiency. ICT industry participants, as well as standardization and international bodies, should continuously working towards a viable and sustainable ICT framework for M2M progression. These workgroups will have to incorporate both the needs of enterprises and behaviour of digital citizens in the next generation M2M and IoT scenarios. The outcomes will go a long way in helping ICT industry participants define future security considerations and propose solutions for the safe operation of a connected world.

It is a must: Security should begin at the lower layers of M2M architecture, M2M modules manufacturers, connectivity providers, and application enablement platform firms will all play important roles in the creation of a market leading portfolios and building a strong ROI business case for enterprises to deploy M2M.

Conclusions

M2M communication applications and scenarios are rapidly growing and lead the way to new use and business cases. Due to the nature of M2M scenarios, which involve un-guarded, distributed devices, new security threats have emerged. The use case scenarios for M2M communications bring with them new requirements for security that also address the new requirement on flexibility, due to deployment scenarios of the M2M devices in the field.

It was presented that data collected by devices and then processed by applications is always with interest for hackers. So information stored on them is not secured and giving solution to this concern first of all it is needed to have a deep understanding what makes a system secure enough. Risk analyses and defense analysis are the main points in which organizations should be focused. In this article a model of secure system was given. The first is trusted environment that ensure isolation of software and data that are stored by separating them from the M2M device in order to protect them from unauthorized access. Furthermore securing operation is also needed and for this root of trust is essential. It secures the internal system operation and can expose properties or system's identity to external entities. Based on root of trust, the trusted environment is protected by a secure process which provide this environment to reach the state of trustworthy.

Besides these and due to expansion of M2M communication globally there is a need for a common framework on which all services and devices can interoperate and scale, and be widely available, with maximum achievable efficiency. ICT industry participants, as well as standardization and international bodies, should continuously working towards a viable and sustainable ICT framework for M2M progression.

And do not forget! Security is a chain thus all the links must be secured!

Bibliography

3GPP . (2008). *3GPP, TR 22.868, Study on Facilitating Machine-to-Machine Communication in 3GPP Systems.* Valbonne: 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TTA, TTC). Retrieved from http://www.qtc.jp/3GPP/Specs/22868-800.pdf

3GPP. (2009). *"3GPP Technical Report 33.812 draft version 1.3.0 Feasibility Study on Remote Management of USIM Application on M2M Equipment.*

Atzori, L., Iera, A., & Morabito, G. (2010, October 28). The Internet of Things: A Survey. *ELSEVIER-Computer Networks, 54*(15), 2787–2805. Retrieved from https://cs.uwaterloo.ca/~brecht/courses/854-Emerging-2014/readings/iot/iot-survey.pdf

Boswarthick, D., Elloumi, O., & Hersent, O. (2012). *M2M Communications: A Systems Approach.* Chichester, West Sussex: John Wiley & Sons, Ltd.

Breitbach, M. (2013, July 29). *CASE STUDY: Building a smarter security camera with M2M.* (Government Security News Magazine) Retrieved from http://gsnmagazine.com/article/31112/case_study_building_smarter_security_camera_m2m

ECEE. (2013). *UMTS.* Retrieved from Electrical, Computer & Energy Engineering University of Colorado Boulder: http://ecee.colorado.edu/~liue/teaching/comm_standards/LTE/e_utran.html

Emmerson, B. (2010). M2M: The Internet of 50 Billion Devices. Win-Win. Retrieved from http://www.mouser.in/pdfdocs/EPCOSSAWM2MArticle.pdf

ERICSSON. (2011). *More than 50 billion connected devices.* ERICSSON.

ETSI. (2010). *TR 102 691 Smart Metering Use Cases.*

ETSI. (2012). *TR 102 897 Use Cases of M2M Applications for City Automation.*

ETSI. (2013). *ETSI TS 102 690: M2M Functional Architecture.* ETSI.

ETSI. (2013). *TR 102 732 Use Cases of M2M Applications for eHealth.*

ETSI. (2013). *TR 102 857 Use Cases of M2M Applications for Connected Consumer.*

ETSI. (2013). *TR 102 898 Use Cases of Automotive Applications in M2M Capable Net-works.*

Evans, D. (2011). *The internet of Things: How the Next Evolution is Changing Everything.* Cisco Internet Business Solutions Group (IBSG). Retrieved from http://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf

Galetic, V., Bojic, I., Kusek, M., Jezic, G., & Desic, S. (2011). Basic Principles of Machine-to-Machine Communication and its Impact on Telecommunications Indusrty. *Proceedings of the 34th International Convention MIPRO,* (pp. 89-94). Zagreb. Retrieved from https://bib.irb.hr/datoteka/515808.Galetic2001.pdf

Hatton, M. (2013). *The Global M2M Market in 2013.* Machina Research. Retrieved from http://www.telecomengine.com/sites/default/files/temp/CEBIT_M2M_WhitePaper_2012_01_11.pdf

Hayes, C. (2015, November 5). *Building Trust in a Connected World*. Retrieved from EECatalog: http://eecatalog.com/IoT/2015/11/05/building-trust-in-a-connected-world/

Kirk, J. (2013, July 26). *Study finds that hackers can attack oil, gas field sensors with radio transmitters*. Retrieved from PCWorld: http://www.pcworld.com/article/2045270/oil-gas-field-sensors-vulnerable-to-attack-via-radio-waves.html

Lee, M. (2013, January 10). *M2M and the Internet of Things: How secure is it?* (ZDNet) Retrieved from http://www.zdnet.com/article/m2m-and-the-internet-of-things-how-secure-is-it/

Naraine, R. (2010, September 14). *Stuxnet attackers used 4 Windows zero-day exploits*. Retrieved from ZDNet: http://www.zdnet.com/article/stuxnet-attackers-used-4-windows-zero-day-exploits/

Rouse, M. (2013, May 16). *Definition: distributed denial of service (DDoS) attack*. (Whalts.com) Retrieved from http://searchsecurity.techtarget.com/definition/distributed-denial-of-service-attack

Singtel. (2012). *M2M Singtel*. Retrieved April 2017, from https://www.singtel.com/business/enterprise-solutions/m2m

TCG. (2008). *TCG Mobile Trusted Module Specification Version 1.0. Revision 6.* TCG.

Telecom ABC. (2015). *UTRAN-Telecom ABC*. Retrieved from Telecom ABC: http://www.telecomabc.com/u/utran.html

Watson, D. S., Piette, A. P., Sezgen, O., & Motegi, N. (2004). Machine to Machine (M2M) Technology in Demand Responsive Commercial Buildings. *Proceedings from the ACEEE 2004 Summer Study on Energy Efficiency in Buildings: Breaking out of the Box.* Washington. Retrieved from https://www.smartgrid.gov/files/Machine_to_Machine_M2M_Technology_in_Demand_Responsive_Comme_200402.pdf

Zetter, K. (2014, March 11). *An Unprecedented Look at Stuxnet, the World's First Digital Weapon*. Retrieved from WIRED: https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/