Towards Resilient Cyber-Physical eHealth Systems

JYRI RAJAMÄKI
Research, Design and Innovations
Laurea University of Applied Sciences
Vanha maantie 9, FI-02650 Espoo
FINLAND

Abstract: - Current eHealth systems are cyber-physical systems (CPS) making safety-critical decisions based on information from other systems not known during development. To achieve the trust of users, measures of safety have to be taken into consideration in accordance with the "privacy by design" approach. This requires secure storage of information and guaranteeing safe exchange of data preventing unauthorized access, loss of data and cyber-attacks. From citizens' point of view, eHealth is wholeness in which sectors of information security (availability/confidentiality/integrity) hold true. Present procedures emphasize confidentiality at the expense of integrity and availability, and regulations/instructions are used as an excuse not to change even vital information. The mental-picture of cyber security should turn from "threat, crime, attack" to "trust". Creating confidence in safe digital future is truly needed in the integration of the digital and physical world's leading to a new digital revolution. The precondition for the exchange of information "trust" must be systematically built at every CPS' level (cyber, platform, and people).

Key-words: - eHealth, resilience, cyber trust, cyber-physical system

1 Introduction

Free movement of people is one of the cornerstones of the EU. According to the Directive on Cross-Border Healthcare (effective in the whole European Union since 2013) European citizens, no matter where they live, have the right to choose where to receive medical treatment across the EU, and to be reimbursed for it. Solutions to secure the storage and cross-border exchange of eHealth data are vital in order to secure the above mentioned rights and unleash the potential of cross-border eHealth in Europe.

After the revelations of Edgar Snowden, it is clear that widely used closed-source security solutions have serious defects and intentionally planted backdoors. It is commonly accepted that real information security can only be based on the openness of the security solution and the secrecy of its encryption keys. Externally auditable open-source security solutions are needed in order to ensure the privacy and integrity of eHealth data and gain the trust of the customers.

In Europe, we should build a security solution which will not only be strong against common cyber-crime but will also present a major obstacle to the democracy and intelligence organizations of entire countries. By open-sourcing and transparency, we will make it a subject to external audits and improvements by the user community and policy development. This will create a European open security systemic level nexus which can be used by governments, corporations and SMEs alike to build secure eHealth services. The same platform can also be adapted for other application areas, including the applications dealing with personal information as well as emerging areas such as the mHealth, Internet of Things (IoT) and global cyberinfrastructure.

2 General principles of information security

ISO/IEC 27001 standard defines information security as the protection of information and information systems against unauthorized access or modification of information, whether in storage, processing, or transit, and against denial of service to authorized users. According to it, the information security includes also the measures that are needed to detect, document, and counter such threats. Information security is composed of computer security and communications security [1].

Information Security Handbook [2] defines information security as follows: The term information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide: *1) integrity,* which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity, *2) confidentiality,* which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information, and *3) availability,* which means ensuring timely and reliable access to and use of information.

These definitions are based on the concept that a person, business or government will suffer harm if there is a loss of confidentiality, integrity or availability of information and that it is the role of information security to minimize the possibility that such harm will occur [2].

ISO/IEC 27032 [3] addresses “cybersecurity” as the “preservation of confidentiality, integrity and availability of information in the Cyberspace”. The cyberspace” can be considered as “the complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it. Cybersecurity can also be thought of the sub-discipline of information security.

The International Telecommunications Union [4] defines cyber security as follows: Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user’s assets. Organization and user’s assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user’s assets against relevant security risks in the cyber environment.

The Department of Homeland Security [5] defines situational awareness as “the ability to identify, process, and comprehend the critical elements of information about what is happening to the team with regards to the mission.” While the notion of situational awareness has been around for some time in military combat scenarios, it is a relatively new development in the field of computer security.

2.1 Security threats

There are many security threats in our current networked world, including but not limited to malware, phishing, DDoS, vulnerabilities, compromised devices, interception and industry automation faults. Here are some examples of serious cyber security threats: i) Snowden’s revelations [6] [7] illustrate how dependable devices and services are and how large scale monitoring and interception are feasible. It is possible to intercept devices, network traffic and even isolated networks. Because of large scale mobility and communication, our location and privacy has been compromised. ii) One example of serious security incidents is the heartbleed bug concerning the Open SSL. The bug allows an intruder to read the private key from the vulnerable system key without leaving any traces. Thus, all network traffic and login credentials could be read. The bug made most of Internet users’ accounts vulnerable as Open SSL is largely used. Moreover, as users tend to use the same password in different places, also invulnerable systems were affected. iii) Yet another example is the IoS goto bug, which was a result of a wrongly used goto statement in the code. Similarly, the bug allows capturing network traffic and login credentials from a vulnerable system.

Computer networks in general are typically a shared resource used by applications with different interests. The Internet is a particularly widely shared resource where a network conversation may be compromised by an adversary.

In computer networks, an obvious threat is that an adversary would eavesdrop on network communication. Eavesdropping is an example of passive threats. By definition, passive threats involve attempts to by an attacker to obtain information relating to prevailing communication [8]. It is, however, possible to encrypt messages to prevent an eavesdropper from understanding the contents of the messages. A protocol and mechanisms that do encryption are said to provide message confidentiality. In traffic confidentiality, the quantity and destination of communication are concealed as well.

Active threats involve modifications of the transmitted data or the creation of the false transmission. An adversary who cannot read the contents of the encrypted message may still be able to change it, copy and retransmit it or delay it. Techniques or protocols that detect such message tampering, replay attacks, and delaying provide data integrity, originality, and timeliness. Data integrity, originality, and timeliness are aspects of the more general property of integrity.

Another active threat is that the traffic is unknowingly being directed to a false node such as a false host, a false router or a false website. An authentication protocol is a way to ensure that one is actually talking to whom one thinks one is talking. Authentication includes integrity because it is meaningless to get tampered messages from a certain participant [8].

The owner of the service provider, e.g., the website, can be attacked as well. The websites may be defaced by remotely modifying without authorization the files that make up the website. The rules that define who is allowed to do what are an issue of access control. The services may also be subjects to Denial of Service (DoS) attacks that unable to access to the service because of the overwhelmed bogus requests. This is an issue of availability.

The customer and the service also face threats from each other. Each could deny a transaction to occur or invent a non-existent transaction. Nonrepudiation means that a bogus denial of a transaction can be disproved, and nonforgeability means that claims of bogus transaction can be disproved.

Risk analysis, traffic monitoring and analysis, and incident observations are considered to be in a key role in the prevention of forthcoming security threats. Detection of more security incidents enables us to have a better understanding of what types of security incidents occur and the source of those incidents as well.

3 Principles of building of cyber trust

Today’s discussion on cyber security is motivated by the rapidly growing cyber-crime and cyber-attacks. For example, Berkman Internet Monitor report states: “*As the stories of malicious cyber-attacks against individuals, companies, and governments continue to mount, attention to Internet security now features prominently in public policy discussions*” [9].

In addition to closing and restricting (access), cyber security can be seen as a key enabler for the development and maintenance of trust in the digital world. It is important to complement the “cyber security as a barrier” perspective by emphasizing the role of “cyber security as an enabler” of new business, interactions and services - and recognizing that trust is a positive driver for growth!

As the digitalization of every aspect of society, business and everyday life proceeds at increasing speed, trust in digital space has become of prime concern for (eHealth) businesses, public actors and citizens. When parties trust each other, they can readily engage in cooperation and interaction with the goal of mutual profit or advantage while the transaction costs are low. As more and more of commercial interactions take place over the Internet, it also becomes more important to enhance trust in the Internet. Successful development of a hub for trusted and trust enhancing services involves activities at several levels, ranging from the infrastructure and technology to regulation and policymaking for the creation of a favorable environment that meets the needs of individuals, companies and public actors. Transparency and openness will be fundamental approaches for building the environment and services that establish and enhance trust in the digital world.

We, however, also realize that the idea of establishing co-operation as a dominant survival strategy directly between hosts is not supported by the theory of evolution of co-operation. The classical theory of co-operation tells us that if interaction among selfish players is un-ending, the players have a reasonably long memory and they are able to gossip effectively, then a co-operative strategy will become dominant under the condition that obstinate violators of co-operation can be effectively controlled. These conditions are not in-force directly between hosts. Interactions between Internet Service Providers (ISPs) and operators and reasonably large networks are mostly un-ending.

Trustworthy and secure technologies and platforms are a basis to build on. As the security risks keep increasing with cybercrime and other unauthorized access, the security solutions and management of IT security need constant development and new approaches to keep up with the pace. Likewise, their successful use requires awareness and education. While the reports on cybercrime and attacks call for tighter security and monitoring of data traffic to detect threats, there are increasing concerns on privacy raised both by the public and businesses. There is a delicate balance that is needed for development of trust and confidence and the development of technology and services needs to be guided with appropriate regulatory frameworks that take into account the needs of the key stakeholders (i.e. the citizens, the businesses, the public sector and government). While this is a challenge among stakeholders in a specific market, the complexity increases as we recognize the global nature of Internet based services.

3.2 Trust and confidence enhancing services and platforms

Investing in systems that improve confidence and trust can significantly reduce costs and improve the speed of interaction. Conversely, costs increase dramatically and citizens are much more cautious about online transactions when trust and confidence have been compromised [7]. Key services include management of trustworthy identities and user (service) profiles, as well as management of the multitude of personal data, also known as "digital identity", i.e. information about our life and activities that is becoming increasingly complete and traceable. Consequently, the services related to privacy and data ownership will be prime elements for the development of trustworthy services and enabling trusted flows of data.

As the public services and business services domains have traditionally not been well linked, a new opportunity has also been identified in providing an environment for public and commercial services based on trustworthy service bus and trustworthy identities (e.g. in Estonia).

There are also opportunities in the creation and maintenance of the underlying trustworthy platforms, ranging from ubiquitous embedded and mobile platforms to data centers and providing trust assessment for services, applications and devices that are based on observed behaviors and reputation.

We need to be aware, have correct understanding of security incidents, network traffic and other important aspect that affect security. Therefore, we need situational awareness. For protection, we need security technologies, but we must not forget human aspects and managing security correctly, either. For that, we need security management. As a result, we will have resilient systems and infrastructures that are able to resist and recover from disturbances caused by the surrounding hostile environment.

3.3 Human behavior

Rapid increase of cybercrimes has effected how end users use new technology and services surprisingly little. This statement is supported, e.g., by fast adaptation of social media and new mobile phones based on new unprotected technology. Still, two behaviors of users have been emerging during recent years that both have an effect on transparent cyber trust: i) Consumer applications bring changes to business and governmental structures and services - behaviors arise from the quest of usability and user experience; and ii) we are seeing trust being organized based on networks of people, not based on software. Behaviors are polarizing, and the topic of transparency and cyber trust needs to be thought from different perspectives: personal/private awareness, family, workplace, national and global.

The concept of security and privacy vary from culture to culture, which is due to behavioral differences between North America - "very private", individualism, Asia - "hyper social, collective; and Europe being in the middle. This has an effect not only on how businesses and governments behave, but what is considered as transparent, open or thread. In other words, in more collective cultures, the view that everything is shared, and it is not seen as being wrong, if someone else accesses the data of one's digital behavior and identity. People share data proactively, also the argument of "I've got nothing to hide", may not yet be a global trend, but can be identified as a week signal. Trust is also situational, i.e., built always in relation to the context and actors. One view is saying that the only sustainable way forward is that each person is solely in control and responsible for their own personal data - and others may only be granted rights. If so, we need to create structures and processes to enable this. Reliable access control may become even more important as all societal infrastructures are controlled by computers in which network connection and even water supply system data may be stored in the Cloud.

3.4 Privacy by Design

Privacy by Design (PbD) is an approach to systems engineering which takes privacy into account throughout the whole engineering process. PbD is based on seven foundational principles [10]: 1) proactive not reactive, 2) privacy as the default, 3) privacy embedded into design, 4) full functionality: positive-sum, not zero-sum, 5) end-to-end lifecycle protection, 6) visibility and transparency, and 7) respect for user privacy. The essence of a resent cybermodel for PbD (C4P) [11] approach is to develop an open privacy framework using a services-based approach (similar to the platform as a service cloud construct) applying data-centric-security methods, which are integrated into an system of systems package using existing commercial off-the-shelf technology. The open privacy framework foundation leverages, aligns, and is integrated with

NIST’s Risk Management Framework and Cybersecurity Framework. By developing and documenting a common open privacy framework for which it is easy for privacy-enhancing technologies to develop capabilities, C4P enables more integrated privacy capabilities to become available to enhance usability, reuse, and innovation [11].

4 Discussion and conclusions

Digital technologies have significantly changed the role of healthcare patients in seeking and receiving medical help, as well as brought up regulatory issues in the health area. Citizens continue to take a more central role in decisions about their own healthcare, and new technologies enable and facilitate this trend. New type of patient is evolving, similar to retail consumers. These former patients – new healthcare consumers – are driven by desire to take control over own health records and want to take active part in choosing health care providers and services. They are also driven by the desire for more trustworthy, secure and timely healthcare information. Due to this changing role of patients their empowerment has become a key priority for policy makers, professionals and service providers. EU citizens’ role is transforming from passive receivers of health care to active decision makers; and managing own health data and security is important aspect to empowering and creating the trust [12].

On the other hand, current challenges in cyber security are one barrier towards eHealth expansions. The term cyber security is understood here as a key enabler for the development and maintenance of trust in the digital eHealth world. It is important to complement the currently dominating ‘cyber security as a barrier’ perspective by emphasizing the role of ‘cyber security as an enabler’ of new interactions and services - and recognizing that trust is a positive driver for growth and empowerment. Safety and security issues are increasingly dependent on unpredictable cyber risks. If cyber security risks aspects are not made ready, eHealth service providers will face as continuums of disasters over time. However, investing in systems that improve confidence and trust can significantly reduce costs and improve the speed of interaction in the health sector, for example, homo morphism allows cloud services to be applied as a secure storage medium. From this perspective, cyber security and safety viewpoints should be seen as a key enabler for the development and maintenance of trust in the digital world.

References

[1] ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems – Requirements, International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), 2013.

[2] US Code Title 44, Chapter 35 Coordination of Federal Information Policy, U.S. Government Printing Office, 2008.

[3] ISO/IEC 27032:2012 Information technology — Security techniques — Guidelines for cybersecurity, 2012: International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).

[4] ITU-TX.1205: series X: data networks, open system communications and security: telecommunication security: overview of cybersecurity, International Telecommunications Union (ITU), 2008.

[5] Team Coordination Training, Student Guide, May 2004, United States Department of Homeland Security, 2004.

[6] E. MacAskill and E. Snowden, “NSA files source (2013): 'If they want to get you, in time they will',” The Guardian, 10 June 2013.

[7] E. MacAskill, N. Davies, N. Hopkins, J. Borger and J. Ball, “GCHQ intercepted foreign politicians' communications at G20 summits,” The Guardian, 17 June 2013.

[8] L. Peterson and B. Davie, Computer networks: a systems approach, San Francisco: Morgan Kaufmann Publishers Inc., 2007.

[9] R. Faris and R. Heacock, “Introduction,” in Internet monitor 2013: Reflections on the Digital World, Berkman Center Research Publication No. 27, Harvard University - Berkman Center for Internet & , 2013, pp. 1-9.

[10] A. Cavoukian, “Privacy by Design: The 7 Foundational Principles,” January 2009. [Online]. Available: https://www.ipc.on.ca/images/Resources/7foundationalprinciples.pdf. [Accessed 29 January 2016].

[11] M. Davis, U. Lang and S. Shetye, “A Cybermodel for Privacy by Design: Building privacy protection into consumer electronics,” IEEE Consumer Electronics Magazine, vol. 4, no. 1, pp. 41-49, 2015.

[12] E. Lettieri, L. Fumagalli, G. Radaelli, P. Bertele, J. Vogt, R. Hammerschmidt, J. Lara, A. Carriazo and C. Masella, Empowering patients through eHealth: a case report of a pan-European project, European Commission, 2015.