Funded by the European Commission
Seventh Framework Programme

Cyber ROAD

Development of the Cybercrime and Cyber-terrorism Research Roadmap

Grant Agreement N. **607642**

Healthcare

Author(s): Enrico Frumento (CEFRIEL), Federica Freschi (CEFRIEL)

CC RG-55 and CT RG-55 – Better harmonization of health care protocols and better testing of existing solutions against security (also using Secure Software Development Solutions) against real and modern threats.
CT RG-57 - New ways to protect health records that goes beyond encryption and access control. Monitoring solutions that can track the data either in storage and transmission and detect misuses, breaches and deny of services.

ABSTRACT

Healthcare is increasingly becoming a service-oriented ecosystem. This is based on solid market trends in the wearable industry, social needs of an ageing society and economic sustainability of the healthcare services.
The digital revolution of healthcare started several years ago with the introduction of informatics into hospitals. Nowadays, healthcare operators and patients' worlds are definitely highly digitalized, modifying how healthcare operators and patients offer and use services respectively. Since a few years, healthcare is migrating to an ecosystem logic which consists in the evolution of the hospital, typically seen as a physical place of care, to a distributed network of services for patients, provided in home environments through different channels and technologies. Today's most common style of living in the western-world is to blend working and private lives, largely using digital ecosystems in which personal and professional services coexists and exchange data. One of the most important challenges for healthcare is hence to evolve its services to match these new societal trends. Furthermore, Cybercriminals are adopting corporate best practices and establishing professional businesses in order to increase the efficiency of their attacks against enterprises and consumers. This also implies a major rethink of most of the security solutions adopted in the past years in healthcare.
Today, healthcare is one of the most attacked and promising areas of exploitation for cybercriminals and cyberterrorists due to the overabundance of valuable information and for its nature as a critical infrastructure. The modern healthcare ecosystems can be abused in different ways. As a matter of fact, hospitals became incrementally digitalized often with complex and still largely unsolved security problems, tied to the standards used, the lack of harmonization of services and problems with different roles in the hospitals and harmonizing laws among different countries (especially in Europe). On the other side, advanced attack techniques are becoming extremely flexible, ready to catch all the possible economic advantages.
The solutions for these trends are complex because the problem does not only involve the owner of the data (the user) and the official handler (the health services), but also external actors (e.g. insurances), in some cases also based in foreign countries (e.g. companies selling health monitoring services through wearable bracelets, which are hosting data abroad).

RESEARCH ACTION #1

Better harmonization of health care protocols and better testing of existing solutions against security (also using Secure Software Development Solutions) against real and modern threats.

DISTANCE TO THE MARKET: **TRL 3-4**
COST OF THE TOPIC: **3-5 STREPs + 3- IP**
AVAILABILITY OF COMPETENCE IN EUROPE: **5**
TIME SPAN FOR ADDRESSING THE ACTION: **42 months**
ACTORS: **healthcare operators, research centres specialized in security, security market leaders, healthcare device/solution providers, standardization bodies.**

The cyber threats that evolved, as well as targeted attacks that appeared during the last few years, can be considered as one of the main worrisome trends, especially for high value organizations like hospitals. On one side, the usage of proprietary solutions and the specificity of the used protocols (e.g., DICOM, HL7) kept specialized threats away so far (typically hospitals fell for opportunistic threats, not specifically created for healthcare). On the other side, the increasing number of targeted attacks allows to foresee a change of direction.

Due to the ground-breaking innovative and business driven approaches of latest attacks, most of the previously installed defence solutions do not suffice anymore. A new set of protection mechanisms, going under the names of "threat intelligence" and "analyst-driven solutions" appeared on the market. These mechanisms involve a mixture of human experts and Artificial Intelligence (AI) at different degrees. These new defence systems are often complex enough to require a service oriented approach (often offered as SaaS) and involve AI, trained by humans, where heuristics were used in the past (e.g. the future of antiviruses is foreseen to involve AIs more than heuristics).

Beside these problems, modern hospitals still suffer from another class of issues, that has been addressed for decades: the existing security standards in the eHealth world lack on-field testing against complex real world attacks. Standards specified by SDOs (Standard Developing Organizations) are in use and their robustness has still often not been proven against real modern attacks. After spending millions to upgrade and protect the existing hospital information services. new upgrades to face a completely new set of threats will become necessary. It is important hence to:

1. Protect the data along its whole lifecycle (creation, storage, transmission and destruction) and across all security relevant layers (network, application, device, physical, human).
2. Test the effectiveness of the new defence solutions in the healthcare world.
3. Coordinate and update the existing specific health standards with respect to latest trends and attack techniques.

Protect and train the human capital

DISTANCE TO THE MARKET: **TRL 3-4**
COST OF THE TOPIC: **2 STREPs + 2 IP**
AVAILABILITY OF COMPETENCE IN EUROPE: **5**
TIME SPAN FOR ADDRESSING THE ACTION: **42 months**
ACTORS: **healthcare operators, research centres specialized in security, security market leaders, healthcare device/solution providers, sociologists, cognitive scientists, psychologists, HCI experts, medical staff**

Healthcare is one of the few critical infrastructures whose services could largely survive even in case of a big technological disruption: one of the most important assets of an hospital is the human capital (e.g., physicians and nurses) while technology's main role is to support and increase their overall efficiency. Technology must hence be protected and kept stable because, simplifying, it is the enabling factor through which the hospitals "serve" a large population, but very few energy has been devoted to the protection of people. Today's cybercriminals and cyberterrorists largely use Social Engineering tactics to exploit the human side of security: modern Social Engineering is the crucial step involved in almost all the attacks. This is especially critical, since data protection is not only a matter of privacy protection, but hospitals are increasingly depending on the availability of their data for their daily business of helping patients. With this background, the increasing danger of becoming a paying victim of ransomware is further increased. Thus, not only awareness on the users' side must be increased, but also on the side of HIS-developers,

Nevertheless, solving the problem of Social Engineering is not simple, since, beside the new defence technologies, the only available solution is "awareness". However, generating awareness is still an open problem. However, it is recognized that the best approach should be based on a concrete and profound collaboration among different competences (e.g. psychologists, HCI experts, sociologists, medical staff, cognitive sciences, security experts, ...).

Nevertheless, the most interesting recipes for new awareness strategies in security are all involving the following three elements:

- Gamification: traditional ICT security trainings do not present particular appealing characteristics. In contrast, gamification frames such trainings as hacking games of different formats (e.g., attack-defence capture the flag, jeopardy), fostering competitiveness and promoting problem-solving activities.
- Incidental learning: partial yet continuous learning and knowledge improvement, for example through mini-sessions during the day, trying to avoid monolithic tracks.
- Personalization: adapt the learning experience to individuals' attitudes, habits and mind-sets.

The healthcare sector, more than others, is a special test area for improving awareness strategies, because of the specific mind set of healthcare operators which makes them particularly vulnerable to Social Engineering attacks. The natural predisposition of healthcare operators to support others (second opinions and collaborations are an everyday best practice in medicine), together with their continuous exposure to different technologies and at the same time their relatively low training in security, makes them the perfect victims of cyber threats.

Junction of cyber and real threats

DISTANCE TO THE MARKET: **TRL 5**
COST OF THE TOPIC: **4 STREPs + 2 IP**
AVAILABILITY OF COMPETENCE IN EUROPE: **5**
TIME SPAN FOR ADDRESSING THE ACTION: **42 months**
ACTORS: **healthcare operators, research centres specialized in security, Law Enforcement Agencies, security market leaders, healthcare device/solution providers**

Cybercrime and Cyberterrorisms are converging to the same strategies and business models as traditional crime and terrorisms, thus resulting in an increased blending of cybercrime and crime and a commonality of interests between cyberterrorism and terrorism. What is starting to appear, in the evidences collected, is a multi-staged approach to threats and a coordination of efforts aimed at reaching a final goal: for example, disrupting the Hospital Information Services (HIS) through ransomware in conjunction with a terrorist attack, could be used to increase the ensuing social "chaos" and to reduce the hospitals efficiency when it would be needed most.

Healthcare is double exposed to these problems because of its nature as a critical infrastructure and the extreme value of its assets (the Personal Healthcare Information –PHI– and Personal Identifiable Information –PII–) for either citizens and the black market. It will be beneficial to investigate the exposure of the critical infrastructures and especially healthcare with respect to the following topics:

1. Conjunction of cybercrime and traditional crime, for example the increasing probability of cyber-murders through e.g. exploitation of life-support devices. The objective could be:
    a. Investigation: understanding the economic and strategic plans of criminals and terrorists from an attackers' point of view.
    b. Mitigation: fostering the adoption and adaptation of e.g. secure code development best practices at all the technological levels in healthcare and promoting official certifications in order to reduce the attack surface.
2. Coordination of efforts between cyber threats and terroristic acts in order to amplify the effects of a terrorist attack. Mitigation means:
    a. Improving the investigation efforts and the inter-force coordination among LEAs and healthcare operators.
    b. Further studying the possible blending of real and cyber threat models (either by an economic or strategic point of view).