Exploring Security Issues in Telehealth Systems

Gastón Márquez
gaston.marquez@sansano.usm.cl

Hernán Astudillo
hernan@inf.utfsm.cl

Carla Taramasco
carla.taramasco@uv.cl

UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA

7oeska

Universidad
de Valparaíso
CHILE

1st International Workshop on
Software Engineering for Healthcare
(SEH 2019)

In conjunction with ICSE 2019
May 27th, 2019, Montréal, QC, Canada.

Table of contents

Table of contents

1 Background

2 Problem

3 Proposal

4 Results

5 Findings

6 Challenges

7 Conclusions

Telehealth systems

- **Telehealth systems** are telecommunication technology that support and promote long-distance clinical health care, patient and professional health-related education, public health and health administration

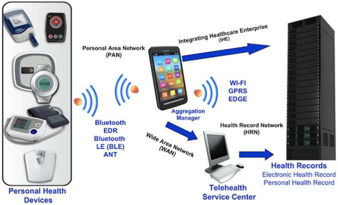


Figure 1: TeleHealth systems overview (www.rednewswire.com)

Telehealth systems [*Security*]

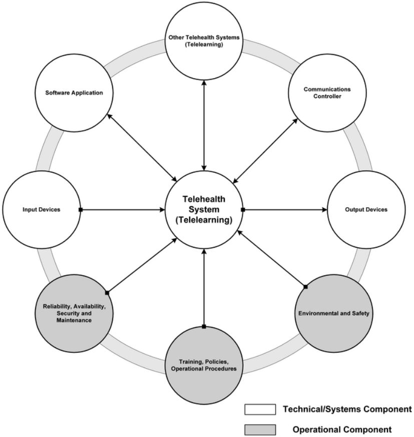

Other Telehealth Systems (Telelearning)
Software Application
Communications Controller
Input Devices
Telehealth System (Telelearning)
Output Devices
Reliability, Availability, Security and Maintenance
Environmental and Safety
Training, Policies, Operational Procedures
Technical/Systems Component
Operational Component

Figure 2: ISO/TS 16058:2004 Telehealth reference architecture[1]

[1] https://www.iso.org/obp/ui/fr/iso:std:iso:ts:16058:ed-1:v1:en:fig:7

Telehealth systems [*Security*]

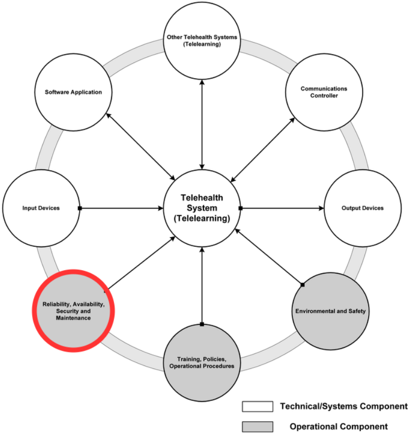

Other Telehealth Systems (Telelearning)
Software Application
Communications Controller
Input Devices
Telehealth System (Telelearning)
Output Devices
Reliability, Availability, Security and Maintenance
Environmental and Safety
Training, Policies, Operational Procedures
Technical/Systems Component
Operational Component

Figure 2: ISO/TS 16058:2004 Telehealth reference architecture[2]

[2] https://www.iso.org/obp/ui/fr/iso:std:iso:ts:16058:ed-1:v1:en:fig:7

Telehealth systems [*Security*]

- Health organizations are using the benefits of emerging technologies, such as robotics, mobile, The Internet of Things (IoT), and others to provide better remote services to their patients.
- This adoption brings various benefits to patient care, but also leads to new challenges, such as *security*.

Telehealth systems [*Security*]

- Reports and surveys from the Center for Connected Medicine[3] describe that
  - Hackers and other cyber-criminals are stepping up their attacks on the health care industry
  - 87% respondents say they expect to increase spending on cyber-security in 2019
  - Health system executives were not uniformly confident in their ability to recover quickly from cyber-attacks

[3] https://www.connectedmed.com/blog/content/top-of-mind-2019-interoperability-cybersecurity-telehealth

Table of contents

Telehealth systems [*Problem*]

- Although researchers and practitioners have reported several security issues related to Telehealth systems, there is **not a clear vision** about which *type* of security issues Telehealth systems must face and which telehealth components and medical supplies are affected.
- Moreover, it is also **not explicit** which solutions have been proposed for these issues and which is the role of Software Engineering (SE) in this context.

Table of contents

1. Background
2. Problem
3. Proposal
4. Results
5. Findings
6. Challenges
7. Conclusions

Telehealth systems [*Proposal*]

- We propose a **systematic mapping study** in order to detect and characterize security issues in Telehealth systems.
- The goals are
    - Illustrate an *updated map of state of the art* in security issues in Telehealth systems
    - *Identify security issues* concerning Telehealth systems
    - *Classify security solutions* according to their strategy, target problem, proposal and technique or method used
    - Discuss the *role of SE* in the development of secure Telehealth Systems

Process

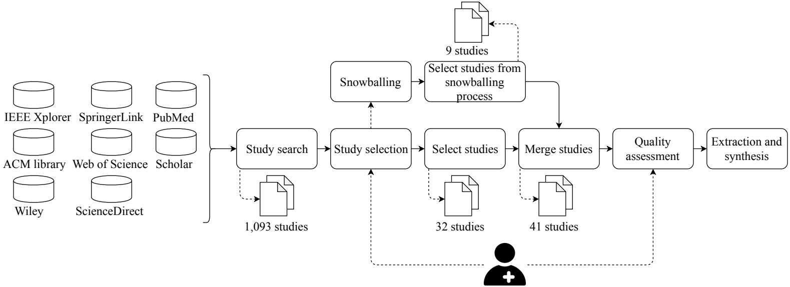


Figure 3: Mapping review process

- We invited healthcare professionals to review and discuss the study selection and selection criteria

Research questions

- RQ1: *Which are the **research approaches** associated with security in Telehealth systems?*
    - *Purpose*: Publication years, publication venues, research strategies, and target problems
- RQ2: *Which **security issues** have been reported in Telehealth systems?*
    - *Purpose*: Security issues (such as attacks, vulnerabilities, and others) and components affected
- RQ3: *Which **solutions** have been proposed for security issues in Telehealth systems?*
    - *Purpose*: Proposals, techniques and methods

Table of contents

1. Background
2. Problem
3. Proposal
4. Results
5. Findings
6. Challenges
7. Conclusions

RQ1: Research approaches *[Publication years and venues]*

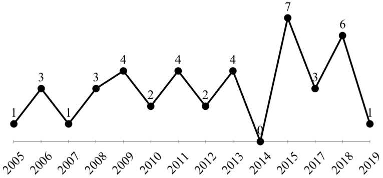


Figure 4: Publication years

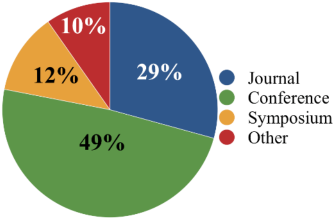


Figure 5: Publication venues

- During 2015 there is an increase in publications, which subsequently, is maintained during 2018

- Most publications focused on conferences and journals

RQ1: Research approaches [*Research strategies*]

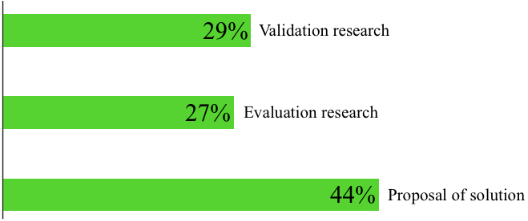


Figure 6: Research strategies

- We used the proposal of Wieringa et al. to classify articles[4]
- Most primary studies are focused on *Proposal of solution*

[4] Wieringa, R., Maiden, N., Mead, N., Rolland, C. (2006). Requirements engineering paper classification and evaluation criteria: a proposal and a discussion. Requirements engineering, 11(1), 102-107.

RQ1: Research approaches [*Target problems*]

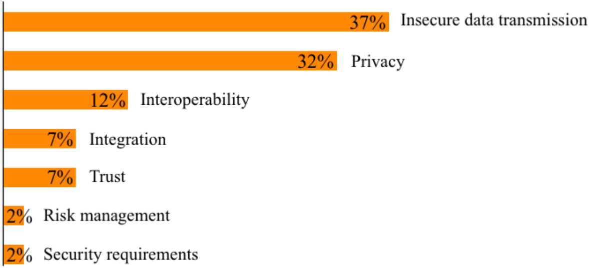


Figure 7: Target problems

- Through consensus-based filtering, we filtered the problems, and we recognized 7 common target problems

RQ2: Security issues

- **5 Attacks** (*Information security incident that involves an attempt to obtain, alter, destroy, remove, implant or reveal information without authorized access or permission*)
- **4 Vulnerabilities** (*Cyber-security term that refers to a flaw in a system that can leave it open to attack*)
- **2 Threats** (*Anything that has the potential to cause serious harm to a computer system*)
- **1 Weakness** (*Flaws, faults, bugs, and other errors in software implementation, code, design, or architecture that if left unaddressed could result in systems and networks being vulnerable to attack*)

RQ2: Security issues [*Attacks* (1/2)]

- *Privilege escalation attacks*: Network intrusion that takes advantage of **programming errors** or **design flaws** to grant the attacker elevated access to the network
- *Sensors-based covert channels attacks*: Attacks that allows the communication of information by **transferring objects** through existing information channels
- *Tags attacks*: Attacks which its target is the **identification** of Radio Frequency Identification Systems

RQ2: Security issues [*Attacks* (2/2)]

- *Device Mis-Bonding (DMB) attacks*: A DMB attack targets the mobile gateway running the Google Android Operating System
- *Offline dictionary attacks*: Attacks where hackers **steal the password storage file** from the target system

RQ2: Security issues [*Vulnerabilities*]

- *Denial of Service*: **Interruption** of the devices normal functioning
- *Data secrecy vulneration*: A vulnerability that compromises **the patient's personal data**
- *Identity theft*: Acquisition of critical information about someone in order to impersonate them and commit **various crimes** in that person's name
- *Open Web Application Security Project (OWASP) vulnerabilities*

RQ2: Security issues [*Threats and weaknesses*]

- *Communication channel threats*: Impossibility to guarantee that every computer on the Internet is **safe and secure**
- *Social threats*: Threats related to **malicious** human behaviors
- *Fail to revoke the stolen/lost smart card (weakness)*: Impossibility of a system to **activate and update** smart cards

RQ2: Security issues *[components and medical supplies]*

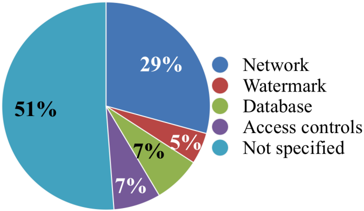


Figure 8: Telehealth components affected by security issues

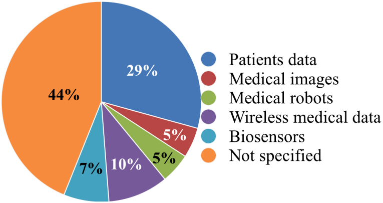


Figure 9: Medical supplies affected by security issues

RQ3: Solutions

- We found several and different solutions
- We classified them using the following categories[5]:
  - Detect attacks (*identify attacks*)
  - Stop or mitigate attacks (*resisting an attack*)
  - React to attacks (*respond to a potential attack*)
  - Recover from attacks (*restore systems once it has detected and attempted to resist an attack*)

[5] Fernandez, E. B., Astudillo, H., Pedraza-García, G. (2015, September). Revisiting architectural tactics for security. In European Conference on Software Architecture (pp. 55-69). Springer, Cham.

RQ3: Solutions

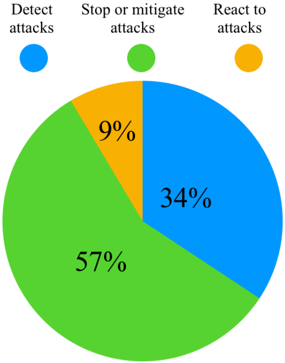


Figure 10: Solutions distribution

- We don’t find solutions related to **recovery from attacks** (which match with the survey results)

RQ3: Solutions

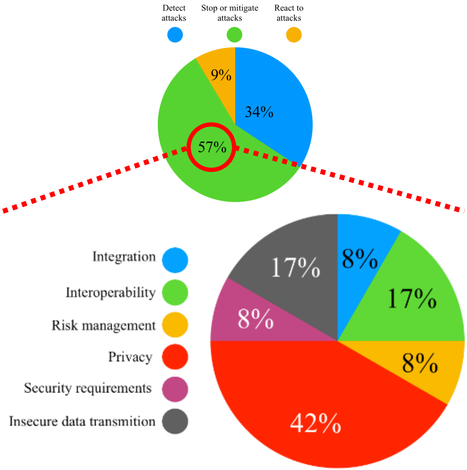


Figure 11: Solutions distribution-Stop or mitigate attacks

RQ3: Solutions

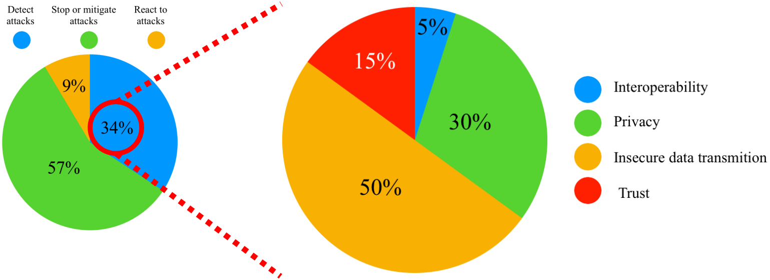


Figure 12: Solutions distribution-Detect attacks

RQ3: Solutions

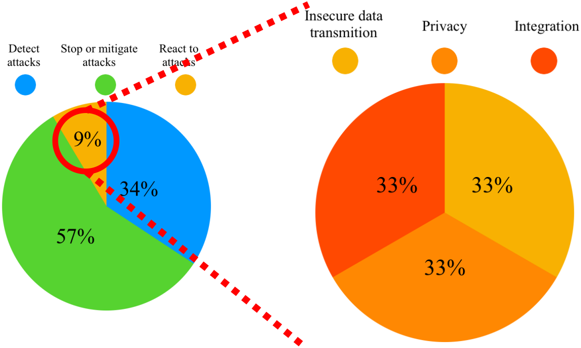


Figure 13: Solutions distribution-React to attacks

Table of contents

1. Background
2. Problem
3. Proposal
4. Results
5. Findings
6. Challenges
7. Conclusions

SE and Telehealth

- SE and security issues in Telehealth Systems
  - Requirements
  - Software architecture
  - Security patterns

Requirements

- *Requirements elicitation is important*
- The developers' inexperience produces security incidents on specific telehealth domains
  - Often, medical doctors and nurses are considered, but other stakeholders (such as nutritionists, social workers, paramedics, and others) should be considered too.

Software architecture

- *Lack of discussion about architectural styles*
  - It is not possible to identify if a specific architectural style helps to handle security issues in Telehealth systems
- *Lack of key stakeholders identification*
  - Leaving aside key stakeholders increase the "clinical bias" in the system

Security patterns

- *Lack of recurring architectural solutions*
- The primary studies do not specify if they use *security patterns* in their contributions
    - Security patterns describe solutions to the problem of controlling a set of specific threats through some security mechanism, defined in a given context

Table of contents

Challenges

- *Exponential growth in medical data*: Achieve **confidentiality** and **integrity** in Big Data Telehealth software systems
- *Number of connected Telehealth devices*: Build Telehealth software systems that are highly **interoperable** and **scalable**
- *High availability on Telehealth devices*: Build non-monolithic and flexible Telehealth systems in order to provide **high availability**

Challenges

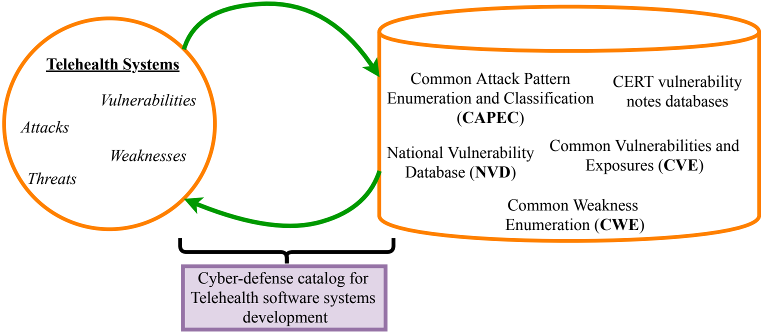

Telehealth Systems
Vulnerabilities
Attacks
Weaknesses
Threats
Common Attack Pattern Enumeration and Classification (CAPEC)
CERT vulnerability notes databases
National Vulnerability Database (NVD)
Common Vulnerabilities and Exposures (CVE)
Common Weakness Enumeration (CWE)
Cyber-defense catalog for Telehealth software systems development

Figure 14: Future research

SEH 2019

Background

Problem

Proposal

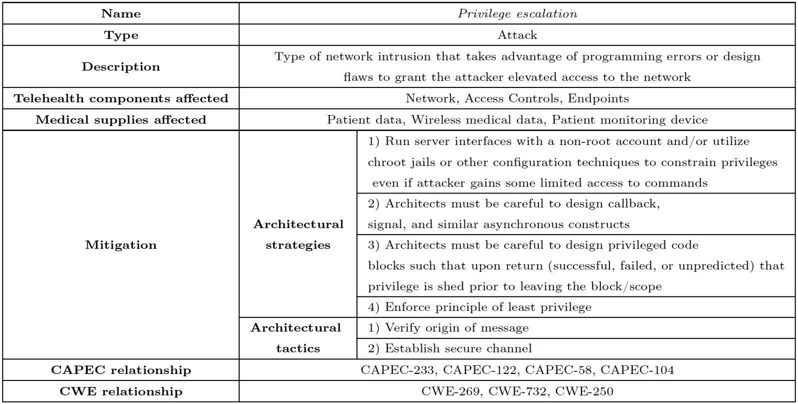
Results

Findings

Challenges

Conclusions

Challenges



Name	*Privilege escalation*	
Type	Attack	
Description	Type of network intrusion that takes advantage of programming errors or design flaws to grant the attacker elevated access to the network	
Telehealth components affected	Network, Access Controls, Endpoints	
Medical supplies affected	Patient data, Wireless medical data, Patient monitoring device	
Mitigation	**Architectural strategies**	1) Run server interfaces with a non-root account and/or utilize chroot jails or other configuration techniques to constrain privileges even if attacker gains some limited access to commands
		2) Architects must be careful to design callback, signal, and similar asynchronous constructs
		3) Architects must be careful to design privileged code blocks such that upon return (successful, failed, or unpredicted) that privilege is shed prior to leaving the block/scope
		4) Enforce principle of least privilege
	Architectural tactics	1) Verify origin of message
		2) Establish secure channel
CAPEC relationship	CAPEC-233, CAPEC-122, CAPEC-58, CAPEC-104	
CWE relationship	CWE-269, CWE-732, CWE-250	

Figure 15: Catalog example

SEH 2019

Background

Problem

Proposal

Results

Findings

Challenges

Conclusions

Table of contents

1. Background
2. Problem
3. Proposal
4. Results
5. Findings
6. Challenges
7. Conclusions

Conclusions

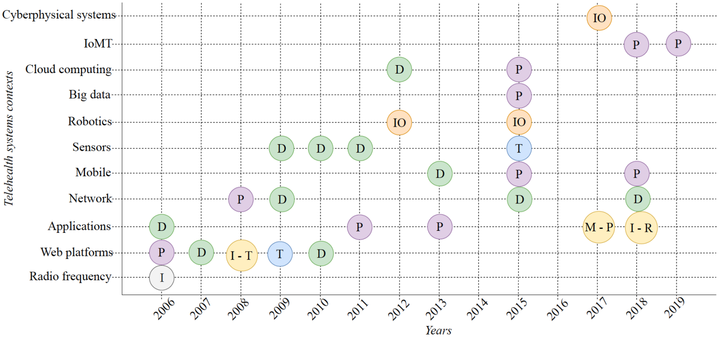


Figure 16: Evolution of target problems according to Telehealth systems contexts and years

Conclusions

- Security concerns on Telehealth systems cover several contexts such as mobile, cloud, robotics, and others
- Requirements, software architecture, and security patterns have a significant role in addressing security requirements

Exploring Security Issues in Telehealth Systems

Gastón Márquez
gaston.marquez@sansano.usm.cl

Hernán Astudillo
hernan@inf.utfsm.cl

Carla Taramasco
carla.taramasco@uv.cl

UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA

Toeska

Universidad
de Valparaíso
CHILE

1st International Workshop on
Software Engineering for Healthcare
(SEH 2019)

In conjunction with ICSE 2019
May 27th, 2019, Montréal, QC, Canada.