SAFEguard of Critical Health infrastructure

SAFECARE Project Overview

Isabel Praca
icp@isep.ipp.pt

SAFECARE has received funding as part of the “Secure societies – Protecting freedom and security of Europe and its citizens” challenge of the Horizon 2020 Research and Innovation programme of the European Union under grant agreement 787002
'Paramedic Of The Year' Arrested For Stealing Covid Vaccines In Florida

Nicholas Reimann  Forbes Staff

Security Blogwatch

WHO attacked by hackers, mid-pandemic, confirms CISO

Nawal Bensalem

Prosecutors open homicide case after cyber-attack on German hospital

Cyber gangsters hit UK medical firm poised for work on coronavirus with Maze ransomware attack

Arizona man steals dozens of coronavirus testing kits from health clinic

Hackers steal Pfizer/BioNTech COVID-19 vaccine data in Europe, companies say

The rapid deployment of remote testing, telehealth, and temporary hospitals amid COVID-19 has significantly increased vulnerabilities in healthcare, which could have lasting impacts beyond the crisis.
Challenge for health systems managers

• 3 perimeters that overlap and collaborate:
  • Medical devices
  • Building management
  • Medical data and software

• Polymorphic, agile, and combined threats: today and tomorrow, a strong attraction for cybercriminals and terrorists

• A strong dependence between assets and complex impact chains... that can affect the lives of patients and staff

• Paradoxically: A lot of information in specialized supervision systems without communication or integration

Need for a global vision in anticipation, protection, and crisis management
## Scenarios Definition

<table>
<thead>
<tr>
<th>Objective</th>
<th>Covered by</th>
</tr>
</thead>
</table>
| To improve risk prevention capacities: analysis of vulnerabilities, risk assessment and recommendations on operational active systems. | - Identification of critical assets in health infrastructures  
- Requirements analysis & crisis management lexicon  
- Definition of the cyber-physical scenarios of threat  
- Cyber-physical risk assessment and impact analysis |
| Increase the compliance between security solutions and domain-specific requirements in terms of ethics and privacy. | - Analysis of ethics, privacy and confidentiality constraints  
- Implementation of ethics, privacy and confidentiality |
Scenarios Definition

**TYPES OF REPORTED ATTACKS RELATED TO COVID-19**

- Physical Assault
- Denial of Services
- Psychological Threat
- Obstruction
- Eviction from Home
- Individual Weapon
- Heavy Weapon
- Cyber Attack

Note: This infographic aims to portray the different types of attacks identified through secondary sources or the reports on the Surveillance System for Attacks on Health Care (SSA). This is not an exhaustive list of all types of attacks under WHO's definition of Attacks on Health Care.
Scenarios

- Sc1: Cyber-physical attack targeting **power supply** of the hospital
- Sc2: Cyber-physical attack to steal **patient data** in the hospital
- Sc3: Cyber-physical attack **targeting IT systems**
- Sc4: Cyber-physical attack to cause a **hardware fault**
- Sc5: Cyber-physical attack targeting the **air-cooling system** of the hospital
- Sc6: Cyber-physical attack on **medical devices**
- Sc7: Cyber-physical attack **to steal credentials** to access IT systems
- Sc8: Cyber-physical attack in access control provider **to steal medical devices**
- Sc9: Physical attack against hospital **staff using a gun**
- Sc10: Physical attack **to steal drugs - vaccines (COVID)**
- Sc11: Cyber-physical attack **due to a personal laptop**
- Sc12: Cyber-physical attack to **block national crisis management**
Cyber Physical Scenarios

Cyber-physical attack targeting the air-cooling system of the hospital:

- Break the door
- Steal key/badge
- Identification of the temperature sensor
- Identifying the PLC of the air cooling system
- Spear phishing email
- Virus seeds expand
- Data center crash
- Air cooling does not start and temperature increases
- Contaminated

SAFECARE
(integrated cyber-physical security for health services)
Scenarios and Risks Assessment

Scenarios Definition

Risk assessment

Bowtie Method

National Health Agency

Population

Health practitioners

Police & Firefighters

SOC Operators

Building Security Agents

Scenarios and risk assessment
Scenarios Risk assessment
High Level Architecture
## Physical Security Solutions

<table>
<thead>
<tr>
<th>Objective</th>
<th>Covered by</th>
</tr>
</thead>
</table>
| O1: To develop intelligent modules and integrate efficient technologies to improve physical security. |  - Suspicious behaviour detection.  
  - Intrusion and fire detection. |
| O3: Provide cost-effective solutions taking into account the latest financial restrictions within the European Union. |  - BTMS based on existing Video Mgt. System, XProtect. |
| O4: To develop intelligent modules to integrate different data sources and better take into account the combination of physical and cyber security threats. |  - Integration of data collection, and cyber incidents / impact models, via Data Exchange Layer. |
| O6: To improve threat detection capacities: data fusion, analytics, cascading effects models, notification of alerts. |  - Implementation of complex events, e.g. tailgating, via rule engine, to alarm system of BTMS. |
Physical Security Solutions

- Suspicious Behavior Detection system
- Intrusion and fire detection system
- Ubiquitous services for integrated alert system
- Data Collection from physical subsystems
- Building threat monitoring system
Physical Security Solutions

- Dangerous object
- Loitering in restricted areas
- Covered face
- Tailgating
Physical Security Solutions

Data Collection
Physical Security Solutions

Integrated mobile alerting system
# Cyber Security Solutions

## Objectives

<table>
<thead>
<tr>
<th>Objectives</th>
<th>Covered by</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cover cyber-security aspects related to e-Health, IT and BMS systems in health services</td>
<td>IT threat detection system</td>
</tr>
<tr>
<td></td>
<td>BMS threat detection system</td>
</tr>
<tr>
<td></td>
<td>Advanced file analysis system</td>
</tr>
<tr>
<td></td>
<td>E-health devices security analytics</td>
</tr>
<tr>
<td></td>
<td>Cyber threat monitoring system</td>
</tr>
<tr>
<td>Increase prevention and detection capabilities on threats and Advanced Persistent Threats (APT) in health services and infrastructures</td>
<td>IT threat detection system</td>
</tr>
<tr>
<td></td>
<td>BMS threat detection system</td>
</tr>
<tr>
<td></td>
<td>Advanced file analysis system</td>
</tr>
<tr>
<td></td>
<td>E-health devices security analytics</td>
</tr>
<tr>
<td></td>
<td>Cyber threat monitoring system</td>
</tr>
<tr>
<td>Provide monitoring tools in order to improve cyber threat detection, to report the appropriate level of risks and to enhance incident response</td>
<td>IT threat detection system</td>
</tr>
<tr>
<td></td>
<td>BMS threat detection system</td>
</tr>
<tr>
<td></td>
<td>Advanced file analysis system</td>
</tr>
<tr>
<td></td>
<td>E-health devices security analytics</td>
</tr>
<tr>
<td></td>
<td>Cyber threat monitoring system</td>
</tr>
<tr>
<td>Send cyber incidents to the central database toward and integrated solution (WP6) covering both physical and cybersecurity threats</td>
<td>IT threat detection system</td>
</tr>
<tr>
<td></td>
<td>BMS threat detection system</td>
</tr>
<tr>
<td></td>
<td>Advanced file analysis system</td>
</tr>
<tr>
<td></td>
<td>E-health devices security analytics</td>
</tr>
<tr>
<td></td>
<td>Cyber threat monitoring system</td>
</tr>
</tbody>
</table>
Cyber Security Solutions

Airbus

- BMS threat detection system
- IT threat detection system
- Advanced file analysis system

Cyber threat monitoring system

E-health device security analytics
Cyber Security Solutions
E-health device security analytics

E-health devices in scope concern **radiology equipment**, which may be generalized to include automated syringe, any electronic equipment fixed on the patient catheter, scanners, and medical database
- risk model
- security analytics solution
Cyber Security Solutions
BMS threat detection system

![Forescout Network Map](image-url)
Cyber Security Solutions
Advanced File Analysis System
Cyber Security Solutions
IT threat detection system
Cyber Security Solutions

Cyber Threat Monitoring System
## Integrated Solutions

<table>
<thead>
<tr>
<th>Objectives</th>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>To develop intelligent modules to integrate different data sources and better take into account the combination of physical and cyber security threats.</td>
<td>Data exchange layer</td>
</tr>
<tr>
<td>To improve risk prevention capacities: analysis of vulnerabilities, risk assessment and recommendations on actual active systems.</td>
<td>Central database</td>
</tr>
<tr>
<td>To improve threat detection capacities: data fusion, analytics, cascading effects models, notification of alerts.</td>
<td>Impact propagation model and decision support model</td>
</tr>
<tr>
<td>To improve threat response capacities: defence strategies, reaction cards, automated processes (bpm).</td>
<td>Threat response and alert system</td>
</tr>
<tr>
<td>To improve impact mitigation capacities: manage hospital availability, inform the population, and increase user awareness about impacts on critical assets.</td>
<td>Hospital Availability Management System</td>
</tr>
<tr>
<td></td>
<td>E-health security risk management model</td>
</tr>
</tbody>
</table>
Integrated Solutions

- Threat Response and alert system
- Impact Propagation and Decision Support
- Hospital availability management system
- E-health security risk management model

Data Exchange layer

Central Database
Integrated Solutions

Data Exchange Layer  The Heart of the Integrated Solutions

Central Database

- Assets
- Events
- IT Assets
- Alerts
- incidents

Data Exchange layer

Central Database

All SAFECARE system
Integrated Solutions
Impact Propagation and Decision Support

A model capturing assets, theirs relationships and related security concepts
A set of rules managing impacts propagation
Integrated Solutions

Hospital availability management system
Integrated Solutions

Threat response and alerting system
End-Users Training

• Training process (plan; prepare; facilitate and; evaluate)
• E-learning platform, based on LMCS Moodle, called Smart Life Long Learning (Smart3L)

* Planning training process (user-groups; training goal and objectives; training framework; training modules and content; training methods and delivery tools; evaluation methodology)
Simulation and Tests Platform

- Simulation Platform
  - Integration of all solutions
  - Pilots workzone (confidential)
  - Scenarios simulation
Simulation and Tests Platform

WP6 - Integrated cyber-physical security solutions

- IP & DS (T6.4)
- HAMS (T6.6)
- DXL (T6.2)
- CDB (T6.3)

WP4 - Physical Security Solutions

- SBS (T4.1)
- IFDS (T4.2)
- DCS (T4.3)
- MAS (T4.4)
- BTMS (T4.5)

WP5 - Cyber Security Solutions

- CTMS (T5.5)
- BMS TDS (T5.2)
- Malware A (T5.3)
- IT IDS (T5.1)

Cyber Range

- SBS (T4.1)
- IFDS (T4.2)
- DCS (T4.3)
- MAS (T4.4)
- BTMS (T4.5)
- DXL (T6.2)
- CDB (T6.3)

SIMULATION & TESTING SYSTEMS

- le cnam
- LINKS

Cyber Range

- IT IDS (T5.1)
Tests and Demonstration

Test Platform

Cyber Range

Pilots

Marseille

Turin

Amsterdam
Scientific activities

4 events organised.

4 chapters written for ECSCI book; 7 open access publications and extra conference proceedings.

Workshop organised in September 2020

Website traffic growth.
Scientific activities

Special Issue "Cyber-Physical Security for Critical Infrastructures"

- Print Special Issue Flyer
- Special Issue Editors
- Special Issue Information
- Keywords
- Published Papers

A special issue of *Journal of Cybersecurity and Privacy* (ISSN 2594-806X).

IEEE CBMS Special Track on:
Security of e-Health Systems and Connected Medical Devices

Thank you!

More details available on:
- Our website: [https://www.safecare-project.eu/](https://www.safecare-project.eu/)
  - Twitter: @SafecareP
  - LinkedIn: SAFECARE Project

Isabel Praça
icp@isep.ipp.pt