TOWARDS METRICS-DRIVEN ADAPTIVE SECURITY MANAGEMENT IN E-HEALTH IoT APPLICATIONS

Reijo M. Savola\textsuperscript{1}, Habitamu Abie\textsuperscript{2}, Markus Sihvonen\textsuperscript{3}
\textsuperscript{1}VTT Technical Research Centre of Finland, FI
\textsuperscript{2}Norwegian Computing Center, NO
\textsuperscript{3}Mikkelin Puhelin Oyj, FI

SeTTIT 2012
Oslo, Norway
CONTENTS

• Introduction
• High-Level Security Objectives
• Proposed Adaptive Security Approach
• Conclusions and Future Work

"An activity cannot be managed well if it cannot be measured."

Reijo Savola, SeTTIT 2012, Oslo, Norway
INTRODUCTION
Number of people with chronic diseases on the rise

- **Diabetes**: rising from 171 million (2000) > 366 million (2030) according to WHO
- **COPD**: (Chronic Obstructive Pulmonary Disease), rising, major cause of chronic morbidity and mortality worldwide
- **Arthritis**: rising

Immediate and effective preventive actions are needed to reserve the trend!

- Self-care support by technology is very promising direction!
INTRODUCTION

Use of IoT technology in self-care

Healthcare Provider A

- Private E-Health Database
- Shared E-Health Database
- Doctor
- Other relevant systems

Healthcare Provider B

- Private E-Health Database
- Doctor
- Other relevant systems

Senior Service Company

- Services
- Other Services
- Private E-Health Database
- Other relevant systems

Gateway

- Motion detector
- Well-being wristband
- Blood glucose meter
- Other sensor

Reijo Savola, SeTTIT 2012, Oslo, Norway
INTRODUCTION
Collaboration and adaptiveness in security/privacy

• Controlled collaboration and information sharing needed
  • Healthcare providers can change
  • People travel a lot
• Support for adaptiveness is crucial
  • Security and privacy risks change dynamically
• **Sufficient** security and privacy level should be maintained during the changes

Reijo Savola, SeTTIT 2012, Oslo, Norway
**INTRODUCTION**

Communication levels, security domains

*Leister et al.:

<table>
<thead>
<tr>
<th>CL</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Patient</td>
</tr>
<tr>
<td>1</td>
<td>Personal sensor network like BSN (Biomedical Sensor Network). The sensors form BSN.</td>
</tr>
<tr>
<td>IIa</td>
<td>Paramedic scenarios</td>
</tr>
<tr>
<td>IIb</td>
<td>Smart home scenarios.</td>
</tr>
<tr>
<td>IIc</td>
<td>Mobility scenarios.</td>
</tr>
<tr>
<td>IId</td>
<td>Intensive care or surgery.</td>
</tr>
<tr>
<td>IIe</td>
<td>Pre- or postoperative sensor data management</td>
</tr>
<tr>
<td>III</td>
<td>Healthcare information system comprising the hospital network, computing facilities, databases and access terminals in the hospital.</td>
</tr>
</tbody>
</table>

**Proposal of additional levels:**

| IIIa | Utilization of BSN data by medical doctors and other healthcare personnel in non-emergency treatment of individual patient with a chronic disease. |
| IV   | Information sharing between different healthcare providers concerning medical information of an individual patient. |
| V    | Information sharing between healthcare providers and medical research organizations for the purposes of research, new solutions development and feedback to CL 0-IV. |
HIGH-LEVEL SECURITY OBJECTIVES
Authentication and authorization

High-level objectives

• **End-user and sensor authentication**: adequate authentication strength is a highly critical parameter in ensuring that the right person receives the right treatment.

• **Service provider user authentication and authorization**: (1) take different privacy levels into account, (2) define pre-authorized roles to indicate the type of data that a person can access.

• Usability of authentication mechanism(s) is emphasized especially for seniors.

Adaptivity need

• Support changing context of use, security threats, privacy requirements, and user behavior.

• Setting requirements and enforcing mechanisms.
HIGH-LEVEL SECURITY OBJECTIVES
Data integrity

High-level objectives

• Especially in paramedic situations, lost, delayed or altered data can cause direct damage to the patient’s health. Moreover, indirectly, data integrity is important to longer-time treatment decisions.

Adaptivity need

• Carefully designed adaptation needed especially during alarm situations.
HIGH-LEVEL SECURITY OBJECTIVES
Privacy and confidentiality

High-level objectives
• Privacy and confidentiality are very emphasized in healthcare information systems.
• Strong confidentiality algorithms, key management and associated processes are crucial.
• Compliance to privacy legislation and regulations are needed despite of varying use cases.

Adaptivity need
• Adaptation to privacy and confidentiality requirements needs to take into account data processing needs, roles of stakeholders, regulations/legislation and privacy level information.
High-level objectives

• Availability of sensor data are important especially in paramedic and alarm situations.
• Availability of the service provider’s systems can be critical for health and life.

Adaptivity need

• Adaptive techniques are needed to balance the load in the system and to use resilience solutions to maintain adequate availability.
High-level objectives

• Non-repudiation can be potentially a challenge especially in senior citizen care and in medical alarm situations.
• Sufficient non-repudiation solutions for these challenging situations are needed.

Adaptivity need

• Adaptive techniques are needed to ensure the adequate non-repudiation level despite of changing conditions.
Adaptive security involves

- Gathering contextual information,
- Measuring security level and metrics,
- Analyzing the collected information and responding to changes by:
  - Adjusting internal working parameters (like encryption schemes, security protocols, security policies, algorithms authentication and authorization mechanisms and QoS)
  - Making dynamic changes in the structure of the security system.
PROPOSED ADAPTIVE SECURITY APPROACH

Adaptive security management model

Adaptive Monitoring
- Reporting
- History, real time data & metrics
- Sensors

Analytics & Predictive Models
- Machine learning
- Game theory
- Rule-based reasoning
- Context awareness

Adaptive Security Models
- Decision making
- Security and privacy
- Actuators

Metrics-based Adaptive Security Models
- Security metrics and measurement
- Simulation and Verification
- Requirements and Design based metrics

Sul IoT: Things, and their Interactions and Environments

Feedback to Medical Expert

Reijo Savola, SeTTIT 2012, Oslo, Norway
Security metrics objectives

- **SECURITY CONTROL**
  - Security controls are means of managing privacy risk, which can be administrative, technical, management, or legal in nature (based on ISO/IEC 27000’s security control concept)

- **SECURITY CONTROL CORRECTNESS**
  - Security correctness denotes assurance that privacy controls have been rightly implemented in the SuI, and the system, its components, interfaces and the processed data meet privacy requirements.

- **SECURITY CONTROL EFFECTIVENESS**
  - Security effectiveness denotes assurance that stated privacy objectives are met in the SuI and expectations for resiliency in the use environment are satisfied, while the SuI does not behave in any other way than what is intended.

- **SECURITY CONTROL EFFICIENCY**
  - Security efficiency denotes assurance that the adequate privacy quality has been achieved in the SuI meeting resource, time and cost constraints.
PROPOSED ADAPTIVE SECURITY APPROACH

Risk-driven = Top-down metrics development

(1) Identify successive components from each security requirement

(2) Examine the subordinate nodes to see if further decomposition is needed. If so, repeat (1) and (2).

(3) Terminate the decomposition when none of the leaf nodes can be decomposed any further.

E.g. authentication:

In practice: The same example is >100 detailed metrics

PROPOSED ADAPTIVE SECURITY APPROACH
Factors contributing to security effectiveness

Security Effectiveness Assessment of a Software System

- Security correctness measurement (configuration, correct deployment, etc.)
- Software and system quality measurement (e.g. vulnerability management)
- Direct (partial) security effectiveness measurement
- Support of other security controls, e.g. organisational

Security measurement

Confidence on measurement
PROPOSED ADAPTIVE SECURITY APPROACH
Gaps and biases – metrics can help!

Security effectiveness measurement objectives

Inherent security risks of the SUL

Identified and prioritized risks from Risk Analysis

B_RA

G_RA

Security Objectives

B_SO

B_RA

G_SO

G_RA

Security Requirements

B_SR

B_SO

B_RA

G_SR

G_SO

G_RA

Security Control realization

B_SC

B_SR

B_SO

B_RA

G_SC

G_SR

G_SO

G_RA

Improvement potential

Achieved security effectiveness

Improvement potential

Security correctness α

Security correctness β

Security correctness γ

Figure: Savola, R., Frühwirth, C., Pietikäinen A., "Risk-driven security metrics in agile software development – an industrial pilot study". Accepted to Journal of Universal Computer Science, 2012.
CONCLUSIONS AND FUTURE WORK

- Security objectives of e-health IoT scenarios are specific
  - Need to share information
  - High privacy regulation
  - Paramedic and alarm situation are a challenge
  - Usability is a challenge
- Adaptive security management is needed for
  - Setting the sufficient security requirements
  - Enforcing the adequate security controls in the face of changing security risks and use context
- Informed adaptive security decision-making is based on adequate security metrics
- Future work: (1) detailed analysis and specification of security metrics and adaptive decision-making algorithm, (2) experimentation system
Thank you!
Questions?