SMART HOMES CYBERTHREATS IDENTIFICATION BASED ON INTERACTIVE TRAINING

Zlatogor Minchev & Luben Boyanov

Institute of Information and Communication Technologies
Bulgarian Academy of Sciences

UNDER THE AUSPICES OF

Sofia, UNWE
ICAICTSEE – 2013
December 6, 2013
OUTLINE

- TECHNOLOGICAL CHALLENGES
- STUDIED CONTEXT
- METHODOLOGICAL FRAMEWORK
- PRACTICAL EXPERIMENTS
- DISCUSSION
TECHNOLOGICAL CHALLENGES

Web 1.0
Web 2.0
Web 3.0
Web 4.0
Web 5.0

2000
2050

syssec
THE STUDIED CONTEXT

THE HUMAN FACTOR

SMART HOMES
General Smart Home Organization

Boyanov, 2013

Sensors oriented

Service oriented
Methodological Framework

Present situation

Alternative future 1
Alternative future n

Believes

Morphological Analysis
System Analysis

Brainstorming, discussions, q-based surveys

Formalized believes

Scenario 1
Scenario k

Validated Believes

Results Assessment
Validation

Multicriteria & BSC Analysis

Interactive agent based simulation with environment & users monitoring
Multiaspect survey for web technologies cyber threats evolution 2013
5 years time horizon

<table>
<thead>
<tr>
<th>Technology/Dimension</th>
<th>Civil society</th>
<th>Banks &amp; finances</th>
<th>State governance</th>
<th>Critical Infrastructure</th>
<th>Emerging technologies</th>
<th>Education</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web 1.0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Web 2.0 / Web 3.0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Web 4.0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Web 5.0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Legend:
- Low
- Moderate
- Critical
- Uncertain

~150 participants

Social media trends 2012
Smart Devices Cyberthreats Survey 2013

Technologies

- Smartphone: 24%
- Tablet: 23%
- Laptop: 10%
- Smart TV: 19%
- Robot companions: 6%
- Home automation systems: 4%
- Gaming Consoles: 2%
- Other: 2%

Activities

- Entertainment: 23%
- Household support: 13%
- Everyday work: 41%
- Communications: 23%

Data

- Documents: 45%
- Multimedia: 24%
- Text messages: 26%
- Other: 5%

~ 250 participants
# Smart Homes Cyberthreats Classification 2013

<table>
<thead>
<tr>
<th>Smart Home Services</th>
<th>Possible Threats</th>
<th>Critical Attack Points</th>
<th>Possible Consequences from the Attack</th>
</tr>
</thead>
<tbody>
<tr>
<td>Health Care</td>
<td>DO NOT TAKE MEDICINE, PACEMAKER MALFUNCTIONING, ETC.</td>
<td>SENSORS, VIDEO SURVEILLANCE, COMMUNICATION SYSTEM, INTEGRATING SYSTEM, EXTERNAL COMMUNICATIONS</td>
<td>CRITICAL</td>
</tr>
<tr>
<td>Care for Children or People with Disabilities</td>
<td>REQUIRES ATTENTION</td>
<td>SENSORS, VIDEO SURVEILLANCE, COMMUNICATION SYSTEM, INTEGRATING SYSTEM, EXTERNAL COMMUNICATIONS</td>
<td>CRITICAL</td>
</tr>
<tr>
<td>Security and Safety</td>
<td>INTRUSION</td>
<td>SENSORS, VIDEO SURVEILLANCE, COMMUNICATION SYSTEM, INTEGRATING SYSTEM, EXTERNAL COMMUNICATIONS</td>
<td>CRITICAL</td>
</tr>
<tr>
<td>Care for Children or People with Disabilities</td>
<td>REQUIRES ATTENTION</td>
<td>SENSORS, VIDEO SURVEILLANCE, COMMUNICATION SYSTEM, INTEGRATING SYSTEM, EXTERNAL COMMUNICATIONS</td>
<td>CRITICAL</td>
</tr>
<tr>
<td>Home Environment</td>
<td>FIRE, FLOODING, GAS LEAKAGE</td>
<td>SENSORS, VIDEO SURVEILLANCE, COMMUNICATION SYSTEM, INTEGRATING SYSTEM, EXTERNAL COMMUNICATIONS</td>
<td>CRITICAL</td>
</tr>
<tr>
<td>Smart Home Appliance</td>
<td>DOES NOT TURN OFF, TURNS ON/OFF AT WRONG TIME</td>
<td>SENSORS, VIDEO SURVEILLANCE, COMMUNICATION SYSTEM, INTEGRATING SYSTEM</td>
<td>NON-CRITICAL, BUT DANGEROUS</td>
</tr>
<tr>
<td>Privacy</td>
<td>VIOLATION OF PRIVACY, DATA GATHERING</td>
<td>VIDEO SURVEILLANCE, COMMUNICATION SYSTEM, INTEGRATING SYSTEM, EXTERNAL COMMUNICATIONS</td>
<td>NON-CRITICAL BUT DANGEROUS</td>
</tr>
<tr>
<td>Entertainment and Pleasure</td>
<td>MALFUNCTIONING OF THE PLEASURE, COMFORT AND ENTERTAINMENT SYSTEMS</td>
<td>SENSORS, COMMUNICATION SYSTEM, INTEGRATING SYSTEM</td>
<td>NON-CRITICAL</td>
</tr>
</tbody>
</table>
**Morphological Analysis**

1620 scenario combinations

Minchev, Boyanov & Georgiev, 2013

<table>
<thead>
<tr>
<th>Devices</th>
<th>Activities</th>
<th>Communication Medium</th>
<th>Environment Characteristics</th>
<th>Human Factor Characteristics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mobile Smart Devices</td>
<td>Entertainment</td>
<td>Cable Networks</td>
<td>Physical</td>
<td>Bioelectrics</td>
</tr>
<tr>
<td>Home Entertainment Systems</td>
<td>Communication</td>
<td>Wireless Networks</td>
<td>Structural</td>
<td>Spacial</td>
</tr>
<tr>
<td>Home Automation Systems</td>
<td>Everyday Work</td>
<td>Social Networks</td>
<td>Functional</td>
<td>Sensual</td>
</tr>
<tr>
<td>Household Support</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Scenario**

![Scenario Diagram](image)

**Plausible Future**

**Active scenarios**

**Passive scenarios**
System Analysis

Communication Medium

Activities

Devices

Human Factor

Environment

Boyanov & Minchev, 2013
RESULTING CLASSIFICATION

Legend

<table>
<thead>
<tr>
<th>Object</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Communication: Medium: 80, 20, 60</td>
</tr>
<tr>
<td>2</td>
<td>Human Factor: 70, 65, 5</td>
</tr>
<tr>
<td>3</td>
<td>Activities: 30, 65, 35</td>
</tr>
<tr>
<td>4</td>
<td>Environment: 30, 25, 5</td>
</tr>
<tr>
<td>5</td>
<td>Devices: 20, 55, 35</td>
</tr>
</tbody>
</table>
KEY ATTACKS AGENT

ENTERTAINMENT AGENT

DATA STORAGE AGENT

DIGITAL ASSISTANT AGENT

CONNECTIVITY AGENT

HUMAN-IN-THE-LOOP AGENT

MONITORING AGENT

SMART HOME TEST-BED VALIDATION
Practical Experiments
Some Interesting Results

EEG Study

Minchev, 2013
MORE RESULTS

ECG & BODY TEMPERATURE STUDY

Georgiev & Minchev, 2013
**Discussion**

**Studying today’s fast progressing digital world is a complex task. The present communication and living environment in the Web 2.0/Web 3.0 era are just opening an incredibly huge field for different ICT applications. These however are generating a number of cyber threats for their users. The present methodological study based on interactive training of cyber threats nature and human factor response, showed useful support to further improvements in the digital world security evolution.**

The experiments in the study were methodologically supported by: “A Study on IT Threats and Users’ Behaviour Dynamics in Online Social Networks”, DMU03/22, Bulgarian Science Fund, Young Scientists Grant, 2011-2013, www.snfactor.com.

A special gratitude for the context definition and Q-based survey support is given to: EU Network of Excellence in Managing Threats and Vulnerabilities for the Future Internet – SysSec, FP7 Grant Agreement No. 257007, 2010 – 2014, www.syssec-project.eu.
Thank you for the attention!