SECURING SMART HOMES USING INTRUSION DETECTION SYSTEMS

CHRISTOPH HAAR, Erik Buchmann
Hochschule für Telekommunikation Leipzig
E-Mail: haar@hft-leipzig.de

CHRISTOPH HAAR

- 2010-2015 Business Informatics (Bachelor) Martin-Luther-University Halle/Wittenberg, Germany

- 2015-2017 Business Informatics (Master) Martin-Luther-University Halle/Wittenberg, Germany

- Since 2018 Scientific Assistant Hochschule für Telekommunikation Leipzig, Chair for Data Privacy and Security in Information Systems

AGENDA

- 1. Motivation and Objective
- 2. Research Question One
  - Method
  - Requirements
  - Results
- 3. Research Question Two
  - Method
  - Experimental Setup
  - Experimental Procedure
  - Results
- 4. Conclusion

1. MOTIVATION AND OBJECTIVE

- Botnets such as Mirai or Reaper are showing that Smart Home devices are attractive aims for attackers.
- Conventional IDS are not suitable for securing a Smart Home for several reasons.
- We consider IDS for the Smart Home by answering the following research questions:

1) How can an IDS be integrated into a Smart Home operated by private users without IT-Security expertise?

2) Which IDS approaches can be adapted for that purpose?

2. RESEARCH QUESTION ONE – METHOD

- To systematically approach an IDS that secures Smart Homes, we investigate the following four levels.
  - Network Segmentation
  - System Architecture
  - IT-Security Process
  - Contract Liabilities
- Our levels have been compiled from proposals to secure Smart Home networks, from well-known IT-Security concepts, and from challenges discussed in the IDS context.

2. RESEARCH QUESTION ONE – REQUIREMENTS

- Our starting point is a set of three requirements that arise from security challenges for Smart Home devices.
  - Expertise: The user does not need to possess in-depth expertise of technical internals, such as network protocols and IT-Security.
  - Separation: Smart Home devices have dedicated use cases that can be separated from others.
  - Understandability: The interaction between a user and a Smart Home device should be as understandable as possible.

2. RESEARCH QUESTION ONE – RESULT (1/4)

- Network Segmentation

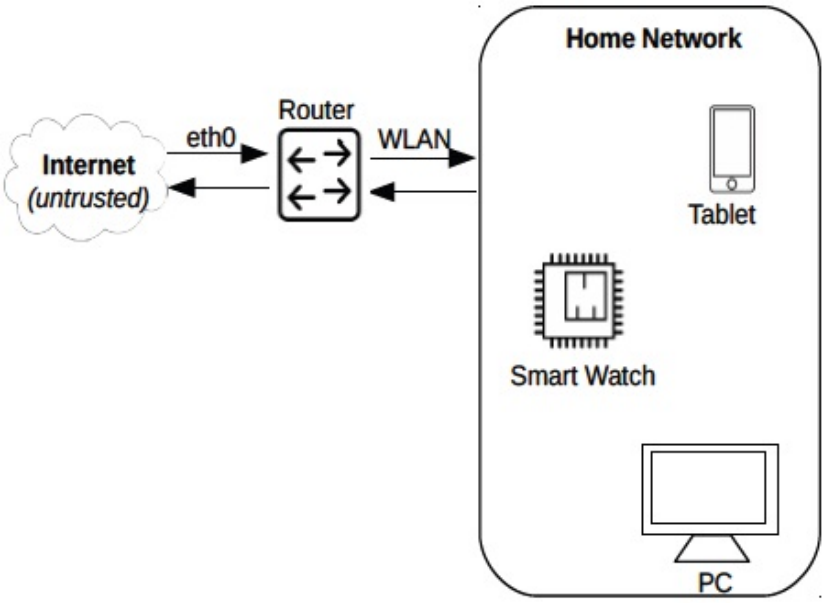

Figure 1: Typical Smart Home Architecture

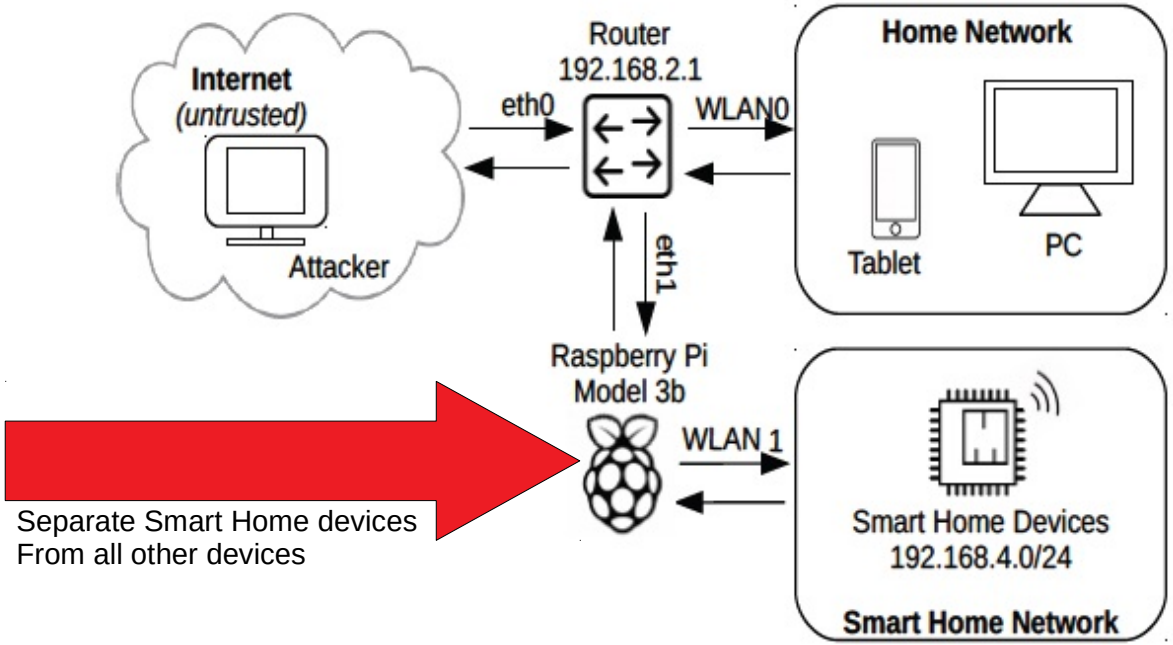

Figure 2: Experimental Smart Home Architecture

2. RESEARCH QUESTION ONE – RESULT (2/4)

- System Architecture

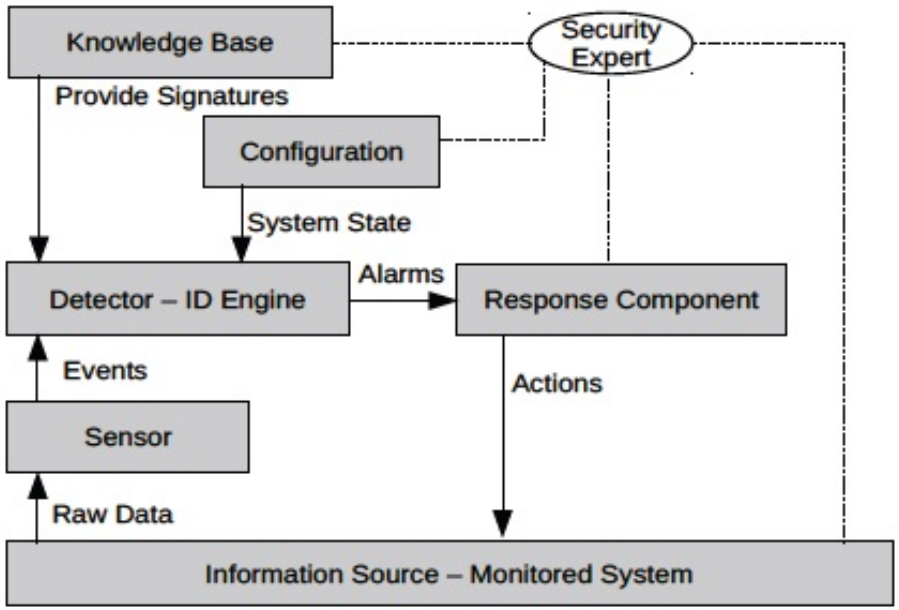

Figure 3: Existing IDS

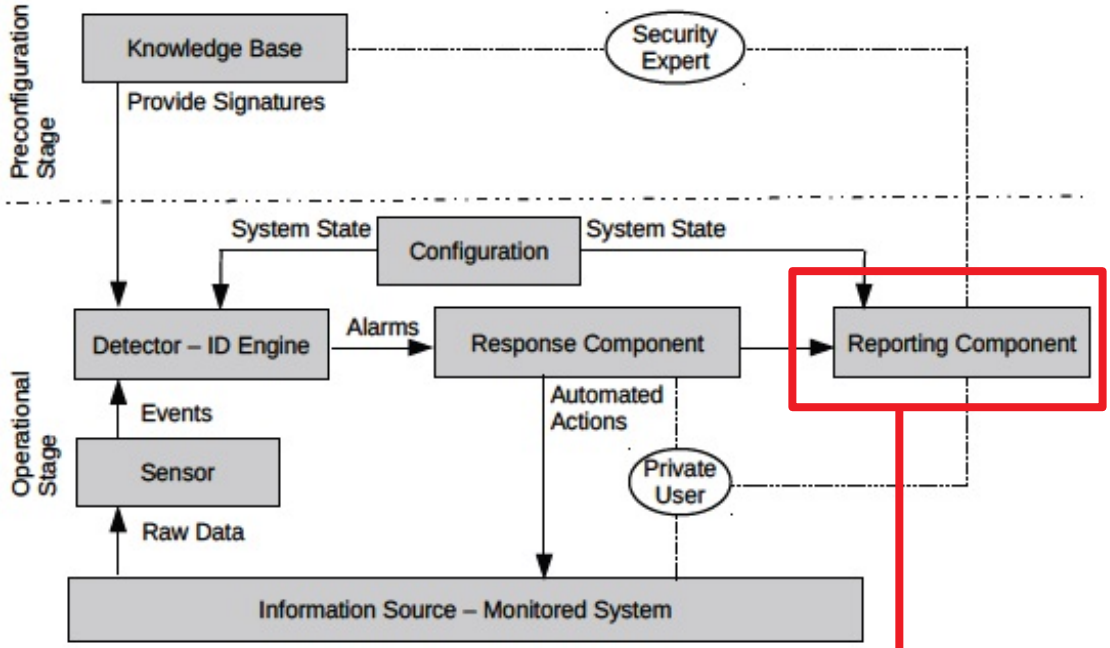

Figure 4: Smart Home IDS

We expanded the classic IDS to include a Reporting Component.
If there are no automated actions available the private user can use the Reporting Component to ask a security expert for help.

2. RESEARCH QUESTION ONE – RESULT (3/4)

- IT-Security Process

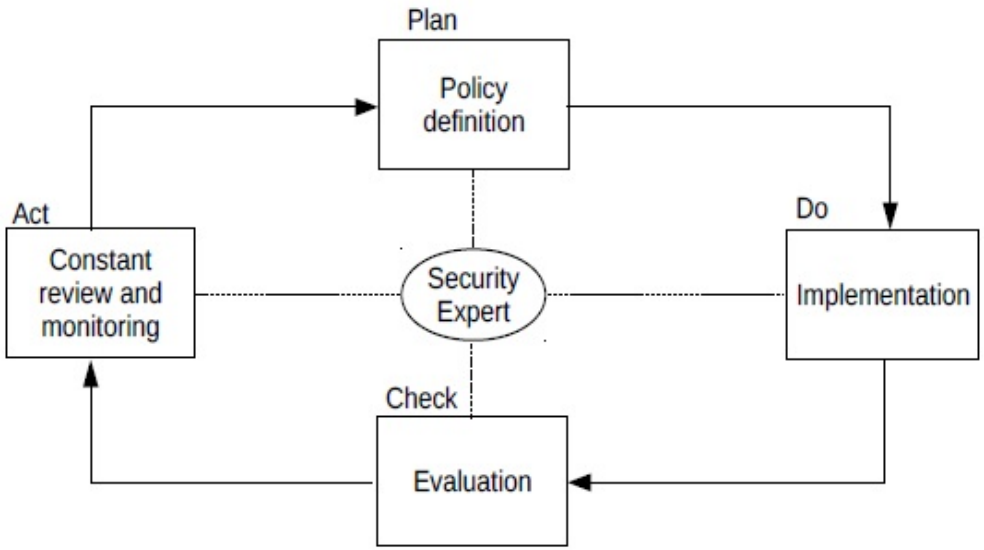

Figure 5: IT-Security Process

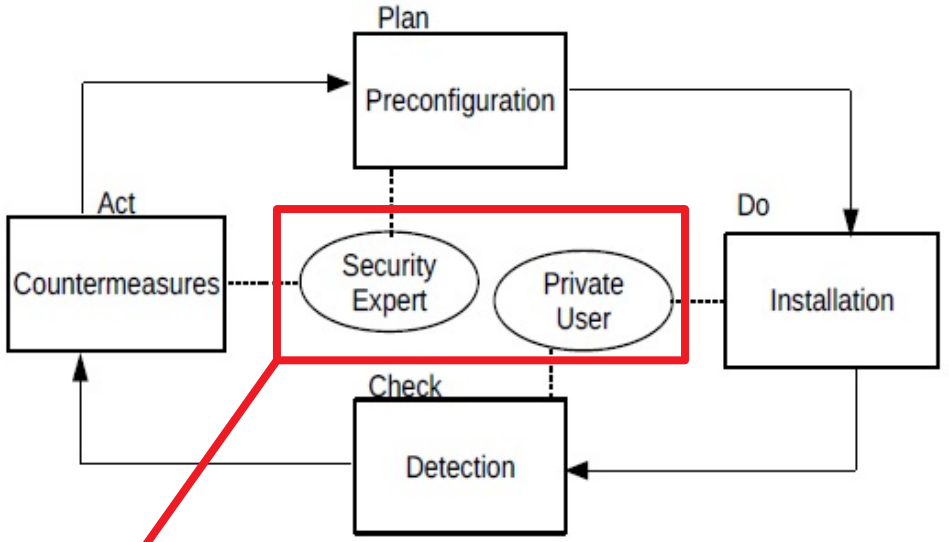

Figure 6: Adapted IT-Security Process

The private user has to install the IDS.
The IDS will inform the private user in case of an attack.
The security expert is responsible for pre-configuration of the IDS and initiating non-automatic countermeasures.

2. RESEARCH QUESTION ONE – RESULT (4/4)

- Contract Liabilities
  - Traditional IDS
    - The manufacturer is responsible for the code.
    - The private user is responsible for everything else.
  - Current IDS Approach
    - Separation: A Smart Home IDS must be able to define a distinct service. It includes all devices in the Smart Home network that are connected to the IDS.
    - Expertise: Specify the abilities of the IDS without referring to certain transmission protocols or attack names.
    - Understandability: It must be clearly communicated to the private user that an IDS does not offer a complete protection against any kinds of attack to the Smart Home.

3. RESEARCH QUESTION TWO – METHOD (1/2)

- With our experiments we will confirm that our IDS approach can be used to secure a Smart Home in practice.
- We will also find out if signature-based or anomaly-based IDS are better suited.
- We have conducted experiments with the system architecture illustrated in Figure 2.
  - The IDS is installed on a Raspberry Pi 3B that operates as a Wi-Fi Bridge between the Smart Home network (wlan1) and the Internet router (eth1).
  - The Raspberry Pi 3B is sufficient to evaluate network packets in real-time.

3. RESEARCH QUESTION TWO – METHOD (2/2)

- We have tested two different IDS:
  - Suricata:
    - realizes a signature-based detection
    - implements state-of-the-art detection algorithms
    - uses multi-core processors
    - starts with 27.000 preconfigured signatures and can be updated from a repository
  - Kitsune:
    - realizes an anomaly-detection
    - implements a number of neuronal networks
    - is installed with neuronal networks and a voting mechanism that are preconfigured

3. RESEARCH QUESTION TWO – EXPERIMENTAL PROCEDURE

- Stage one: We used all four Smart Home devices normally for 60 minutes and we recorded the produced traffic.

Device	Intervall	Duration	Interactions
Amazon Dash	10 minutes	1 sec.	6
Amazon Echo	10 minutes	5 minutes	6
IP-Camera	10 minutes	2 minutes	5
Temperature	10 seconds	-	60

- Stage two: We have used nmap to perform a portscan and we recorded the produced traffic.
- Stage three: We have performed a Telnet attack and we recorded the produced traffic.

3. RESEARCH QUESTION TWO – RESULT (1/3)

- Normal use:
  - During the first stage we have recorded 112.602 packets.
  - Suricata correctly identified all packets as benign.
  - Kitsune has misclassified 43 packets as malicious.

		Suricata		**Kitsune**	
		Malicious	Benign	Malicious	Benign
Reality	Malicious	0	0	0	0
	Benign	0	112.602	43	112.559

3. RESEARCH QUESTION TWO – RESULTS (2/3)

- Portscan:
  - Suricata has identified 48 packets as malicious and 131.089 others as benign.
  - Sucicata does not consider a Portscan as an attack. Thus, depending on the point of view, either 48 or 131,089 packets were misclassified.
  - Kitsune has classified 129.987 packets as malicious because sending packets to all ports differs from normal user behavior.

		Suricata		**Kitsune**	
		Malicious	Benign	Malicious	Benign
Reality	Malicious	48	131.089	129.987	1.150
	Benign	0	106.472	178	106.294

3. RESEARCH QUESTION TWO – RESULTS (3/3)

- Telnet Attack:
  - Suricata has correctly identified all benign and malicious packets.
  - Surprisingly, Kitsune was unable to identify malicious packets.
  - Kitsune has classified 2.848 benign packets as malicious. This is because Kitsune was confused by the user switching the radio station played by the Echo Dot.

		Suricata		**Kitsune**	
		Malicious	Benign	Malicious	Benign
Reality	Malicious	1.117	0	0	1.117
	Benign	0	113.384	2.848	110.536

4. CONCLUSION

- Typically, private users are no IT-Security experts.
  - They are not able to implement adequate security measures.
- We have developed a concept to implement an IDS into a Smart Home installation.
- We adapted the network segmentation, system architecture, IT-Security Process and the contractual liabilities of an IDS.
- We tested our concept with a series of experiments on four different Smart Home devices.
  - Considering our requirements, signature-detecting IDS are suitable to secure Smart Home installations.
  - Anomaly-detecting IDS are problematic because the anomaly detection algorithms tend to misclassify changing user behavior as an attack.

THANK YOU FOR YOUR ATTENTION