Instituto Superior Técnico - Universidade de Lisboa
Department of Computer Science and Engineering

Network and Computer Security
Alameda Campus
Group 38

HomeMgr

Secure Smart Home

Manuel Goulão
75254

Pedro Mela
78876

Leif Marius Reppen
89010

Fall 2017

1 Problem

In the present day, the rise in the use of Internet-of-Thighs (IoT) devices has skyrocketed. In fact, in 2011, the number of interconnected devices was larger than the number of people in the world, and by 2020, 24 billion devices are expected to exist [2].

From the typical computer to a large-scale smart city [5], a large array of interconnections may be found throughout most of the developed world. Indeed, smart houses pose a huge role in interconnectivity, with more and more devices being incorporated in this network, guiding, and simplifying the lives of many. Smart houses may have a large variety of purposes, from the simple simplification of some bothersome activities, to specifically designs directed at promoting energy efficiency [4], or aiding people with disabilities by providing assisted living [1].

Notwithstanding, smart houses require substantial concerns regarding security. In fact, the entire division of IoT should be considered with care when dealing with security, as described in [3], where Mirai and other botnets are described, making use of IoT devices to perform distributed denial-of-service (D-DOS) attacks. Moreover, personal privacy must be taken into consideration, as everyone is legitimately entitled to privacy, thus this right must be enforced by all means. Finally, personal safety is an obvious element when modelling a smart house, preventing hazardous effect which could happen if a malicious agent were to take control of the house, e.g. overheating leading to fires, if heating apparatus are connected; or turning off an alarm, if it ought to be connected.

In conclusion, a smart house could be a large help, simplifying and automating many tasks, and also providing essential aid to people, improving their quality of live. However, precautions regrading the security of the systems should be thoroughly studied, as IoT devices have been shown to be valuable targets for an attack.

2 Requirements

As stated in the previous section, the IoT world presents plenty of challenges regarding security implications. In fact, the following security requirements have been identified as being the most critical for a real-world smart house application:

- **Encrypted communications**. Encrypt the traffic coming from and going to the smart house devices in order to preserve users' privacy rights.
- **Home network segmentation**. Prevent attacks both from compromised smart house devices against devices on the network (e.g. computer), and from compromised machines against smart house devices.
- **Firewall incoming traffic**. Protection against intrusions by limiting the incoming traffic, as most IoT devices have limited hardware resources, thus restricting the use of resource-heavy security applications.
- **Firewall outgoing traffic**. Protection against compromised devices by limiting the outgoing traffic, preventing the execution of DOS attacks from a possible compromised component of the smart house.
- **Permission control and logging**. Limit access to devices depending on the user, in a "principle of least privilege" manner, and log events enhancing the chances to identify an attack.
- **Critical shutdown mechanism**. Intrusion detection, identifying the compromise of the smart house infrastructure, shutting-down the system to prevent catastrophic failure, and life threatening situations.

3 Proposed solution

First, for the **basic** system, there is the requirement to create an encrypted virtual network within the house's network, and enable a connection from, and to the smart devices. Then, this communications should only be allowed through a gateway. This would be implemented using a Raspberry Pi, with its ethernet interface connected to the home router, and connecting the smart devices to its wireless interface. All the traffic inside this new virtual network would be encrypted. Lastly, a management console would work as the interface to the user.

For the **intermediate**, more security enforcing mechanisms would be put in place. There, the gateway would have an active involvement in providing protection, implementing a firewall to limit inbound and outbound traffic volumes, preventing malicious activity from an external source, or the use of compromised devices to be used as part of an attack.

Finally, for the **advanced** system, more sophisticated measures would be implemented, as a user permission control method. Critical operations should only be possible from an administrator from inside the home network, logging the performed actions from each user. Furthermore, a critical shutdown would be triggered if the system were found to be compromised.

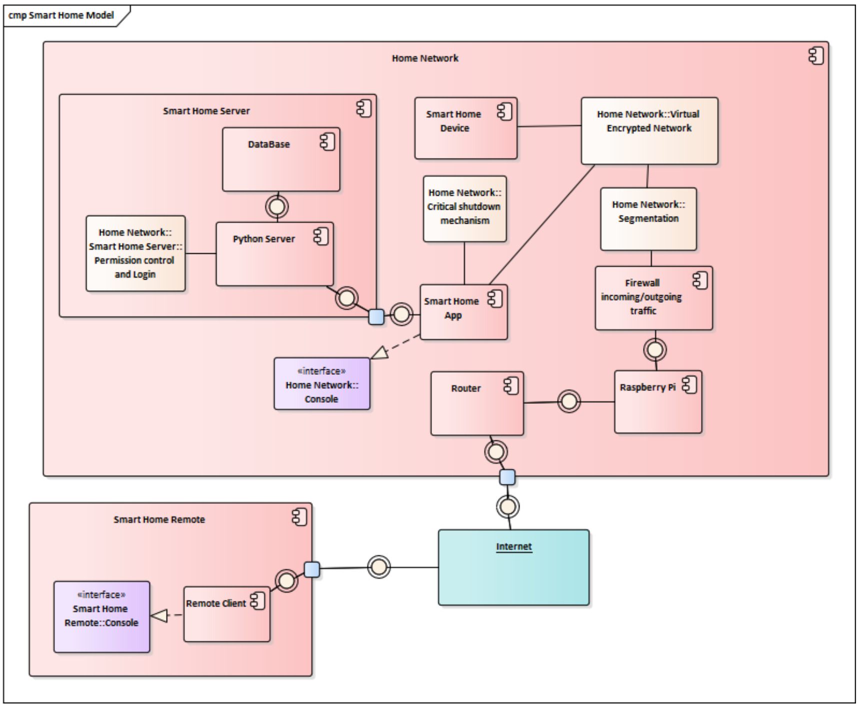
cmp Smart Home Model
Home Network
Smart Home Server
DataBase
Smart Home Device
Home Network::Virtual Encrypted Network
Home Network:: Critical shutdown mechanism
Home Network:: Segmentation
Home Network:: Smart Home Server:: Permission control and Login
Python Server
Smart Home App
Firewall incoming/outgoing traffic
«interface» Home Network:: Console
Router
Raspberry Pi
Smart Home Remote
Internet
«interface» Smart Home Remote::Console
Remote Client

Figure 1: UML Component diagram of the project.

4 Tool references

This section will describe the tools required for the successful execution of the proposed model, which was described using an UML Component diagram in Figure 1. Indeed, two different subsections will be presented. First, Subsection 4.1 will depict the tools used in order to organize and segment the collaboration among the team. Then, Subsection 4.2 will describe the technical tools needed for the actual implementation of the project, such as hardware, software and software libraries required.

It should be noted that, for this project, an emulation of the system will be preformed using virtual machines created for the purpose, taking into account the resources which would be present in the smart devices, e.g. a light-bulb would have very limited resources.

4.1 Project management tools

- Time manager: Trello
- Source code version management: Git and GitHub

4.2 Technical tools

Software and software libraries (all are yet to be installed and tested, except VirtualBox, which was tested in this course's labs):

• VirutalBox	`https://www.virtualbox.org/`
• Ubuntu Server Linux	`https://www.ubuntu.com/server`
• nginx	`https://nginx.org/en/`
• slite3	`https://www.sqlite.org/`
• Python	`https://www.python.org/`
• Python *socket*	`https://docs.python.org/2/library/socket.html`
• Python *ssl*	`https://docs.python.org/2/library/ssl.html`
• Pyhton *pycrypto*	`https://pypi.python.org/pypi/pycrypto`
• Python *sqlite3*	`https://docs.python.org/2/library/sqlite3.html`

5 Work plan

Table 1: Work plan for each week of project work.

Week	**Manuel**	**Pedro**	**Leif Marius**
1. Oct 30 - Nov 5 2017	Create virtual network	Implement end to end encryption	Create the server
2. Nov 6 - 12 2017	Socket programming	Implement end to end encryption	
Complete Basic Nov 10	Encrypted communications, Home network segmentation, Testing		
3. Nov 13 - 19 2017	Create the simulator for IoT Device	Create user interface	Test the IoT devices
4. Nov 20 - 26 2017	Create the simulator for IoT Device	Configure firewall	Test the firewall
Complete Intermediate Nov 24.	Firewall incoming and outgoing traffic , Testing		
5. Nov 27 - Dec 3 2017		Create simulator for IoT device	Permission control
6. Dec 4 - 10 2017	Critical shutdown Mechanism		Critical shutdown Mechanism
Complete Advanced Dec 8	Critical shutdown Mechanism, Permission control and user management		

References

[1] M. C. Domingo. An overview of the internet of things for people with disabilities. *Journal of Network and Computer Applications*, 35(2):584–596, 2012.

[2] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami. Internet of things (iot): A vision, architectural elements, and future directions. *Future generation computer systems*, 29(7):1645–1660, 2013.

[3] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas. Ddos in the iot: Mirai and other botnets. *Computer*, 50(7):80–84, 2017.

[4] D. Shahgoshtasbi and M. Jamshidi. Energy efficiency in a smart house with an intelligent neuro-fuzzy lookup table. In *System of Systems Engineering (SoSE), 2011 6th International Conference on*, pages 288–292. IEEE, 2011.

[5] A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi. Internet of things for smart cities. *IEEE Internet of Things journal*, 1(1):22–32, 2014.