FACULTY OF INFORMATION TECHNOLOGY CTU IN PRAGUE

Review report of a final thesis

Student:	Peter Páleník
Reviewer:	Ing. Alexandru Moucha, Ph.D.
Thesis title:	Chytrý strážce domácí sítě
Branch of the study:	Computer Security and Information technology

Date: 27. 5. 2018

Evaluation criterion:	*The evaluation scale: 1 to 4.*
1. Fulfilment of the assignment	*1 = assignment fulfilled,* ***2 = assignment fulfilled with minor objections,*** *3 = assignment fulfilled with major objections,* *4 = assignment not fulfilled*

Criteria description:
Assess whether the submitted FT defines the objectives sufficiently and in line with the assignment; whether the objectives are formulated correctly and fulfilled sufficiently. In the comment, specify the points of the assignment that have not been met, assess the severity, impact, and, if appropriate, also the cause of the deficiencies. If the assignment differs substantially from the standards for the FT or if the student has developed the FT beyond the assignment, describe the way it got reflected on the quality of the assignment's fulfilment and the way it affected your final evaluation.

Comments:
The work was fulfilled according to the requirements except the last one: the device should be easy to use, secured and cheap. Such a system is impossible to build and it was proven countless of times. The designed system in the thesis is not secured, as a couple of simple attacks will either pass unobserved or will degenerate into more complicated ones fairly simply.

Evaluation criterion:	*The evaluation scale: 0 to 100 points (grade A to F).*
2. Main written part	*100 (A)*

Criteria description:
Evaluate whether the extent of the FT is adequate to its content and scope: are all the parts of the FT contentful and necessary? Next, consider whether the submitted FT is actually correct – are there factual errors or inaccuracies? Evaluate the logical structure of the FT, the thematic flow between chapters and whether the text is comprehensible to the reader. Assess whether the formal notations in the FT are used correctly. Assess the typographic and language aspects of the FT, follow the Dean's Directive No. 26/2017, Art. 3. Evaluate whether the relevant sources are properly used, quoted and cited. Verify that all quotes are properly distinguished from the results achieved in the FT, thus, that the citation ethics has not been violated and that the citations are complete and in accordance with citation practices and standards. Finally, evaluate whether the software and other copyrighted works have been used in accordance with their license terms.

Comments:
Excellent written work, easy to read and understand.

Evaluation criterion:	*The evaluation scale: 0 to 100 points (grade A to F).*
3. Non-written part, attachments	*100 (A)*

Criteria description:
Depending on the nature of the FT, comment on the non-written part of the thesis. For example: SW work – the overall quality of the program. Is the technology used (from the development to deployment) suitable and adequate? HW – functional sample. Evaluate the technology and tools used. Research and experimental work – repeatability of the experiment.

Comments:
Excellent wrok with the hardware and software.

Evaluation criterion:	*The evaluation scale: 0 to 100 points (grade A to F).*
4. Evaluation of results, publication outputs and awards	*50 (E)*

Criteria description:
Depending on the nature of the thesis, estimate whether the thesis results could be deployed in practice; alternatively, evaluate whether the results of the FT extend the already published/known results or whether they bring in completely new findings.

Comments:
The results for the student are very interesting but cannot be used to anything else rather than a student project. Please see my comments.

Evaluation criterion:	*No evaluation scale.*
5. Questions for the defence	

Criteria description:
Formulate questions that the student should answer during the Presentation and defence of the FT in front of the SFE Committee (use a bullet list).

Questions:

Not a question: in the commercial solutions explained in 2.2.1.1 it is interesting to see in which countries those solutions were developed. I was also surprised not to find BitDefender Box (Romanian product) or Turris (Czech product).

How much time did you spend on developing this system?

Evaluation criterion:	*The evaluation scale: 0 to 100 points (grade A to F).*
6. The overall evaluation	*79 (C)*

Criteria description:
Summarize which of the aspects of the FT affected your grading process the most. The overall grade does not need to be an arithmetic mean (or other value) calculated from the evaluation in the previous criteria. Generally, a well-fulfilled assignment is assessed by grade A.

Comments:
A SOHO (Small Office Home Office) is a core-collapsed network in which, most probably, the switch and the router are one single piece of hardware. Thus, as it is clearly mentioned in Fig. 31., the SOHO network is formed by an ISP (Internet provider)and a box which provides: switching, routing, wireless and services. To this box all the other end-devices are connected either by cable or by wireless. A SOHO network can be compromised thus by either compromising this “box” or an end-device (which may be a computer, IoT device or anything else).

In the case the “box” is compromised, most of the detection functions of the proposed solution will fail, it means that they will be unable to detect anything suspect. Here are some examples:

DNS request to iphone.moucha.org should give 89.24.79.13 but a malware on the box gives the address 11.11.11.11 instead. Thus a genuine computer sends a DNS request to the box (or any other external DNS) and the box replies with an address - exactly as expected, but the address is false. The only solution is to make the Smart Home Network Guard (SHNG) the DNS server and to always use DNSSEC. The only problem is: what DNSSEC provider are you going to use and in case you need to update it to the sold SHNGs to the customers, how are you going to update the DNSSEC provider in case of a change? Send them an email for them in their Android app to change it manually?!?!? But such an email can be written by anyone!

ARP snooping is implemented in switches which keep an internal memory containing the following data: on which port there is a trusted DHCP server and the MAC and IP addresses associated in the DORA DHCP process. DNCP snooping detects DHCP replies on non-trusted ports triggering an alarm while ARP snooping detects wrong MAC-IP associations in the ARP reply messages (when compared to the genuine MAC-IP association given by the trusted DHCP server). In all cases the suspicious port is error-disabled.

If the box in the network is compromised, then all this above activity will pass unobserved as it follows the normal procedure. The problem is is there is yet another DHCP server or a compromised ARP related device in the network. If it is on one of the physical box of the box, you will be able to detect it immediately as the attacker had to enter the house, plug in a rogue computer, pull a cable to your box and exit the house, all without notice. If the device is on the wireless side of the network, it becomes interesting as you need to de-auth the device, as properly stated in the thesis. The problem is: that device can assume (by listening your other genuine devices) different MACs and IPs and what your SHNG will do is to essentially disconnect all your devices.

What is really interesting is that this SHNG has some signature detections (IDS). The problem in this case is how to inform the user (as you specified that the user is an untrained, normal, plain home user) - if you send him this:

04/10/2018-12:13:31.936426 [**] [1:2018919:3] ET POLICY
possible Xiaomi phone data leakage HTTP [**] [Classification:
Potential Corporate Privacy Violation] [Priority: 1] TCP
10.9.8.109:54050 -> 52.76.188.200:80

he will understand exactly what my wife and my mother understood: nothing. Their immediate question was: “ok, what should I do now”?

If you imagined this project as having a cheap box and a central management system which will push for updates of firmware, signatures, etc, then this is done and patented. Cisco has FibrePower, NIC.CZ has Turris, Bitdefender has BitDefender Box. The problem even in these cases is that each SHNG will cost 2-300 Euro and you also need an infrastructure to maintain these updates.

Regarding the price of 1470 Kc on page 41, this price does not take into account the work and the infrastructure needed for maintaining these SHNGs. To have these, the price of a box will be as mentioned above which will create no concurrence for existing security systems from well-established companies, with budgets maybe millions of times your budget.

As a conclusion: it was told you that there is a thing preventing us to have cheap, secured and easy to use devices and you cannot reach optimality on all these three aspects simultaneously.

Thus, your work was for you an excellent way to learn a lot of new and interesting things, from the formal perspective I would give an A; from the perspective that you were warned about the limitations of such systems I would give an E for the proposed solution. On average I quantise your entire work as GOOD - mark C.

Signature of the reviewer: