Introducing Mobile Network Security Experiments to Communication Technology Education

Stig F. Mjølsnes and Ruxandra F. Olimid(✉)

Department of Information Security and Communication Technology, NTNU, Norwegian University of Science and Technology, Trondheim, Norway
{sfm,ruxandra.olimid}@ntnu.no

Abstract. We describe a new viable lab assignment that enhances the theoretical study of wireless network security in our master-level communication technology education with hands-on mobile access network experimentation for the students. This new part is added to a well established student lab on wireless network security, by making use of low cost software defined radio devices and readily available open source software for experiments with one-cell GSM mobile access networks. The students can use their own smartphones. The overall objective of the lab is to support the students' practical understanding of the technical problems of building and managing wireless network security mechanisms. We report our findings and experiences from designing, constructing, testing and managing this lab assignment in the autumn semester of 2016.

Keywords: Education · Communication technology · Wireless · Mobile networks · Information security · GSM · Software defined radio

1 Introduction

1.1 Motivation

Cellular mobile access networks (GSM, UMTS, and LTE) have become a ubiquitous part of the world-wide communication systems and are used in both personal and professional everyday life now. Access authorization and authentication, confidentiality, integrity, and location and tracking privacy are some of the highly important communication security properties. The topic of mobile network security has been included in university level curricula at some engineering and computer science programs. Typically, however, the teaching is theory-only with no provision for lab work with real wireless setups.

We propose that gaining experience by a process of doing hands-on experimentation will significantly improve the intuition and understanding of mobile network security concepts and theory, and ought to be an essential component

M. Bishop et al. (Eds.): WISE 10, IFIP AICT 503, pp. 74–83, 2017.
DOI: 10.1007/978-3-319-58553-6_7

of teaching network security. It should make students skilled in both practical attacks, and the best practice of security mechanisms and protocols. As a consequence, a natural question arises: *"How to introduce mobile network security experiments to network engineering education?"*. We describe our recent work of designing, constructing, testing and managing a lab assignment for mobile network security included in a master level course in wireless network security.

1.2 Our Contribution

For many years, the student assignment associated with our Wireless Network Security course within the Master's Programme in Communication Technology has helped students explore the security mechanisms and protocols used in wireless LANs. Useful open source software and inexpensive equipment for this communication technology have been easy to acquire and set up. During the autumn semester of 2016, we have successfully extended this lab assignment with realistic mobile network security experiments based on software-defined radio devices controlled by readily available open source software. The students are able to explore mobile network security protocols by building a one-cell mobile access network and run tests with their own smartphones. For a start, the students can analyze live radio communication protocols, authentication, encryption, and anonymity mechanisms for the GSM mobile system. Equipment and devices useful for setting up such experimental mobile wireless networks are now available at affordable cost, and this creates exciting new possibilities for communication security engineering education. Let this new part of the lab assignment be referred to as the *Mobile Access Network Security section*. This paper describes both the technical details of the lab equipment and tools, and the pedagogical experiences that we have gained so far. Finally, we indicate possible directions for further developments that we plan to take.

2 The Course

The Wireless Network Course is part of the first year master's program in Communication Technology. It builds upon our basic Cryptography, Computers, and Network Security course. Other recommended prerequisites are courses in Access and Transport Networks, Mobile Networks and Services. In general, the scope of the course is functions, protocols, and configurations for realizing authentication, key distribution, integrity, confidentiality and anonymity in wireless access networks for mobile users. Mobile forensics has been included too. The course presents and analyses security techniques employed in existing systems, including WPAN, WLAN, GSM/UMTS/LTE, IMS. In addition, we may present proposed solutions for new wireless technologies, such as ad-hoc and sensor networks. One of the main learning objectives is to acquire analytical skills for information security assessment of communication systems that provide services for mobile users by wireless access networks.

The lab assignment is 20% of the total course. The content of the assignment has steadily evolved since the start in 2006. The original inspiration for

creating the course and the lab assignment did not come from similar teaching at other universities. It is our perception that there have been, and still are, few courses on wireless *security* in university level curricula. A major part of our early inspiration came from open source network tools and WiFi hacker tools that were developed and emerged at that time, such as `wireshark`, `kismet`, and the `aircrack-ng` suite of tools [1–3]. Note that the first cryptanalytic results on WEP were published a few years earlier, in 2001. Note also that around that time the term *ethical hacking* became a professional security testing skill sought after by big corporations and governments, which spawned a heated discussion at universities whether computer engineering students ought to be taught attacker/hacker skills. Retrospectively, we are now able to find that Hartpence paper from 2005 describes some of the same considerations that we started out with [4].

This same sort of practical impetus that we had for creating the lab in the first place also holds for our newly added *Mobile Access Network Security* part. Our inspiration here is the availability and low cost of USRP devices, together with open source software [5–8]. After having constructed and conducted this new part, we found out that similar labs exist at some very few other universities, suggesting that the approach starts to gain momentum [9].

3 The Lab Organisation

3.1 Structure

A total of 40 students enrolled in the course for the autumn semester of 2016, whereof 31 males and 9 females. The course attracts a significant number of international exchange students (9 students in 2016). Over the years, the total number of students have fluctuated around 50 students.

Table 1. Student grouping

No. of students per group	No. of groups
3	11
2	3
1	1

For 2016: 40 students divided into 15 groups

We measure that the entire assignment will nominally require at most one full week effort for a group of three students sharing the work load. We advice cooperation on problems both within the group and across groups, and commend self-organised designation of roles and responsibilities within each group. We allow flexibility in establishing the groups (student driven), and Table 1 shows the numbers for the groups last year (2016).

We allocate two calendar weeks due to limitation in lab space and for various other reasons, such as computer resources, noise level, course staff availability. This allows some flexibility for the students or groups to pick a preferred week, thus eliminating absence problems that might be caused by personal circumstances or conflicts with other courses and activities. The groups are granted access to the laboratory room for the week they are registered for.

One week before the lab work, the course staff will give an introductory talk on the lab objectives, description, deliverables and grading criteria. The complete lab assignment description becomes available well in advance for the students to understand the theoretical background needed and to organize their work.

The lab assignment is a mandatory 20% portfolio of the course, and consists of two main tasks over two weeks' time:

(1) Carry out the lab experiments, and demonstrate the results after each milestone to a teaching assistant. All milestones must be passed and approved by a teaching assistant by the end of the first week (pass or fail).
(2) Prepare and submit a written lab report for grading and the end of the following week. We encourage the students to record their progress in a lab journal. The submitted lab report is graded by the course staff.

3.2 Content

The work plan for the mobile network security part contains four main tasks:

1. Set up a one-cell GSM network.
2. Enable 'Open Registration'.
3. Enable 'Cached Authentication'.
4. Enable link encryption.

First task aims to become familiar with the hardware and software tools that will be used later in the lab. The main objective is to set up the hardware and the software for the GSM one-cell network, for which they will configure and test security mechanisms.

The next three tasks challenge the students to experiment with the GSM authentication and access control, (un)linkability, and confidentiality mechanisms. The 2G mobile access networks should issue random strings for TMSI (Temporary Mobile Subscriber Identity), replacing the permanent identity string of IMSI (International Mobile Subscriber Identity). So, students first enable TMSI allocation for their network service, having in mind a purpose for this: to secure their network against passive adversaries (eavesdroppers) that want to break the privacy of a targeted subscriber (identified by a given IMSI).

The access control and authentication protocols of mobile networks are central topics in the course. Hence we ask the students to perform some experiments with two (quite naive) access control mechanisms implemented in OpenBTS: *Open Registration* and *Cached Authentication*. This offers the students a practical environment to reflect on different access control mechanisms. They will

analyze the security performance of the mechanisms used, and compare against the real mechanisms in GSM networks. Finally, we ask to enable encryption, keeping in mind the goal of private communication.

Each of the four main tasks corresponds to one milestone. By this, we expect the students to demonstrate the operation, the functionality and their comprehension. We find these milestones to be a good method for the teaching assistants to monitor the progress of each group.

4 Instrumentation

A student group will normally use the following equipment:

- One networked computer.[1]
- One USRP (Ettus B200mini) as in Fig. 2.
- Two smartphones enabled for 2G access (optional).

Universal Software Radio Peripheral (USRP). A USRP is a device used to prototype wireless communication systems. The B200mini is a USRP with size less than a payment card that can be programmed to operate over a wide radio-frequency range (70 MHz - 6GHz) and communicate in full duplex. For instance, it can be used in all of the standard GSM, UMTS, and LTE frequency bands. Figure 1 shows the USRP B200mini board, while Fig. 2 shows the hardware enclosed and with antennas mounted [10], as presented to our students in the lab. More detailed technical specifications on the B200mini can be found at Ref. [11].

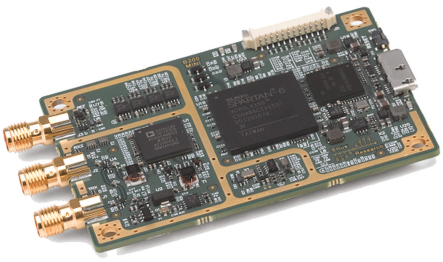

Fig. 1. The Ettus Research B200mini USRP board, size 83.3×50.8 mm [11].

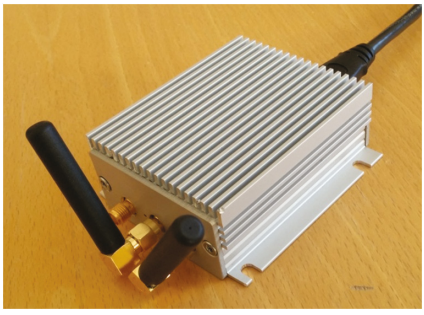

Fig. 2. We built our own robust enclosure for the USRP boards and antennas.

[1] In fact, each group will use two desktop computers equipped with 802.11 network interface cards required for parts of the lab assignment not reported on here.

OpenBTS. OpenBTS is a Linux-based open source software that can interface to software-defined radio hardware [5]. The OpenBTS implements most of the GSM stack above the radio modem; however, it requires some other distinct applications as prerequisites:

SMQueue (SIP Message Queue) stores and forwards text messages, being a prerequisite for the SMS service between mobile stations using OpenBTS.

Asterisk is a Voice over IP (VoIP) switch that performs call establishment between mobile stations using OpenBTS. Asterisk is an open source framework sponsored by Digium [12].

SIPAuthServe (SIP Authorisation Server) is an application that manages the subscriber database, thus replacing the HLR (Home Location Register) entity found in a conventional GSM network architecture.

The OpenBTS suite and all the prerequisites were installed and configured by the course staff to work with the USRP B200mini before the lab started. More detailed information on OpenBTS is available at Ref. [13,14].

Computers. The computers used in the lab are desktop computers with Intel Core2 Quad CPU Q9400@2.66 GHz running Ubuntu 12.04. The recommendation is to connect the USRP device via a USB3, but we found out that the USB2 transfer speed is sufficient for our lab activities.

Smartphones. Following the BOYD (Bring Your Own Device) policy, we encouraged the students to switch their own mobile phones to 2G and use them for the experiments. Nevertheless, we provided LG Nexus 5X handsets running Android v6 to a few groups that lacked access to the necessary two mobile phone devices. (This was the case for the "one-student group", as well as for some students whose phones disallowed network type selection - e.g.: older versions of iOS).

5 The Lab Tasks

This is a brief description of the tasks in the mobile access network part of the lab. The tasks focus on the security aspects in GSM, as previously explained in Sect. 3.

The course staff have downloaded and built all the necessary software on all desktop computers prior to the lab start. This assures an effective start for the students and avoids much hassle and frustration that can occur with incompatibility of the operating system, drivers, and building the applications. However, the complete installation guidance is given too, say, for or students who want to reproduce the experiments on their personal computers.

The first task is to connect the USRP device to a computer and check if the device is properly connected, by inspecting the LEDs and running specific commands. Each group creates a one-cell mobile network by starting and running the OpenBTS processes. Running several base stations concurrently in the same lab hall must be done with care to avoid radio frequency interferences. There are at least two concerns:

1. Interference with the commercial networks (that use licensed GSM frequency bands) outside the lab hall.
2. Interference among the lab group networks inside the lab hall.

We have put in place the following strategy to avoid these problems: each group is assigned a distinct ARFCN (Absolute Radio Frequency Channel Number) - chosen such that there are no interferences with cells of the other groups—from a frequency band that is not allocated for commercial mobile communication. This avoids interference with the commercial mobile networks [15]. Additionally, the students are asked to configure the USRP devices to a very low transmission power such that the cell radio coverage is effectively restricted to the lab hall.

Further, the lab tasks include the capture, storage, and analysis of network traffic, identify specific messages and parameters in several scenarios, and find and explain particular handset behaviour corresponding to distinct configurations of the network.

As an example, we outline here the procedure for the task *Enable link encryption*. The main objective for this is to investigate the confidentiality mechanisms in GSM. The students have to inspect encryption related parameters in the OpenBTS command line interface and enable encryption by setting appropriate values. Students can make calls from one handset to another, capture the traffic, and observe the differences between the situation where encryption is disabled, respectively enabled. Students are asked to compare the encryption behaviour they observe in the lab with the GSM encryption standard, and to give a description of the technical differences.

A similar method is applied for the others tasks:

- Enable TMSI allocation and observe which changes occur in the message flow. Check if the security goal is fulfilled.
- Experiment with the two access control mechanisms implemented in OpenBTS: *Open Registration* and *Cached Authentication*. Note the differences between the two and compare them with the textbook description of GSM authentication.

We aim for communication observations and analyses to be conducted both on the network side and on the user equipment side. The students are asked to observe how the mobile devices operate in different scenarios and to evaluate the security functionality on both sides. For example, we ask questions related to user experience and privacy, such as:

> *"Which security modes of operation are signalled by the phone's display to the user? In particular, consider various types of registration, authentication, and encryption modes".*

6 Experience and Students' Feedback

The Mobile Access Network Security assignment part has been well received by the students so far. We suggest possible improvements in the final section of

the paper. We have used two methods for collecting feedback: a question to be answered in the lab report, and direct interviews and report from the student reference group for the course.

Specific Question in the Lab Report. We use one assignment question to probe the students' opinions about the lab, and suggestions for possible improvements.

> *"How can this lab project be improved? (Answering is optional and does not influence your grade.)".*

The question was optional, so not all groups answered. However, we got feedback from several groups, and overall it was positive indeed. Two of the responses are:

> *"We think that the practical part was very interesting, not too difficult nor too easy, and it is possible to finish within one week."*
> *"The motivation behind the lab project was clear, visible, and comprehensible. The tasks to be performed were interesting and informative. The well-prepared equipment enabled us to work directly 'hands-on' without long installation tasks. ... All in all, the lab was a great success."*

Reference Group Report. At our university, it is required that three or four students volunteer to become a reference group for the class and course. They shall represent all students in the class, and provide a formal communication channel between the class and the course staff. They write up a short report at the end of the course, which is used as input to the overall evaluation of the course. Their reported feedback for the lab reads very encouraging:

> *"Lab: Very good, interesting and relevant topics. Hard to find information about different modification that you had to do. The description was very helpful, and the lab was well prepared, including the new part.".*

Finally, we present here some of our findings and experiences from the construction, testing and management of the laboratory.

During the development work of the lab, we tested several USRP devices, mostly from Ettus Research [16]. The final decision on the B200mini was due to several factors: compliance to our needs, affordable price, and small enough to be easily stored and transported in one box. Also, we have tested and found that the B200mini are compatible with our not-so-new desktop computers already in use for the lab. As mentioned earlier, we found that we did not need to upgrade to USB3 ports, so the only additional equipment that had to be bought were the antennas [10] and making the encapsulation for the board. Currently, the USRPs are used in other wireless communication courses and in our master thesis research projects, so they have proved to be a good investment.

We encountered some problems with the software during our lab construction. OpenBTS is an open source platform, always under development, so we sometimes had problems with the up-to-date version of the software, which cracked. We solved this by using a functional version of the source code, but changed the

drivers to the ones compatible to the B200mini. This and the amount of time required for build the executables (approx. 30 min) made us decide to pre-install all the necessary software on the lab computers, thus allowing the students to focus their activities on the security related issues.

Students encountered a problem with identifying their own access network when more cells were up in the lab hall at the same time. This happens because some handsets always display the network as Test PLMN 1-1 (for default Mobile Country Code and Mobile Network Code), independent of the actual name assigned to the network by the software configuration. To avoid this, we asked the students to set the Mobile Network Code to their group number, which makes each cell directly identifiable.

7 Conclusions and Further Developments

We have succeeded in enhancing the theoretical study of wireless network security in our master-level communication technology education with hands-on mobile access network experimentation. We consider this as our first and exciting step into the learning possibilities that the brave new environment of open source based mobile networks can bring.

We decided to start with the GSM mobile networks, and next we want to move on directly to 4G (LTE). There are open source projects for LTE emerging, which makes this plan feasible [6–8]. At the same time, we want to develop further the GSM part of the lab, by making use of configurable SIM cards and allow the complete GSM authentication mechanism and encryption to take place. For this, we already acquired and tested configurable SIM cards [17], which we can configure for our purposes by using the PySim software [18] and a card reader [19]. These ideas were independently suggested by some of our students in their lab report feedback:

> *"It would be a nice feature if we had the possibility to use programmable SIM-cards in order to play with GSM.Cipher. Encryption enabled or disabled and see the difference in the captured traffic in Wireshark."*
> *"Could it be an idea to set up LTE instead of GSM? Obviously LTE have less security vulnerabilities and is probably more time consuming to set up, however the relevance is greater."*

Acknowledgements. Many people have contributed to the development and improvement of this wireless security lab assignment and its form and content. Professor Stig F. Mjølsnes started out in the spring of 2006 and set up the framework and the basic content, structure and text. Master student Lars Haukli joined in during the summer of 2006 and made tremendously good progress by testing out and identifying the best WiFi NICs and drivers for this purpose. He collected, tested, and selected a working environment of software tools for the Linux platform, and contributed enthusiastically to the technical content of this lab description. The first course students of TTM4137 carried out the assignment with success in the fall of 2006. Everything went smoothly, much thanks to dedicated supervision by teaching assistant PhD-student

Marie Moe and lab assistant master student Jan Tore Sørensen. Marie continued as teaching assistant in 2007 and made sure that the experience gained was put to good use in supervision and by editing a new version of the assignment text. The challenge of password dictionary attack was worked out by the teaching assistants and PhD-student Martin Eian and PhD-student Anton Stolbunov in 2008. During the summer 2016, professor Stig F. Mjølsnes, post doc Ruxandra F. Olimid, and engineer Pål Sturla Sæther developed, and built the USRP-based student lab. Ruxandra F. Olimid and student assistant Fredrik Skretteberg tested and managed the first student run-through of the lab assignment in the autumn semester 2016.

References

1. Wireshark Foundation: Wireshark. http://www.wireshark.org/
2. Kismet. http://www.kismetwireless.net/
3. Aircrack-ng: Aircrack-ng suite. http://www.aircrack-ng.org/doku.php#documentation
4. Hartpence, B.: Teaching wireless security for results. In: Proceedings of the 6th Conference on Information Technology Education (SIGITE 2005), pp. 89–93. ACM, New York (2005)
5. Range Networks: OpenBTS. http://openbts.org
6. OpenLTE: An open source 3GPP LTE implementation. https://sourceforge.net/projects/openlte/
7. srsLTE: Open source 3GPP LTE library. https://github.com/srsLTE/srsLTE
8. Open Air Interface: 5G software alliance for democratising wireless innovation. http://www.openairinterface.org
9. Iowa State University: Wireless Security Lab & OpenBTS. http://seniord.ece.iastate.edu/dec1314/documents/Dec13-14_FinalPaper_12_09_13.pdfl
10. Pulse Electronics: W1900 antenna. http://www.pulseelectronics.com/products/old_antennas/products__solutions/antennas_for_wireless_devices/wd_antennas/w1900_/_w1902_penta_band_right_angle_stubby_antenna
11. Ettus Research: USRP B200mini. https://www.ettus.com/product/details/USRP-B200mini
12. Digium: Asterisk. http://www.asterisk.org
13. Iedema, M.: Getting Started with OpenBTS. O'Reilly Media Inc., Sebastopol (2014)
14. Range Networks: OpenBTS application suite - user manual (2014). http://openbts.org/site/wp-content/uploads/2014/07/OpenBTS-4.0-Manual.pdf
15. European Communication Office: ECO Frequency Information System. http://www.efis.dk
16. Ettus Research: A national instruments company. https://www.ettus.com/
17. Sysmocom: SIM+USIM Card. http://shop.sysmocom.de/products/sysmousim-sjs1-4ff
18. Pysim: A python tool to program SIMs. https://github.com/osmocom/pysim
19. Sysmocom: USB CCID reader. http://shop.sysmocom.de/products/scr3310