Contactless Smart Card Experiments in a Cybersecurity Course

Xiaojun Wu, Yongqiang Chen, Shanshan Li

Department of Computer Science and Technology

Tsinghua University

Beijing, China

[xjwu, chenyongqiang, lishanshan]@tsinghua.edu.cn

***Abstract*—This Innovate Practice Work in Progress paper is about education on Cybersecurity, which is essential in training of innovative talents in the era of the Internet. Besides knowledge and skills, it is important as well to enhance the students' awareness of cybersecurity in daily life. Considering that contactless smart cards are common and widely used in various areas, one basic and two advanced contactless smart card experiments were designed innovatively and assigned to junior students in 3-people groups in an introductory cybersecurity summer course. The experimental principles, facilities, contents and arrangement are introduced successively. Classroom tests were managed before and after the experiments, and a box and whisker plot is used to describe the distributions of the scores in both tests. The experimental output and student feedback implied the learning objectives were achieved through the problem-based, active and group learning experience during the experiments.**

Keywords—cybersecurity; smart cards; experimental teaching

I. INTRODUCTION

We are in an era of rapid development of information technology in the Internet. Unconsciously, our daily life, learning, and working have been integrated into the Internet in all directions. Cybersecurity is no longer a strange name to ordinary people, since media reports on cybersecurity incidents appear from time to time. The US government has recognized the importance of cybersecurity education and promote cybersecurity programs such as the National Initiative for Cybersecurity Education (NICE) and the Centers of Academic Excellence [1, 2]. In the report of a workshop organized by ACM's Education Board, advice was proposed on cybersecurity education for all undergraduates and computing majors in universities [3, 4].

Knowledge in various computing courses and practical activities are both essential for the students to learn cybersecurity well. Earlier practical activities for cybersecurity training often involved configuring network equipment (such as network interface cards, switches and routers) and software tools (such as system accounts, firewalls and databases) [5]. In recently years, exercises in the style as Capture the Flag (CTF) competitions were found to be very effective for cybersecurity education [6, 7].

We also developed a platform to manage the exercises in a jeopardy-style competition in an introductory cybersecurity course and got positive feedback from the students [8]. Moreover, some students suggested we arrange hands-on experiments on cybersecurity involving real hardware. This would avoid the unrealistic feeling of online exercises, so that the students could understand better how their learnings were applied. Moreover, if some common items could be used in the experiments, it would be helpful to enhance the students' awareness of cybersecurity in daily life, which was as important as knowledge and skills. The contactless smart card experiments were then designed innovatively and used in the last year's course.

Smart cards are small to carry, easy to use and relatively secured with encrypted storage and calculation, so they can be used as bank cards [9]. In fact, various types of contactless smart cards have been widely used in our life, such as Resident Identity Cards, Public Transport Cards, and access control cards. On the other hand, security in smart card applications has been concerned and studied for a long time [10, 11]. How safe are the contactless smart cards in our daily life? What should we pay attention to when using these cards? We designed three contactless smart card experiments, one basic and two advanced, trying to help the students to find their answers. The basic experiment required the students to make a simple reader, read the information in a variety of contactless smart cards, and compare their security levels. One advanced experiment required the students to read information from UnionPay QuickPass cards. The other one required the students to design an all-purpose campus card solution and implement a prototype system using a Mifare One (M1) 1K card. The basic experiment aimed to help the students to learn the basic knowledge of contactless smart cards, especially the security levels of different types of cards and to make a simple card reader which was necessary in the advanced experiments. The learning objectives of the advanced experiments included comprehensive application of learned knowledge and skills in cybersecurity and prior computing courses, and practice of teamwork.

The subsequent sections are organized as follows. Section II briefly introduces the principles and facilities of the experiments. Then the content of each experiment and the experimental arrangement are described in Section III. In the next section, the learning effect is evaluated by classroom tests and the experimental results with feedback from the students. The last section is conclusion and future study.

II. EXPERIMENTAL PRINCIPLES AND FACILITIES

The contactless smart card experiments involve technologies on Radio Frequency Identification (RFID), Near Field Communication (NFC), and smart cards. An Arduino development board and an RFID-RC522 module are

This work was sponsored by Tsinghua University Undergraduate Teaching Reform Project (2017 Spring ZY01_02).

required with a few types of contactless smart cards common in our daily life.

A. *RFID, NFC and Contactless Smart Cards*

RFID, also known as electronic tags, uses radio signals to identify specific targets without the need for mechanical or optical contact. A passive RFID tag can use the induced current in the electromagnetic field emitted by the tag reader to obtain energy. An active RFID tag can obtain energy directly from the power supply and then send a specific frequency signal, which can be decoded by the tag reader to extract the tag data.

The NFC technology evolved from RFID. The operating frequency is 13.56 MHz and the effective distance is within 20 cm. After establishing the connection between the NFC initiator device (master device) and the target device (slave device), bidirectional data exchange can be performed. The NFC standard is compatible with the standard for common contactless Integrated Circuit (IC) cards, so an NFC-enabled mobile phone can read IC cards' information through an application.

Common contactless smart cards include RFID cards operating at 125 kHz and Radio Frequency Integrated Circuit (RFIC) cards operating at 13.56 MHz. The former only have a fixed serial number without data space. The latter have a data storage area and custom data can be accessed. A common M1 card is an RFIC card with multiple sectors for data storage. Each sector has an independent key and access control. Some IC cards also integrate a microprocessor CPU and a Chip Operating System (COS) to provide stronger capability of command processing and data security protection. They are called CPU cards.

B. *RFID-RC522 Module and Arduino Board*

The RFID-RC522 module can support multi-layer applications of ISO14443A at 13.56 MHz without any other circuit, and can communicate with various types of M1 cards for ease of use. In our contactless smart card experiments, the RFID-RC522 module is connected to an Arduino development board, and a simple card reader can be implemented through the Arduino program. Fig. 1 shows the connection scheme between the RFID-RC522 module and the Arduino Uno board.

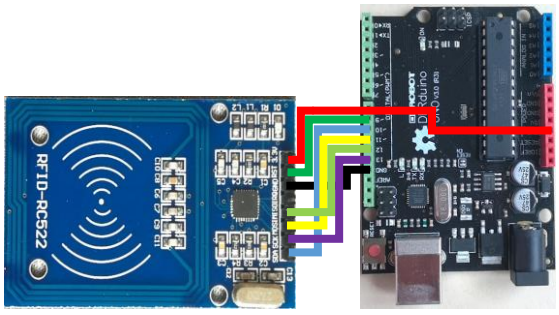

Fig. 1. Connection scheme between RFID-RC522 and Arduino Uno

Many Arduino programs that use the RFID-RC522 module to read and write M1 cards can be found on the Internet. The MFRC522 library provided in [12] has been packaged for reading and writing several types of M1 cards. The example code for important functions support basic reading and writing operations without any modification. In addition to the Arduino language, Python is also possible to program to control the Arduino board through the serial port.

C. *Various Cards and Card Safety Sleeves*

In our class, each student had at least 3 contactless smart cards: a Resident Identity Card, a Student Campus Card, and a UnionPay QuickPass card. Some students had multiple UnionPay QuickPass cards issued by different banks and contactless smart cards for public transport, boiled water supply, and door access control. These cards had different operating frequencies, and there were differences in hardware composition and level of data security. To take the experiments, the students were also provided with blank M1 cards and card safety sleeves, which could shield radio signals to ensure card information security.

III. Experimental Contents and Arrangement

A. *Basic experiment*

The basic experiment was divided into two stages: preparation and practical operation. In the first stage, the students were required to:

1) Learn the basics of Arduino development board and understand the basic structure and syntax of Arduino language.

2) Learn the basics of contactless smart cards, including the working principle, the types of cards, the structure of memory in the cards, and access operations.

3) Learn the basics of the RFID-RC522 module and learn how to connect it to the Arduino Uno development board.

4) Download and install Arduino's MFRC522 library and read the library's document.

In the second stage, the students were required to:

1) Connect the Arduino Uno development board and the RFID-RC522 module to create a card reader. Program to display the type and serial number of the contactless smart card on the serial monitor, and try to display the data stored in each sector of the card.

2) Try to read the Resident Identity Card, the Student Campus Card, the Public Transport Card, the UnionPay QuickPass card, and various types of contactless smart cards in daily life with the card reader to determine which cards can be read and which cards cannot. For those readable cards, what is the type of the card, what data can be read out, and has the data been encrypted?

3) Test the distance from the card reader to access the card. Is the card still accessible in a wallet or in a clothes pocket? Put the card in a card safty sleeve and test whether it can be accessed by the reader.

4) Summarize the types and security levels of various contactless smart cards, and discuss the potential safety problems in daily use.

B. *UnionPay QuickPass Cards Experiment*

The two advanced experiments were extension of the basic experiment. The first advanced experiment asked the students to find files about the standard of UnionPay QuickPass cards and then program to retrieve information from the cards.

UnionPay QuickPass is a small and fast payment application conforming to *China financial integrated circuit card specifications*. The specifications have stipulations on the protocols from the physical layer to the application layer, and are compatible with other international protocols with specific encryption methods. The financial IC card is a CPU card and has its own file system. After the card reader establishes a connection with the card, a payment environment needs to be selected, and then a file named 1PAY.SYS.DDF01 can be accessed to obtain a Directory Definition File (DDF). By reading the DDF, information of various Application Definition Files (ADFs) can be obtained. An application can be selected by its Application Identifier (AID), and the metadata customized by the issuing bank may be further obtained through Short File Identifiers (SFIs).

In this advanced experiment, the bank account number, the transaction log, and the balance of the QuickPass mobile wallet can be retrieved without any secret access key. The card holder's name and resident identity number are also included in some bank cards.

C. *All-purpose Campus Card Experiment*

An all-purpose card supports a number of functions with a single card, for example, a Public Transport Card and a campus card. An M1 card has sector-based data storage and access control, which is ideal for implementing an all-purpose card.

The second advanced experiment asked the students to design a secure all-purpose campus card solution based on an M1 1K card. The elementary functions include validity period management, student enrollment management, and mobile wallet payment. The students should implement a prototype system for the following multiple scenarios: a) creating a new card, b) canceling an old card, c) updating a student's enrollment status, d) configuring access control (i.e. the card can be used to open the specified doors if it is within the validity period and the enrollment information meets the access control condition), and e) recharging and making payment using the mobile wallet.

In real life, some M1 card applications do not make effective use of the card's data security features. For example, some systems only implement the access control application by reading the serial number of the card. Some systems use the default access key to retrieve the application data and the data is not encrypted or the encryption is weak. When designing an all-purpose campus card based on an M1 card in this experiment, security should be considered besides the data storage scheme for different functions. However, depending on the features of specific functions, it may be necessary to compromise between security and convenience of use.

D. *Experimental Arrangement*

These contactless smart card experiments were arranged in a 5-week-long summer course for the third year undergraduates. The students formed 3-person groups to do the experiments. The basic experiment was assigned to 9 groups, from which 2 groups took the UnionPay QuickPass card experiment and another 2 groups took the all-purpose campus card experiment additionally.

The schedule of the experiments was as follows:

- Week 1: The Arduino Uno development board was provided to each group with a number of accessories, such as LED lights, a buzzer and wires. The students were required to learn the basic knowledge and usage of the Arduino development board, and the basic structure and syntax of the Arduino language by themselves.
- Week 2: The RFID-RC522 module was provided with a blank M1 1K card and a card safety sleeve. The students were organized to complete the basic experiment and submit the experimental report.
- Week 3 ~ Week 5: Groups taking the advanced experiments were organized to exchange encountered problems and working progress every three working days.
- Friday in Week 5: Groups taking the advanced experiments turned in the experimental report and gave a presentation to all the class.

IV. LEARNING EFFECT

Classroom tests were managed to assess the learning of knowledge. The full assessment was based on the experimental report and the presentation made by each group.

A. *Classroom Tests*

We organized two classroom tests without early notification on the first and last day of the cybersecurity course. The questions in the two tests were the same, shown in Fig. 2.

1. Multiple Choice: What type(s) do the following contactless smart cards belong to?

① The Resident Identity Card ( )
② The UnionPay QuickPass Card ( )
③ The Student Campus Card ( )
④ The Public Transport Card ( )
⑤ The Boiled Water Supply Card ( )

A. IC Card B. ID Card C. CPU Card D. M1 Card

2. Sort the above cards ①~⑤ according to the safety of internal information in order from high to low.

_____ >= _____ >= _____ >= _____ >= _____

Fig. 2. Classroom test

In practical, the card reader made in the basic experiment cannot read the Resident Identity Card and the Student Campus Card because of operating frequency mismatch. The Public Transport Card latest released and the UnionPay QuickPass card can only be read the card's serial number and card type. Other cards can be read some unused data. So it is impossible for the students to answer correctly only by observation in the experiments. The answers of the classroom test can reflect the depth of knowledge learned by the students themselves.

There were 27 junior students took the basic experiment and 12 of them took the advance experiments in last year's cybersecurity course. Some students were absent from either test, and 23 students took both. The full score of the classroom test was 10 points. Fig. 3 is the box and whisker plot for scores of both tests.

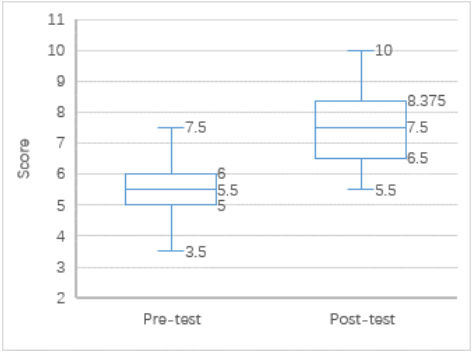

Fig. 3. The box and whisker plot for scores of both tests

B. *Experimental Outcomes*

In the UnionPay QuickPass card experiment, the students implemented a perfect reader for cards issued by Bank of China and China Merchants Bank. The reader was able to display the account number, validity period, QuickPass balance and transaction records. When programming in the experiment, the students discovered that the MFRC522 library on the Internet had a bug when handling the linking blocks in the ISO14443A protocol. The bug report and modification proposal were submitted online, which were confirmed by the original author.

In the all-purpose campus card experiment, the two groups proposed different designs. One group stored all data on the card with strong encryption for security. The other group thought if the card was lost, it was necessary to prevent loss of data so as to issue a new card with the old data recovered. Therefore, all data should be stored in an online database. However, due to ease of use, the balance of the mobile wallet within a limited amount could be stored on the card and the balance must be encrypted. The access control terminal at a non-essential location could maintain a local database and store the successful card records in the last a few days to avoid inconvenience in case of temporary network disconnection.

Both groups modified the default data access key, and the data was also encrypted. In the programs for different application terminals, only the access authority code required by the related application was included, which reduced the risk of the programs being cracked. The group with online database considered the website security of the backend system as well. These designs reflected the students' awareness and skills in cybersecurity.

C. *Student Feedback*

The students gave learning feedback in the experiment reports, which could be roughly grouped into the following aspects:

- Through experiments, the students learned the relevant knowledge of contactless smart cards comprehensively. They had real understanding and experience of the convenience and security concerns in the use of contactless smart cards, which reminded and improved their security awareness.
- The advanced experiments broadly applied the knowledge and skills learned in the cybersecurity course and previous professional courses. Various aspects of ability was exercised and improved. Finishing the experiments brought a great sense of accomplishment.
- The students realized the importance and advantages of group cooperation.

V. Conclusion and Future Study

Cybersecurity has been paid more and more attention. We believe experiments close to daily life, such as the contactless smart card experiments, are helpful for the students to learn the knowledge and skills of cybersecurity through practice, and can effectively enhance the students' security awareness. The problem-based, active and group learning in these experiments, especially in the advanced ones, was somewhat challenging. We would like to investigate the individual engagement of each group member, and try to evaluate personal learning effect in future study.

References

[1] NIST, National Initiative for Cybersecurity Education Strategic Plan, September 2012.

[2] W.A. Conklin, R.E. Cline, and T. Roosa, "Re-engineering cybersecurity education in the US: an analysis of the critical factors," in Proceedings of the Annual Hawaii International Conference on System Sciences, 2014, pp. 2006-2014.

[3] A. McGettrick, "Toward effective cybersecurity education," IEEE Security & Privacy, vol. 11(6), pp. 66-68, 2013.

[4] A. McGettrick, "Toward curricular guidelines for cybersecurity," in Proceedings of the 45th ACM technical symposium on computer science education, 2014, pp. 81-82.

[5] C. Tunc, S. Hariri, F. D. L. P. Montero, et al, "CLaaS: Cybersecurity Lab as a Service -- design, analysis, and evaluation," in Proceedings of 2015 International Conference on Cloud and Autonomic Computing, Boston, MA, 2015, pp. 224-227.

[6] L. Mcdaniel, E. Talvi, and B. Hay, "Capture the flag as cyber security introduction," in Proceedings of the Annual Hawaii International Conference on System Sciences. 2016, pp. 5479-5486.

[7] K. Boopathi, S. Sreejith, and A. Bithin, "Learning cyber security through gamification, " Indian Journal of Science & Technology, vol. 8(7), pp. 642-649, April 2015.

[8] X. Wu, and S. Tian, "Student-centered learning in cybersecurity in summer semester," in Proceedings of the 45th Annual Frontiers in Education Conference, El Paso, TX, USA, 2015, pp. 1-4.

[9] M. Savari, and M. Montazerolzohour, "All about encryption in smart card," in Proceedings of the International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), Kuala Lumpur, 2012, pp. 54-59.

[10] X. Dua, B. Niu, "A change password attack resistant scheme for remote user authentication using smart card," in Proceedings of the IEEE International Conference of Online Analysis and Computing Science (ICOACS), Chongqing, China, 2016, pp. 269-272.

[11] M. Roland and J. Langer, "Cloning credit cards: a combined pre-play and downgrade attack on EMV contactless," in Proceedings of the 7th USENIX conference on Offensive Technologies (WOOT'13), USENIX Association, Berkeley, CA, USA, 2013, pp. 1-12.

[12] https://github.com/miguelbalboa/rfid