



Using the Security Protocol Game to teach computer network security

Leonard G. C. Hamey, Department of Computing, Macquarie University
len@ics.mq.edu.au

Abstract: The Security Protocol Game is a highly interactive game for teaching secure data communications protocols. Students use the game to simulate security protocols and explore possible attacks against them. The power of the game lies in the representation it provides for secret and public key cryptography – a unique combination of game rules and playing pieces has been devised that accurately represents the mathematical capabilities of cryptographic systems. Using pen and paper, envelopes and printed game pieces, students can simulate a wide range of computer network security protocols including well-known protocols such as SSL and Pretty Good Privacy. Such simulations enable students to gain a deep understanding of how the protocols operate and how protocol design affects security of the protocol. Student response to the game is positive and engaging. It has been successfully used with both information technology students and management students. This paper presents the game briefly followed by analysis and discussion of a recent survey of student response to the game.

Introduction

Internet security is now an important aspect of information technology in business applications. Internet security is dependent upon two key elements. Cryptographic methods are used to secure data for transmission, and secure communication protocols provide the framework for communication. Information technology students need to understand both these concepts in order to properly understand secure data communications.

Students often have difficulty understanding secure communication protocols. Unlike other data communication protocols, security protocols must be designed with an adversary in mind – an intruder whose intent is to subvert the communication. The design of security protocols is largely driven by the need to prevent intrusion. Subtle errors in a protocol may make it vulnerable to attack. The Security Protocol Game (Hamey 2003) provides a simulation environment where students can study various protocols and explore the possible attacks against them, providing a real understanding of protocol operation and design. In this paper, we present an overview of the game results of a survey of student response to the game.

The Security Protocol Game uses a simple representation of public key (Diffie and Hellman 1976) and secret key cryptographic systems and related algorithms. The representation uses coloured envelopes, coloured paper and coloured key tokens to incorporate the key properties of the cryptographic systems into the game. For example, to encrypt a message, a player encloses it in a coloured envelope. This represents the confidentiality provided by encrypting the message – other players cannot read a message that is enclosed in an envelope. The rules of the game complement the representation. For example, a player may only open an envelope if they hold the appropriate cryptographic key token, simulating the mathematical requirement that a player can only decrypt a message if they have the cryptographic key.

The idea of using physical representations to explain security protocols is not new. Chaum (1985) uses a representation involving envelopes and rubber stamps to explain blind signature schemes. Bell, Thimbleby, Fellows, Witten and Koblitz (1999) use a representation involving a chain and padlocks to explain Diffie-Hellman key exchange (Diffie and Hellman 1976) to a non-technical audience. In neither case do the authors attempt to develop a representation that covers the diverse applications of public-key and secret-key cryptographic systems. The Security Protocol Game provides such a representation that can be used to study both simple security protocols and real-world secure communication protocols.

We have used the game for a number of years in teaching secure communications protocols as part of an undergraduate unit on computer networks. The unit covers computer network architecture at all levels, with a focus on the Internet. Secure communications protocols are an important but relatively small part of the unit. Recently, we surveyed students in this unit concerning their response to the use of the game. Our purpose was to identify strengths and weaknesses of the game for future development, and to evaluate it as an educational tool. The results of this survey are presented below.

Overview of the game

Discussions of cryptographic methods commonly involve three parties: Alice and Bob, who wish to communicate, and an intruder, Trudy, who seeks to subvert the security of the communications between Alice and Bob. Some protocols introduce a trusted party variously known as Big Brother or the key distribution centre. The Security Protocol Game uses the conventional roles of Alice, Bob and Trudy, with Gavin as the trusted authority. The game adds the role of Colin, the copying engine. Colin is not a part of the communication protocols. He provides copying and computational services to the other players, representing the innate capabilities of computer systems to produce identical copies of arbitrary messages, and to perform other relevant computations.

Students play the game in groups of 4-5 players. Within each group, one student is selected to play each of Alice and Bob, the two communicating parties. Another student is selected to play Gavin. The same student may also take the role of Colin. The remaining student or students take the role of Trudy the intruder.

The game commences with the students seated around a table: Alice and Bob at opposite ends, Trudy on one side and Gavin opposite her. The students select a game scenario to play, and a protocol to use in the scenario. In a typical scenario, Alice wishes to purchase computer software from Bob over the Internet using her credit card for payment. The students may choose to simulate the Transport Layer Security protocol (TLS; formerly called SSL and used to secure transactions on the world wide web) for this scenario, or other protocols, some of which are vulnerable to various attacks. The protocols involve messages being passed between Alice, Bob and Gavin. All messages are actually passed via Trudy, who may attempt to attack the protocol by monitoring or modifying the messages. The students find this a stimulating group activity as they help each other run the protocol correctly and try to think up ways to subvert it.

Cryptographic systems and their representation

Two important types of cryptographic systems are secret key methods (symmetric algorithms) and public key methods. Secret key cryptography is the conventional form in which Alice and Bob use the same key to encrypt E and decrypt D a plain text message for secure transmission. In the Security Protocol Game, a plain text message is written on white paper (see Figure 1). Secret keys are represented by coloured key tokens. Alice ‘encrypts’ the plain text message by enclosing it in an envelope of the same colour as the key. A player must hold the colour matched key token to open the envelope. Using secret key cryptography, Alice and Bob can ensure that the message is not readable by Trudy (confidentiality), that it cannot be modified during transmission (integrity) and that it originates from a person who knows the secret key (authentication).

Public key cryptography differs from secret key methods in that encryption and decryption use the same algorithm P but different keys for encryption and decryption. Each party has their own pair of keys. One of the keys (for example, Bob’s key EB) is public knowledge while the other key DB is private. In the Security Protocol Game, coloured key tokens are used to represent private and public keys, and a matching coloured envelope is used for encryption with a public key.

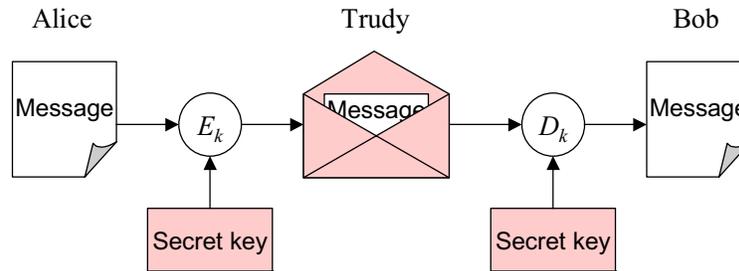


Figure 1: Secure transmission from Alice to Bob using secret key cryptography

Public key cryptography can also be used for authentication. Bob encrypts a message using his private key DB and other players can then decrypt it with the public key EB . In the Security Protocol Game, the holder of a private key authenticates a message by writing it on coloured paper. Since the public key is assumed to be public knowledge, this representation explicitly allows Trudy to read the message, although she may not modify it.

A variety of other key concepts of secure communications protocols can also be represented in the game, including public key certificates, message digests and digital signatures, transmitting encrypted keys and key exchange techniques. Hamey (2003) presents the game in greater detail.

Using the game

We have used the game as an exercise for postgraduate management students and as a tutorial activity for third year computing students in the unit Computer Networks. In the computing unit, the game was used for two tutorial hours. In the first tutorial hour, the tutor demonstrated the game on a simple example, and the students subsequently played up to two rounds of the game. In the second hour, the students had become familiar with the representation and were able to explore more complex protocols or even create and test their own protocols.

Student survey

To evaluate student response to the game, we conducted a survey of students who used the game in our third year undergraduate Computer Networks unit. This is the first computer networks unit undertaken by these students. It provides an overview of computer network architecture with detailed study of issues at each level. Secure communications protocols are an important part of the unit, but receive only limited lecture coverage. To complete the presentation, students experience two tutorial hours with the Security Protocol Game. The survey was conducted during the second tutorial hour.

The purpose of the questionnaire was to obtain student evaluation of the game, and to identify issues for further investigation in future work. 71 students completed the questionnaire, representing half of the unit enrolment. The response rate was primarily related to attendance at tutorials – most of the students present in the tutorials chose to complete the questionnaire.

The questionnaire consisted of two parts. The first part contained nine statements that students responded to using a Likert scale from ‘strongly disagree’ (1) to ‘strongly agree’ (5), with the option to select ‘not applicable’. The second part contained three open-ended questions about the game and an additional opportunity for students to comment on other aspects of the unit unrelated to the game.

The survey was developed and conducted with the assistance of the Centre for Professional Development of Macquarie University. The centre regularly conducts student evaluation surveys of units of study. The administration of the survey was in accordance with procedures familiar to the

students, except that the students were informed that this survey was part of a research project and that results of the survey would be published.

Likert statements

The following nine statements were provided to measure student response to the game.

- I enjoyed playing the security protocol game.
- I was able to understand the rules of the game.
- The game helped me understand how security protocols work.
- After playing the game, I understand better how SSL works.
- The game showed me how important it is to design security protocols properly.
- The game helped me understand how to design a security protocol properly.
- The game helped me understand the lecture material better.
- The security protocol game is a worthwhile learning experience.
- I would understand computing better if other units used activities like the game.

These statements were designed to measure student response in the areas of enjoyment, understanding of the game itself, understanding of learning goals, and perceived value of game-based learning. The primary goal of the game is to help students understand how security protocols work and the potential attacks against them – SSL is used as an example protocol. The game models a credit card purchase over the Internet, so we expect students to gain an appreciation of the importance of security protocol design through seeing weak protocols broken. It is possible for students to design and test their own protocols, but students often do not have time in this unit to explore this aspect, so we expect fewer students to learn about protocol design. The last two questions probe the students' evaluation of the game as a learning experience.

Open-ended questions

The open-ended questions were designed to provide feedback about the strengths and weaknesses of the game as a tool, and to identify the students' learning focus. The three questions were as follows.

- What is the best aspect of the security protocol game?
- What would you like to see improved in the game?
- What is the most important thing you learned from playing the game?

Student responses

Student responses to the Likert questions were positive, but not strong. Average response values ranged from 3.5 (halfway between 'neutral' and 'agree') to 4.0 ('agree') with some students strongly agreeing and others strongly disagreeing with individual statements.

Students generally enjoyed the game (average value 3.9) and valued it as a learning experience (average value 4.0). More than 80% of students agreed or strongly agreed that they would understand computing better if other units used activities like the game (average value 4.0).

With respect to learning outcomes, 85% of students agreed or strongly agreed that the game showed them how important it is to design security protocols properly (average response 4.0). 76% of students agreed or strongly agreed that the game helped them understand how security protocols work (average response 3.9). 62% of students agreed or strongly agreed that the game helped them understand the lecture material (average response 3.6). 61% agreed or strongly agreed that it helped them understand how to design a security protocol properly (average response 3.6). 56% of students agreed or strongly agreed that the game helped them understand better how SSL works (average response 3.5).

Understanding of the rules appears to have been an obstacle for some of the students. Only 73% of students agreed or strongly agreed that they were able to understand the rules of the game, while 7%



disagreed. The open-ended question responses also included comments on the rules. We believe this is an area for improvement that would benefit the students significantly.

The responses to the Likert questions indicate that the students believe they benefited from using the game as a learning experience, that they achieved significant learning outcomes and that they believe they would benefit from similar activities in other parts of their course.

We also analysed the Likert question responses for differences between tutorial groups. We found that students who were taught by tutors with prior experience of using the game responded more positively to all questions than students who were taught by tutors using the game for the first time. The differences were between 0.5 and 0.9 in the average response. This result indicates that the tutor's ability to guide the students in their use of the game is important for student success. We believe that improving the written presentation of the game (the rules) may reduce this difference, but we believe that it would also be beneficial to give the tutors practical experience with playing the game themselves in a group before they take their tutorial classes.

Open-ended responses

In response to the open-ended questions, the students wrote 123 distinct comments. These were collated and classified to identify trends and issues.

With regard to the best aspect of the security protocol game, 44 responses were provided. The most common response, given by 15 students, related to learning and understanding security protocols or the attacks upon them. 7 students identified group interaction as the best aspect of the game while 6 students focused on the hands-on approach provided by the game. Many other responses were received ranging over aspects of the game such as its visual appeal, the fun or challenge aspect, and the importance of security on the Internet.

37 responses were received concerning improvements to the game. The dominant response was a request for improvement in the clarity and presentation of the rules (11 students). This area was also identified for improvement by the Likert question responses. The students gave specific suggestions for improvement. We plan to work with a student focus group to develop a rules document that is easier for the students to use.

7 students requested solutions to the game – specific strategies for Trudy to break particular protocols. Such solutions are provided to tutors but have not been provided to the students. A student focus group could be used to identify how much information to provide so that students can explore attacks on the protocols while still facing a suitable learning challenge.

7 students wanted more time devoted to the game, expressing the desire to understand the more difficult concepts that the game supports. A further 7 students requested a computerised version of the game, so that they could play it online. 2 students identified problems they experienced with group interaction.

For the question asking the students to identify the most important thing they learned from playing the game, 37 responses were received. The dominant response (12 students) was that they learned how to attack, break or 'hack' protocols. 8 students identified learning how the protocols work as the most important thing, with a further 3 students specifically focusing on learning about SSL. 5 students said the most important thing they learned was related to the security risks of using the Internet and 3 identified the most important thing they learned as being the importance of security protocols. With a couple of humorous exceptions, the learning outcomes identified by the students were desirable learning outcomes for the unit.

Conclusion

The Security Protocol Game is a stimulating group activity that helps students understand the design and operation of protocols for secure data communications. The game provides a rich environment capable of simulating both simple and complex protocols. A student survey confirms that the game assists students to achieve relevant learning outcomes including understanding the importance of proper design of security protocols, how security protocols work and the attacks against them. The survey has also identified opportunities to improve the game, particularly in the presentation of the rules.

References

- Bell, T., Thimbleby, H., Fellows, M., Witten, I. and Kobnitz, N. (1999) Explaining cryptographic systems to the general public. In L. Yngström and S. Fischer-Hübner (Eds) *Proceedings IFIP TC11 WG11.8 Conference*. Stockholm, Sweden: First IFIP World Conference on Information Security Education (WISE), 221-233.
- Chaum, D. (1985) Security without identification: transaction systems to make big brother obsolete. *Communications of the ACM*, **28**(10), 1030-1044.
- Dierks, T. and Allen, C. (1999) *RFC 2246: The TLS Protocol Version 1.0*. Internet Engineering Task Force.
- Diffie, W. and Hellman, M. E. (1976) New directions in cryptography. *IEEE Transactions on Information Theory*, **22**(6), 644-654.
- Hamey, L. (2003) Teaching secure data communications using a game representation. In T. Greening and R. Lister (Eds) *Proceedings of the Fifth Australasian Computing Education Conference, Conferences in Research and Practice in Information Technology*. Adelaide: SA: Australian Computer Society, **20**, 187-196.

© 2003 Leonard G. C. Hamey.

The author assign to Uniserve Science and educational non-profit institutions a non-exclusive license to use this document for personal use and in courses of instruction provided that the article is used in full and this copyright statement is reproduced. The author also grant a non-exclusive license to Uniserve Science to publish this document in full on the Web (prime sites and mirrors) and in printed form within the UniServe Science 2003 Conference Proceedings. Any other usage is prohibited without the express permission of the author.