

A Simulation Game for Teaching Secure Data Communications Protocols

Leonard G. C. Hamey

Department of Computing, Macquarie University, Sydney, Australia

ABSTRACT

With the widespread commercial use of the Internet, secure data communications over the Internet has become an important aspect of business operations. Thus, it is an important study for information technology and management students. The Security Protocol Game is an interactive group activity for exploring secure data communication protocols. Using pen and paper, envelopes and game tokens, students simulate security protocols and possible attacks against them. The game provides simple and intuitive representations for cryptographic methods, including both public key and secret key techniques. Using these representations, students can simulate Internet application protocols such as Pretty Good Privacy (used to secure email) and Transport Layer Security (used for secure web transactions). They can explore well-known protocols for authentication, key exchange and blind signatures. Students can also develop and test their own protocols using public key certificates, encrypted key transmission, tunnelling and other well-known techniques. Through this learning activity, students gain a deep understanding of how security protocols operate and are designed. The game has been used in tertiary units of study for managers and information technology students.

KEYWORDS

Simulation games, computer network, secure communication, cryptography, protocols.

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 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 and demonstrate its operation with an example play scenario.

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, *et al* (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.

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 4-6 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).

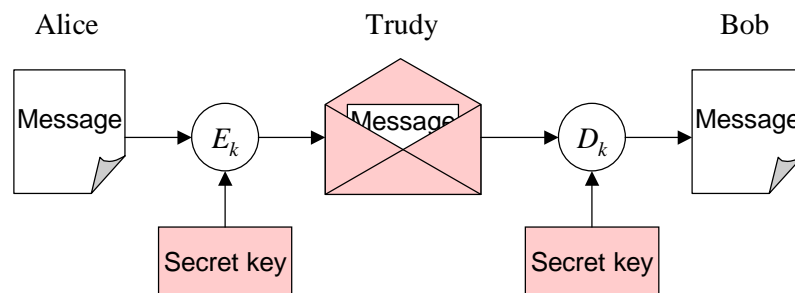


Figure 1: Secure transmission from Alice to Bob using secret key cryptography.

Secret key algorithms require the parties to initially share the key. This limitation can be overcome by using a key distribution centre or public key methods.

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. If Alice encrypts a message using Bob’s public key EB and transmits it to Bob, then only Bob can decrypt it since only he knows the decryption key DB . Thus, confidentiality is achieved without an initial shared secret. 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, as shown in figure 2.

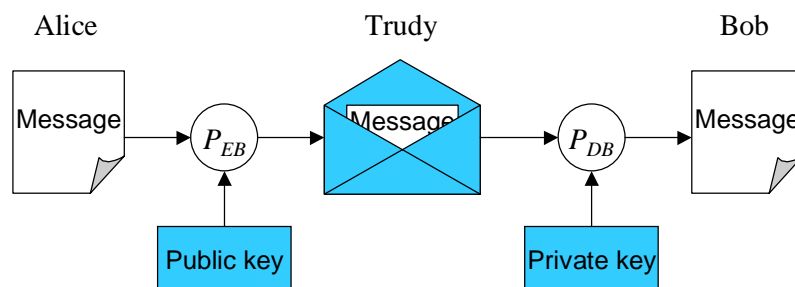


Figure 2: Confidential message using public key cryptography.

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 . Since EB is public knowledge, any party can decrypt and read the message, but only Bob could have created the message since only Bob knows the key DB . This is a simple form of digital signature. In the Security Protocol Game, the holder of a private key authenticates a message by writing it on coloured paper (figure 3). 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.

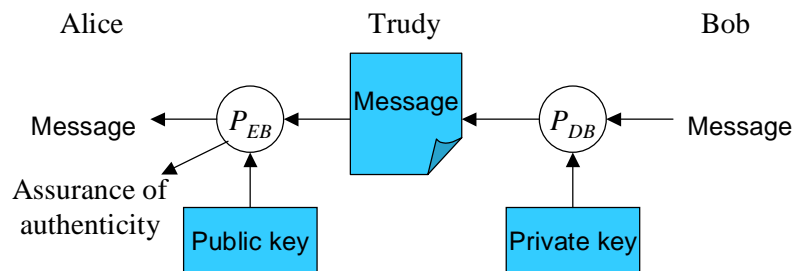


Figure 3: Message authentication using public key cryptography.

Alice's assurance that Bob is the author of the message is dependent upon knowing that the blue public key belongs to Bob. This is achieved with a public key certificate. In the Security Protocol Game, all players know that Gavin's public key is gold. Gavin creates a message stating the holder of a public key and authenticates that message by writing it on gold paper (figure 4). This certificate provides the evidence that Alice needs. Public key certificates are used for authentication on the Internet.

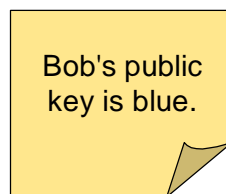


Figure 4: A public key certificate, written on gold paper.

A variety of other key concepts of secure communications protocols can also be represented in the game, including message digests and digital signatures, transmitting encrypted keys and key exchange techniques.

EXAMPLE SCENARIO

Secure data communications is used in a variety of application scenarios. The Security Protocol Game contains a number of such scenarios including purchasing software over the Internet, authenticating free software (such as a web browser plug-in), authorizing a stock market transaction, and establishing and using a virtual private network (VPN) connection.

In the software purchase scenario, Alice wishes to purchase computer software over the Internet from Bob, using her credit card for payment. Trudy wishes to subvert the communication for her own benefit or to the detriment of Alice or Bob. In this scenario, Alice and Bob win the game if they are able to securely transmit the credit card number and the software to the other party. Trudy wins if she is able to obtain Alice's credit card number, obtain a copy of the software without

paying for it, cause Alice to pay double for the software, or cause Alice to accept a corrupted version of the software.

The scenario may be played with a variety of protocols including TLS (Dierks and Allen, 1999). Here we consider a simple protocol that is vulnerable to attack (table 1), demonstrating how Trudy can defeat the protocol.

Step	Transmit	Message
1	A → B	Hello with public key certificate attached
2	B → A	Hello with public key certificate attached
3	A → B	Credit card number encrypted with Bob's public key
4	B → A	Software encrypted with Alice's public key

Table 1: Protocol PK2: A vulnerable protocol for the credit card purchase scenario.

Steps 1 and 2 of protocol PK2 exchange public key certificates so that each party knows the other's public key. Using the public keys to ensure confidentiality, Alice sends her credit card to Bob in step 3 and Bob sends the software to Alice in step 4. Figure 5 (a)-(c) show that first three messages that are exchanged between Alice and Bob in following this protocol.

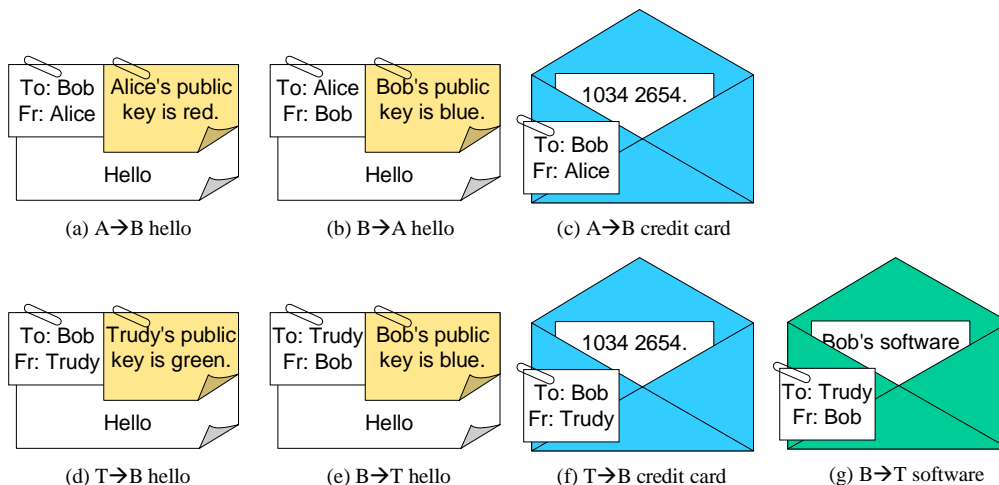


Figure 5: Example scenario – Alice and Bob's messages and Trudy's attack.

Although Trudy cannot read the credit card number in figure 5(c), Trudy can successfully attack the protocol as shown in figure 5 (d)-(g). Trudy first captures the message created by Alice in step 3 and, instead of passing it to Bob, aborts the connection. She now initiates her own communication with Bob (figure 5(d)), following the protocol as if she was a customer. Since Bob is a software vendor, he must be willing to sell to any customer, including Trudy, provided that the customer follows the protocol. The subterfuge occurs in step 3 of the protocol where Trudy passes off the captured message containing Alice's credit card number as her own. Bob accepts the credit card as valid and sends the software to Trudy. Even though she cannot decrypt Alice's message, Trudy can still subvert the protocol and obtain the software while causing Alice to be charged for it.

Notice that the security violation we have demonstrated has nothing to do with breaking the cryptographic security of the public-key cryptography system, but rather exploits a weakness in the

security protocol itself. The Security Protocol Game focuses attention on the strengths and weaknesses of protocols rather than cryptographic systems, demonstrating clearly that security is dependent not only upon using adequate cryptographic algorithms but also requires well designed protocols.

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 units, 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. We found that introducing the game gave students a much greater understanding of security protocols, as evidenced by their examination performance in that aspect of the unit.

We believe that one of the benefits of the game, particularly for computing students, is that it is a very different type of activity from their usual course work. Their laboratory tasks and assignments are all individual computer based work, while their tutorial exercises tend to focus on discussion questions and written exercises. Hands-on simulation activities such as the Security Protocol Game provide a welcome and stimulating change, developing small group interaction within the class and encouraging group learning. The game provides a balance to the computer based learning activities that the students are involved in.

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. The game is suitable for teaching secure data communications to undergraduate and postgraduate students in information technology and management.

REFERENCES

- Bell, T., Thimbleby, H., Fellows, M., Witten, I., and Kobnitz, N. (1999): Explaining cryptographic systems to the general public. In Yngström, L. and Fischer-Hübner, S., *First IFIP World Conference on Information Security Education (WISE), Proceedings IFIP TC11 WG11.8 Conference*. Stockholm University/Royal Institute of Technology, Sweden, 221-233.
- Chaum, D. (1985): Security without identification: transaction systems to make big brother obsolete. *Communications of the ACM*, **28**(10): 1030-1044.
- Diffie, W. and Hellman, M.E. (1976): New directions in cryptography. *IEEE Transactions on Information Theory*, **22**(6): 644-654.
- Dierks, T. and Allen, C. (1999): *RFC 2246: The TLS Protocol Version 1.0*. Internet Engineering Task Force.