

Principles of Information Security CS 5323 Lecture Five

Prof. William Winsborough
September 11, 2007

Business

- There will be a test on the password material in Anderson Chapter 3 on Tuesday September 19
 - It will not be discussed in class
 - The test will be worth about 10% of your grade
- One component (about 5%) of your grade will be based on your own assessment of your class participation

11 September 2007

Winsborough CS 5323 Lecture 5

2

More Sophisticated Challenge and Response: Password Generator

- Add a password generator P that takes input from a user U that knows a PIN and that interacts with server S
 - $S \rightarrow U : N$
 - $U \rightarrow P : N, \text{PIN}$
 - $P \rightarrow U : \{N, \text{PIN}\}_K$
 - $U \rightarrow S : \{N, \text{PIN}\}_K$
- Notice that the encryption need not be invertible in this case
- This protocol combines something you have with something you know

11 September 2007

Winsborough CS 5323 Lecture 5

3

Man-in-the-middle Attacks

- “Middleperson attacks”
- Identify Friend or Foe (IFF)
 - Radar sends challenges
- Attack:
 - Bad guy forwards challenge to one of your friends, who tells the bad guy how to respond to the challenge
- Response signal strength can be strong
 - Can give away location of responder
 - Motivates making challenge be authenticatable

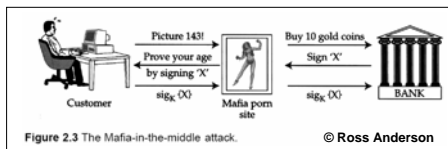
11 September 2007

Winsborough CS 5323 Lecture 5

4

Chosen Protocol Attacks

- Potential problem with simplistic “multifunction smartcard”
 - Problem: the significance of signing a message depends on the protocol



11 September 2007

Winsborough CS 5323 Lecture 5

5

Key Management

- Kerberos was the first widely used authentication protocol for supporting key management
 - The following builds of to a basic outline of Kerberos
- Basic key management
 - A : Alice, who wants to communicate with Bob
 - B : Bob
 - S : Sam, a trusted third party that introduces them
 - T : Timestamp

$$A \rightarrow S : A, B$$

$$S \rightarrow A : \{A, B, K_{AB}, T\}_{K_{AS}}, \{A, B, K_{AB}, T\}_{K_{BS}}$$

$$A \rightarrow B : \{A, B, K_{AB}, T\}_{K_{BS}}, \{M\}_{K_{AB}}$$

11 September 2007

Winsborough CS 5323 Lecture 5

6

Needham-Schroeder Protocol (1978)

Message 1 $A \rightarrow S : A, B, N_A$
 Message 2 $S \rightarrow A : \{N_A, B, K_{AB}, \{K_{AB}, A\}_{K_{BS}}\}_{K_{AS}}$
 Message 3 $A \rightarrow B : \{K_{AB}, A\}_{K_{BS}}$
 Message 4 $B \rightarrow A : \{N_B\}_{K_{AB}}$
 Message 5 $A \rightarrow B : \{N_{B-1}\}_{K_{AB}}$

- Revocation problem
 - Sam will have to keep track of everyone who has ever received a ticket to communicate with Alice in case K_{AS} is ever compromised

11 September 2007

Winsborough CS 5323 Lecture 5

7

Kerberos

- Derived from Needham-Schroeder
- Two kinds of trusted third parties:
 - Authentication server
 - Ticket-granting server
 - Tickets allow access to corresponding resources
- Reason: Scalability
 - Authentication is managed by, e.g., residence hall or payroll department
 - Ticket granting is managed by resource owners/administrators

11 September 2007

Winsborough CS 5323 Lecture 5

8

Kerberos Authentication Server Protocol Sketch

$A \rightarrow AS : A$
 $AS \rightarrow A : \{K_{AS}, \dots\}_{\text{Alice password}}$

- AS is authentication server
- Alice can decrypt and use K_{AS} just in case she knows the right password

11 September 2007

Winsborough CS 5323 Lecture 5

9

Kerberos Ticket-granting Protocol

$A \rightarrow S : A, B$
 $S \rightarrow A : \{T_S, L, K_{AB}, B, \{T_S, L, K_{AB}, A\}_{K_{BS}}\}_{K_{AS}}$
 $A \rightarrow B : \{T_S, L, K_{AB}, A\}_{K_{BS}}, \{A, T_A\}_{K_{AB}}$
 $B \rightarrow A : \{T_A+1\}_{K_{AB}}$

- S is Ticket-granting service
- B is resource
- Last message demonstrates B is live
- Use of timestamps in place of nonces give advantage over Needham-Schroeder
- Vulnerability: clock desynchronization

11 September 2007

Winsborough CS 5323 Lecture 5

10

BAN Logic: Burrows, Abadi, Needham

- One formal method for protocol verification

$A \models X$: A believes X , or, more accurately, that A is entitled to believe X .

$A \sim X$: A once said X (without implying that this utterance was recent or not).

$A \models X$: A has jurisdiction over X ; in other words, A is the authority on X , and is to be trusted on it.

$A \triangleleft X$: A sees X ; that is, someone sent a message to A containing X in such a way that A can read and repeat it.

$\#X$: X is fresh; that is, X contains a current timestamp or some information showing that it was uttered by the relevant principal during the current run of the protocol.

$\{X\}_K$: X encrypted under the key K , as in the rest of this chapter.

$A \leftrightarrow^K B$: A and B share the key K ; in other words, it is an appropriate key for them to use to communicate.

11 September 2007

Winsborough CS 5323 Lecture 5

11

Some of the Rules of Inference

The message-meaning rule. States that if A sees a message encrypted under K , and K is a good key for communicating with B , then A will believe that the message was once said by B . (We assume that each principal can recognize and ignore his or her own messages.) Formally:

$$\frac{A \triangleleft \{X\}_K \quad A \leftrightarrow^K B, A \triangleleft \{X\}_K}{A \models B \sim X}$$

The nonce-verification rule. States that if a principal once said a message, and the message is fresh, then that principal still believes it. Formally:

$$\frac{A \models \#X, A \sim B \sim X}{A \models B \models X}$$

The jurisdiction rule. States that if a principal believes something, and is an authority on the matter, then he or she should be believed. Formally, we write that:

$$\frac{A \models B \models X, A \models B \models X}{A \models X}$$

11 September 2007

Winsborough CS 5323 Lecture 5

12