

Principles of Information Security

CS 5323 Lecture Six

Prof. William Winsborough
September 13, 2007

Business

- Recall: test on the password material in Anderson Chapter 3 on Tuesday 9/18
- Read Gollmann Chapter 4 for Tuesday 9/18

Final Discussion on Protocols

- Formal verification of protocols is an active research area
- Several techniques
 - Belief logic
 - Best known: BAN Logic (Burrows, Abadi, Needham)
 - Random oracle model
 - Favored by cryptographers
 - Other formal methods
 - Model checking
- We'll illustrate using BAN Logic

13 September 2007

Winsborough CS 5323 Lecture 6

3

Typical Smartcard Banking Protocol

- Simplified version of COPAC, a protocol used by VISA

$$C \rightarrow R : \{C, N_C\}_K$$
$$R \rightarrow C : \{R, N_R, C, N_C\}_K$$
$$C \rightarrow R : \{C, N_C, R, N_R, X\}_K$$

13 September 2007

Winsborough CS 5323 Lecture 6

4

BAN Logic

- 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.

13 September 2007

Winsborough CS 5323 Lecture 6

5

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:

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

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:

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

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:

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

13 September 2007

Winsborough CS 5323 Lecture 6

6

Verifying the Payment Protocol

- Want to show the retailer is entitled to trust the check X
 - $R \models X$