

Principles of Information Security CS 5323 Lecture Four

Prof. William Winsborough
September 4, 2007

Business

- Start reading 4.0-4.2 of Anderson
- Any questions about anything related to the course??

4 September 2007

Winsborough CS 5323 Lecture 4

2

Protocol: Objectives and Evaluation

- Security protocols are the rules that govern communications between principals in a given system
- Designed so that the system will survive certain threats (malicious acts)
- Normally it is impractical to protect against all threats—realistic threats (high likelihood and/or high value) are identified by a “threat model”
- Evaluating a protocol involves answering two questions:
 - Is the threat model realistic?
 - Does the protocol deal with it?

4 September 2007

Winsborough CS 5323 Lecture 4

3

Simplest Authentication Protocol: Passwords

- Early applications: car doors, garage doors
- Guessing: 16 bit at 10/second: ~1 hour
- Eavesdropping:
 - “Grabber” device records and retransmits passcode
 - More bits don’t help

4 September 2007

Winsborough CS 5323 Lecture 4

4

Simple Authentication

- Garage door openers
 - $T \rightarrow G : T, \{T, N\}_{KT}$
 - T is in-car token (or its serial number)
 - G is garage
 - N is a *nonce* (a number that is used only once—serves to ensure freshness)
 - KT is a shared secret key (possibly $\{T\}_{KM}$ for some master key KM)
- Such protocols can often be subverted without breaking the encryption
 - Replay attacks
 - Choice of nonce: how to ensure it has not been used before
- Random nonce or counter
 - Random: key has to remember a lot of past nonces
 - Counter: how to synchronize when key is incremented but not lock

4 September 2007

Winsborough CS 5323 Lecture 4

5

Challenge and Response

- A slightly more sophisticated protocol used in car ignitions
 - $E \rightarrow T : N$
 - $T \rightarrow E : \{T, N\}_K$
 - E is engine controller
 - T is transponder for car key
 - N is a *nonce* (a number that is used only once—serves to ensure freshness)
 - K is a secret key shared between engine controller and key transponder
- The values of N generated by E must be difficult to predict (must be random enough)
 - A good source of randomness is physical world

4 September 2007

Winsborough CS 5323 Lecture 4

6

Adding User Knowledge

- Recall Vanessa's observation that today most high-security authentication mechanisms are "multi-factor"
 - Something you have
 - Something you know
 - Something you are

4 September 2007

Winsborough CS 5323 Lecture 4

7

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

4 September 2007

Winsborough CS 5323 Lecture 4

8

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
 - Motivates making challenge be authenticatable

4 September 2007

Winsborough CS 5323 Lecture 4

9