

Principles of Information Security CS 5323 Lecture Three

Prof. William Winsborough
August 28, 2007

Business

- Finish reading chapter 2 and also read chapter 3 of Anderson by Tuesday
- Any questions about anything related to the course??

30 August 2007

Winsborough CS 5323 Lecture 3

2

Important Terms

- Subject – person
 - (Or sometimes a process, I think)
- Principal
 - Subject, role, piece of equipment, communication channel, cryptographic key,...
- Group versus role
- Trust versus trustworthy
 - I (and standard Computer Security terminology) agree with RA's usage
- Anonymity
 - Source and/or destination of a message

30 August 2007

Winsborough CS 5323 Lecture 3

3

Important Terms

- Authenticity versus integrity
 - Protocol literature: authenticity = integrity + freshness
 - Military:
 - Authenticity applies to the principal issuing a command (cf. "authenticate" during login)
 - Integrity is usually applied to non-corruption of data repositories

30 August 2007

Winsborough CS 5323 Lecture 3

4

Important RJA Terms (That I Find a Little Vague)

- Security policy
 - Succinct statement of a system's protection strategy
- Protection profile
 - Device independent version of security target
- Security target
 - A more detailed specification, which sets out the means by which a security policy will be implemented

30 August 2007

Winsborough CS 5323 Lecture 3

5

Important Terms

- A *vulnerability* is a property of a system or its environment, which, in conjunction with an internal or external *threat*, can lead to a *security failure*, which is a state of affairs contrary to the system's security policy.

30 August 2007

Winsborough CS 5323 Lecture 3

6

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?

30 August 2007

Winsborough CS 5323 Lecture 3

7

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

30 August 2007

Winsborough CS 5323 Lecture 3

8

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
- Such protocols can often be subverted without breaking the encryption
 - Replay attacks
 - Choice of nonce: how to ensure it has not been used before

30 August 2007

Winsborough CS 5323 Lecture 3

9