

Principles of Information Security CS 5323 Lecture Two

Prof. William Winsborough
August 28, 2007

Business

- My apologies for not getting the web page set up
 - Anderson's book is available at <http://www.cl.cam.ac.uk/~rja14/book.html>
- Read chapters 1 and 2 of Anderson by Thursday
- Any questions about anything related to the course??

28 August 2007

Winsborough CS 5323 Lecture 2

2

Example Security Application Areas

- Bank
 - Branch book keeping
 - Separation of duties
 - Ensuring credits and debits match up
 - ATMs
 - Authentication
 - High value messaging system
 - Potential for highly motivated attackers
 - Physical security of the vault
 - Internet presence
 - SSL
 - Firewalls

28 August 2007

Winsborough CS 5323 Lecture 2

3

Example Security Application Areas

- Military Air Force Base
 - Radar jamming
 - The original denial of service attack
 - Transmissions
 - Confidentiality: easy
 - Availability: "Low probability of intercept"
 - Logistics and stores
 - Confidentiality requirements: inferences can be drawn from knowledge of stockpiles
 - Multi-level security and information flow restrictions
 - Nuclear weapons
 - Very strong authentication

28 August 2007

Winsborough CS 5323 Lecture 2

4

Example Security Application Areas

- Hospital
 - Integrity of electronic reference materials
 - PDR, patient history
 - Confidentiality of records
 - Different kinds of information are appropriate for different roles (doctors versus financial managers)
 - Staff access to records should depend on what role if any they have providing care to the patient in question
 - Anonymization of clinical data for use in research
 - Assistance in understanding orders
 - My own addition

28 August 2007

Winsborough CS 5323 Lecture 2

5

Security Measures Can Have Unexpected Consequences

- Some cars have electronic immobilizers that sends an encrypted challenge to a radio transponder in the key fob; the transponder has to respond correctly before the car will start
 - Increases car-jackings at gunpoint
- If a fingerprint is needed to transfer large sums, fingers may be removed from their rightful owners

28 August 2007

Winsborough CS 5323 Lecture 2

6

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

28 August 2007

Winsborough CS 5323 Lecture 2

7

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

28 August 2007

Winsborough CS 5323 Lecture 2

8

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

28 August 2007

Winsborough CS 5323 Lecture 2

9

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.

28 August 2007

Winsborough CS 5323 Lecture 2

10

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?

28 August 2007

Winsborough CS 5323 Lecture 2

11

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

28 August 2007

Winsborough CS 5323 Lecture 2

12