CIS 551 / TCOM 401

Computer and Network Security

Spring 2008

Lecture 26

Announcements

- Project 4 is Due Friday May 2nd at 11:59 PM

- Final exam:
  - Friday, May 12th. Noon - 2:00pm DRLB A6

- Today:
  - Course Review
  - Course evaluations

Main Take-away Ideas (1)

- Security is about Tradeoffs
  - Balance risk vs. expense

- *Principles of Secure System Design:*

- Security is a process
- Least privileges
- Complete Mediation
- System Design
  - Economy of mechanism
  - Open standards
  - Failsafe Defaults

Main Take-away Ideas (2)

- Cryptography is important…
  - Can be used for more than just hiding information
  - Authentication and integrity

- … but not the only facet of security
  - Other risks
  - Social engineering is effective
  - Cryptography applied inappropriately is useless

- So: use it where necessary, and use it correctly
  - See Schneier’s book *Applied Cryptography*

Main Take-away Ideas (3)

- Concepts of security:
  - Confidentiality
  - Integrity
  - Availability
- General Mechanisms
  - Authentication
    - Challenge / Response
  - Authorization
    - Reference monitors
    - Access control matrices
  - Audit
    - Logs

Main Take-away Ideas (4)

- Cryptography & Protocol Design
  - Shared vs. Public key cryptography
- Cryptographic protocols can be used for:
  - Authentication, privacy, confidentiality
- Challenge—Response is the fundamental method of authentication
- Nonces, Time stamps, Sequence numbers prevent replay attacks

Main Take-away Ideas (5)

- Malicious Code
  - Viruses & Worms
  - Defense in depth: patching, firewalls, proper configuration, auditing

- Buffer overflows are the #1 vulnerability
  - Choose safe languages:
    - Java, C#, Scheme, ML
  - Be aware of format string and input errors, take care when writing programs and scripts.
  - Software audit and design is important.
  - If you must use C or C++, use StackGuard, ProPolice, or another buffer-overflow preventative measure.

Further study

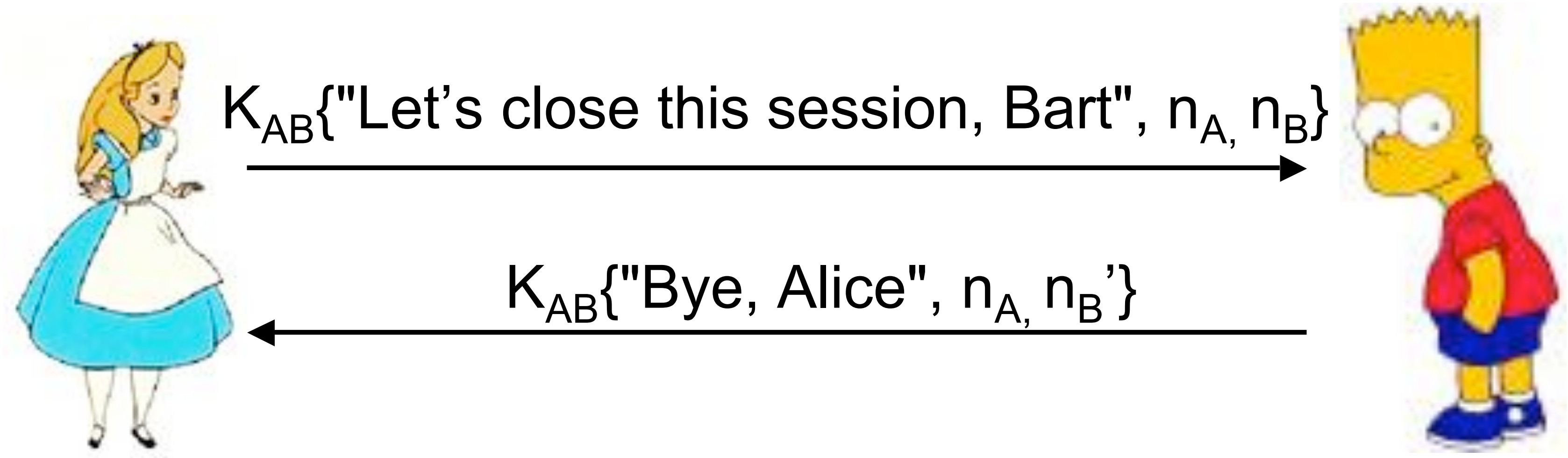
- Advanced cryptography & cryptographic protocols
  - Elliptic curves
  - Protocol analysis - logic and model checkers
  - Secret sharing, voting
- Systems security
  - Fault tolerance: replication, consensus algorithms

- Additional sources of information (research literature):
  - IEEE Symposium on Security & Privacy ("Oakland conference")
  - Usenix Security conference
  - ACM Conference on Computer and Communications Security
  - Computer Security Foundations Workshop
  - CRYPTO, EUROCRYPT

Final Exam

- Monday, May 12   Noon - 2:00pm   DRLB A6
- Will cover all the material in the course
  - But will emphasize the new material since Midterm 2
- Format will be similar to previous exams
  - T/F, multiple choice, short answer, short problems
  - The final will have a security analysis/synthesis question
- Send e-mail to make an appointment if you would like to meet with me

Thanks!



K_{AB}{"Let’s close this session, Bart", $n_{A,}$ n_B}

K_{AB}{"Bye, Alice", $n_{A,}$ n_B’}