Announcements

• Project 3 due TOMORROW
  – Updated web pages now have a UDP trace for testing
  – Unfortunately, no course staff available for last-minute help.

• Final exam:
  – May 5th.
  – 9:00 - 11:00 a.m.
  – Moore 216.
  – Cumulative, but concentrated on material since Midterm II.
Plan for today

• Wrap up digital cash (briefly)

• General course overview & conclusions
  – discussion

• Course evaluations
Digital Cash (1)

- Alice prepares 100 anonymous money orders for $1000 each. Each includes a different nonce.
- Alice puts all 100 anonymous money orders, and a piece of carbon paper, into 100 different envelopes. She sends all of them to the bank.
- The bank opens 99 envelopes and verifies that each is a money order for $1000.
- The bank signs the remaining unopened envelope and the signature is copied on to the money order. The bank hands the money order back to Alice and deducts $1000 from her account.
Digital Cash (2)

- Alice opens the envelope and sends the (signed) money order to the merchant.
- The merchant verifies the bank's signature to make sure the money order is legitimate.
- The merchant takes the money order to the bank.
- The bank also verifies the signature and checks a database to make sure that a previous money order with the same nonce has not been used. If it hasn't the bank credits $1000 to the merchant and records the nonce.
- If the nonce is present, the bank rejects the order.
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")
  - ACM Conference on Computer and Communications Security
  - Computer Security Foundations Workshop
  - CRYPTO, EUROCRYPT
Thanks!

\[ K_{AB}\{"Let’s close this session, Bart", n_A, n_B}\} \]

\[ K_{AB}\{"Bye, Alice", n_A, n_B’}\} \]