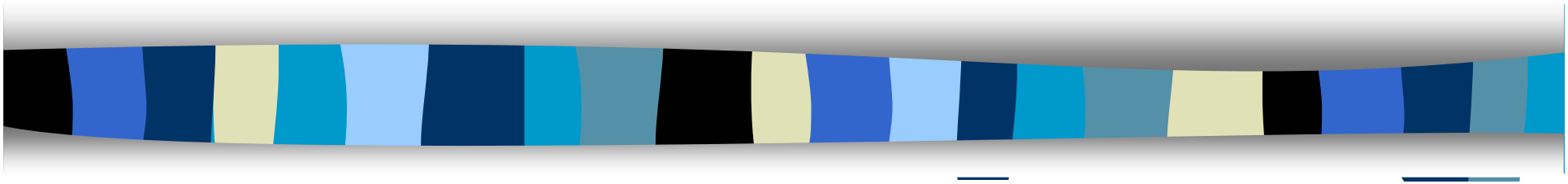
Computer Security
CS 426
Lecture 26



Review of Some Mid-Term Problems

One-Time Pad: Restating The Question

- One may argue that one-time pad cipher is completely useless for the following reason. As OTP requires the agreement of a key that is as long as the message, any channel that is used to send the key can also be used to send the message instead. Hence one does not need OTP encryption. Explain why this argument is incorrect by describing a scenario where one-time pad can still be useful.

Answers to the OTP Question

- Standard Answer: A secure channel can exist before messages exist.
- An interesting answer:
  - One can send message & key through multiple channels, assume that the adversary cannot eavesdrop all channels
  - Related to secret sharing: How to split a secret to be shared in multiple shares so that one needs all shares to recover the secret?

Other Answers to the OTP Question

- With an authentic, but insecure channel, two parties can agree on a secret key without sending it
  - Has integrity (authenticity), but not confidentiality
- Can then use OTP to send messages
- E.g.: Diffie-Hellman Key agreement Protocol:
  - See next slide
- Quantum communication provide another kind of channels suitable for sending keys but not messages: any eavesdropping will be detected

Key Agreement: Diffie-Hellman Protocol

- Key agreement protocol, A and B agree on K
- Setup: choose a prime p, and g in {2,…,p-1}, p and g public.

$g^a \bmod p$

$g^b \bmod p$

Pick random, secret a
Compute and send $g^a \bmod p$

$K = (g^b \bmod p)^a = g^{ab} \bmod p$

Pick random, secret b
Compute and send $g^b \bmod p$

$K = (g^a \bmod p)^b = g^{ab} \bmod p$

Semantic Security Question Restated

- We require secure ciphers to provide Semantic Security (Ciphertext indistinguishability), that is, if an adversary chooses two **equal-length** messages M_0 and M_1, and is given $E_K[M_b]$, where b is uniformaly randomly chosen from {0,1}, the adversary has little advantage in guessing b. Suppose that ECB mode is used, show how to choose M_0 and M_1 such that from the ciphertext $C=E_K[M_b]$, one can easily tell whether it is an encryption of M_0 or M_1.

Why Ciphertext Indistinguishability?

- Information Theoretical Security: Given C, each M is equally likely
  - Cannot achieve in practice
- Computational Security (attempt 1): Given C, cannot recover M
  - What is some information about M is recovered?
  - What if adv. has some knowledge about M already?
- Computational Security (attempt 2): Given C, cannot find any additional info about M, except its length.

How to Formalize Computational Security?

- Given C, suppose adv. knows it is the cihpertext of either M_0 or M_1, still cannot tell which one it is.
  - What if adv. can tell some pairs but not others?

- Have the adv choose M_0 or M_1, let C be ciphertext of one of them, still cannot tell which one it is.

- Note: The Adv sees only one ciphertext C

Answers to the Semantic Security Question

- Choose M_0 be B_1B_1 and M_1 be B_1B_2, where B_1 and B_2 are two different blocks.
  - If C has two repeated blocks, then it encrypts M_0, otherwise, it encrypts M_1
  - Any B_1 and B_2 would work, no need to be all 0's, or all 1's
- Incorrect answer:
  - Let M_0 be all 0's, and M_1 be all 1's.
  - Using a secure block cipher, one cannot tell

New ScareWare: Kenzero [BBC News, April 2010]

- A trojan spread through P2P file sharing
- Prompts you to a game installation window on your PC and asks for your personal information.
- Take browser's history, publishes online.
- Also, once found proof of illegally downloading files, sends an e-mail or another pop-up that threatens legal action if you don't pay (1500 Yen) $15 to "settle your violation of copyright law."
- Website Yomiuri claims that 5500 people have so far admitted to being infected.
- Also similar incident in Europe

Confused Deputy Problem

- How is confused deputy problem solved in UNIX?
  - Use the setuid family of system calls to
    - Drop root privilege when no longer needed.
    - Switch between two users ids
  - Require programmers to proactively use these while writing the programs.

No Confused Deputy Problem in Capability Systems

- Two masters each pass in their own capabilities (for file accesses) to the program
- A file access by the program must select a capability
  - The selection of a capability also selects the master
    - The master for each access is thus specified
  - No designation without authority
    - Cannot talk about an object w/o some authority over it

BLP Question: Possible Flows

- From one object to another of the same level
  - Legal
- Human users leaking information
  - Out of hand channel
- Use channels not intended for transmitting inf
  - Covert channels, not overt
- From low level object to high
  - Integrity concern, but legal wrt intend of BLP
- Read high file, close file, drop to low, and write
  - Satisfy BLP definition, illegal wrt intent