CSE 543 - Computer Security

Lecture 3 - Principles
September 12, 2006
URL: http://www.cse.psu.edu/~tjaeger/cse543-f06/
Data Encryption Standard (DES)

- Introduced by the US NBS (now NIST) in 1972
- Signaled the beginning of the modern area of cryptography
- Block cipher
  - Fixed sized input
- 8-byte input and a 8-byte key (56-bits+8 parity bits)
Cryptanalysis of DES

- DES has an effective 56-bit key length
  - Wiener: 1,000,000$ - 3.5 hours (never built)
  - July 17, 1998, the EFF DES Cracker, which was built for less than $250,000 < 3 days
  - January 19, 1999, Distributed.Net (w/EFF), 22 hours and 15 minutes (over many machines)
  - We all assume that NSA and agencies like it around the world can crack (recover key) DES in milliseconds

- What now? Give up on DES?
Variants of DES

- DESX (XOR with separate keys \(\sim 60\)-bits)
  - Linear cryptanalysis

- Triple DES (three keys \(\sim 112\)-bits)
  - keys \(k_1, k_2, k_3\)

\[
\text{c} = \text{E( D( E( p, k_1), k_2), k_3)}
\]
Advanced Encryption Standard (AES)

• Result of international NIST bakeoff between cryptographers
  – Intended as replacement for DES
  – Rijndael (pronounced “Rhine-dall”)  
  – Currently implemented in many devices and software, but not yet fully embraced
  – Cryptography community is actively vetting the the theory and implementations (stay tuned)
Public Key Cryptography

- Public Key cryptography
  - Each key pair consists of a public and private component: $k^+$ (public key), $k^-$ (private key)
    \[
    D( E(p, k^+), k^- ) = p \\
    D( E(p, k^-), k^+ ) = p
    \]

- Public keys are distributed (typically) through public key certificates
  - Anyone can communicate secretly with you if they have your certificate
  - E.g., SSL-base web commerce
A computing system is (more or less) a program running with external resources.

Memory and external storage are the only real resources.

Everything else is a variant of these.

In its native state (e.g., early OSes), utterly defenseless.
Protection System

Protection domain

- Memory
- Program A
- Files
Protection System

The protection domain restricts access of external parties to our computing system’s resources.

How is this done today?

- Memory protection
- E.g., UNIX protected memory, file-system permissions (rwx...)

Protection domain

Memory

Program A

Files
The confinement problem

Program A

Input

Output

Input'

Service B

Memory

Files
(a brief aside)

• Certification

• Some external body inspects the service and certifies that the program/object is “safe”, “secure”, “reliable”, …

• Whom do you trust to make such assertions?

• Are such assertions realistic even in good?
The confinement problem (cont.)

- Preventing information leakage is a very hard problem in general.
- There are many kinds of input …
- There are many, many ways to leak information …
Some reasonable questions

• What does this have to do with security?
• Given an example where confinement would be a desirable property?
Overt channels

• How does a program leak information to malicious parties?

• Example, Keylogger.Stawin
  • RE: I still love you
  • Virus that loads a keylogger onto your machine, then looks for online Banking information.
  • Then, downloads to foreign site (yikes!)

• Overt Channels
  • Email, HTTP, or any other network transport
  • Leave temporary or hidden files (invisible /dev entries)
  • IPC
• Total isolation
  
  • “… a confined program shall make no calls to any other program”
  
  • This is the trivial solution … if there is no externally observable behavior, then they can be no information transfer *by definition*
  
  • No output, no control transfer (e.g., no underlying OS)
  
  • Is this a reasonable model?
Transitivity

- OK, total isolation is not realistic. What about transitive confinement?
  - “If a confined program calls another program which is not trusted, the called program must be confined.”
  - In essence, it says that the confined program must trust the services it uses.
  - Trusted supervisor - how do we prevent leakage from the program controlling the environment.
  - These are “quite subtle and obscure”, but we can find them and plug them.

- What does confinement control?