COMP 3400 Mainframe Administration[1]

Christian Grothoff
christian@grothoff.org

http://grothoff.org/christian/

[1] These slides are based in part on materials provided by IBM's Academic Initiative.

Computer Security Overview

- Computer Security $\equiv$ protecting information
- **Protecting:** Integrity, confidentiality, authenticity, availability

  Information: Randomness, entropy, correlation, storage, transmission

Topics

- Cryptography and Protocols (theory)
- System Administration (practice)
- Privacy, Policies and Legal Aspects (politics)

Terminology (1/5)

- An adversary is a subject trying to break the security of a system
- A threat is a mechanism that the adversary can employ to achieve his goals
- A risk is a loss that would occur if the adversary succeeds
- A vulnerability is a flaw creating a threat
- A threat model describes the mechanisms available to the adversary
- A trust model describes subjects that are trusted not to have vulnerabilities
- A security model specifies functional and security goals together with threat and trust models

Terminology (2/5)

- Plaintext: P
- Ciphertext: C
- Encryption: $E_K(P) = C$
- Decryption: $D_K(C) = P$
- Cryptography $+$ Cryptanalysis $=$ Cryptology
- Steganography

Terminology (3/5)

- Authentication: receiver ascertains origin of message
- Integrity: verify message was not modified in transit
- Nonrepudiation: sender cannot deny sending message

Terminology (4/5)

- Cipher $= (E, D)$
- restricted algorithm $\equiv$ security based on secrecy of algorithm
- modern algorithm $\equiv$ security based on secrecy of key K

Terminology (5/5)

Attacker limitations:

- Data complexity (how much data required as input to the attack)
- Processing complexity (how much processing is needed)
- Storage requirements (how much memory is needed)

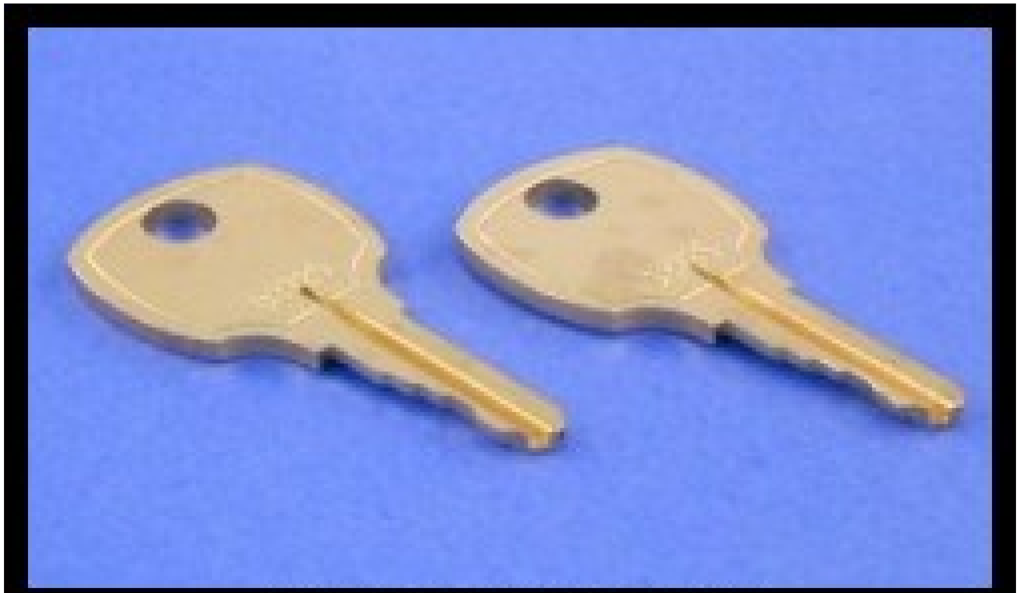
Kerckhoff's principle (1883)

The only thing the adversary does not know is the secret key.

The design of encyrption and decryption algorithms and the protocol is public:

- Allows public scrutiny of the design
- No need to replace system if design is exposed
- Same design can be used for multiple applications
- Focus on security the key!

Secure Voting, US-style



KEYS TO THE KINGDOM
Photo taken from Diebold's online store. The keys that open every Diebold touch-screen voting machine. Working copies have been made from the photo.

Defeating the Evildoers

CERT:

1. Install and Use Anti-Virus Programs
2. Keep Your System Patched
3. Use Care When Reading Email with Attachments
4. Install and Use a Firewall Program
5. Make Backups of Important Files and Folders
6. Use Strong Passwords
7. Use Care When Downloading and Installing Programs
8. Install and Use a Hardware Firewall
9. Install and Use a File Encryption Program and Access Controls

CRISP:

1. Use UNIX-based systems and avoid being `root`
2. Frequently update your software, it is free
3. Refuse to use Microsoft products and document formats
4. Be aware what services you run (`netstat -ntpl`)
5. Use version control for important files
6. Use strong passwords where necessary
7. Avoid using non-free software
8. Do not buy random security equipment
9. Use cryptography appropriately
10. Think. Sometimes, wear black hats.

Review: UNIX File Permissions

- Standard permissions: Read (4), Write (2), eXecute (1)
- Differentiation by: User, Group, Others
- `man chmod`, `man chown`
- Default permissions are $arg\&\ mask$ where `arg` is specified by the application. For `mask`, see `man umask`

Process User Identifiers

- Each process is associated with multiple user IDs: real, effective, saved and possibly others
- Real UID is the UID of the process that created this process. Can only be changed if effective UID is root (0).
- Effective UID is used for permission checks; EUID can be changed to real UID or to saved UID. If EUID is 0, anything goes.
- New files are created using the effective UID

SUID, SGID

- If permissions of executable file are set to SUID, SUID of executed process will be set to UID of the file's owner.
- This allows the program to switch to those permissions using `seteuid(SUID)`
- Processes also have multiple group IDs, the same rules apply.
- Binaries with SUID and SGID can be used to elevate permissions

TCP/IP Security: Terminology

- Stateless Firewall
- Statefull Firewall
- DMZ
- VPN

z/OS Security

- SAF / RACF: Authorization, Authentication, Logging, Tracing
- IPSec (VPN): Encryption, Authentication
- TLS (SSL): Encryption, Authentication

SNA Security

- "Security by Obscurity"
- Subarea: LU authentication, hardware based keys
- APPN: Authentication and Encryption
- EE: IP-based security
- TN3270: SAF/RACF (authentication, application restriction); TLS supported

System Authorization Facility (SAF)

- Part of z/OS
- Central component responsible for security
- Interfaces with security manager for authentication, authorization and logging
- **Control points** are decision-making functions in resource managing components
- SAF “routes” requests from “control points” to the security manager

Resource Access Control Facility (RACF)

- Most important component of IBM's implementation of a security manager
- User with the SPECIAL attribute is the security administrator
- Security manager has other important components, such as the RACF Remote Sharing Facility (RRSF)

RACF Features

- Identify and authenticate users
- Authorize users to access protected resources
- Log and report attempts of unauthorized access
- Control the means of access to resources (i.e., restrict to certain terminals, IP addresses or times of day)

RACF Access Protections for Data Sets

NONE No access at all

READ Reading only (including creating copies and printing)

UPDATE Reading and writing, but no deletion, renaming or moving

ALTER Read, update, delete, rename and move allowed

EXECUTE User can execute (but not read or copy) load modules in the library

Other Access Protection Functions

- Notify: if access is denied, notify a given user
- Erase-on-scratch: when the data set is deleted, overwrite all allocated extents with zeros
- Warn: allow unauthorized users access, but warn them

Setting Permissions

1. Create a profile, default permissions “NONE”:

```
ADDSD ’dataset-name’ UACC(NONE)
```

2. Set permissions for a user:

```
PERMIT ’dataset-name’ ID(USERNAME)
       ACCESS(READ)
```

Inspecting Permissions

```
LISTDSD DATASET ('dataset-name') ALL
```

For more information on RACF, read the **z/OS Security Server RACF General User's Guide** (SA22-7685-01).

Authorized Programs (APF)

- Similar to SUID on UNIX: allowed to perform supervisor calls (SVCs)
- Except also treated as extension to the kernel – more like a kernel module
- Program Status Word (PSW) must have particular values (to indicate supervisor mode)
- APF-authorized programs must reside in authorized libraries
- SYS1.LINKLIB, SYS1.SVCLIB and SYS1.LPALIB are by default authorized libraries

Storage Protection

- Address spaces isolate programs
- Page protection bit can be used to prevent z/OS and APFs from writing to pages

⇒ Used for LPA pages shared across address spaces

- Subsystems also use cross-memory communication to share memory across address spaces
- The **program call** (PC) instruction can be used to call a program in another address space

z/VM Security

- Integrates with RACF and other external security managers
- Used for authentication and access control (to memory pools, disks, networks (VLANs), terminals)
- Alternative: z/VM directory (build-in) instead of RACF or IBM DirMaint

z/VM Priviledge Classes

A	System Operator: accounting, availability, performance
B	System Resource Operator: controls (most) physical resources
C	System Programmer: Changes system-wide parameters
D	Spooling Operator: Controls spool files, readers, printers and punch equipment
E	System Analyst: examines system operation data
F	Service Representative: examines I/O operation data
G	General User
Any	Available to any user
H	Reserved for IBM use
I-Z, 1-6	Defined through user class restructure (UCR) by each installation

Cryptgographic Facilities

z/VM can provide guests with access to cryptographic co-processors (CP Assist for Cryptographic Function):

- DES
- AES
- SHA-1
- SHA-256
- Modular arithmetic (for RSA, DH)

CP USER DIRECT

- The z/VM directory (USER DIRECT) is a flat file used to manage definitions of users
- CP can not directly read the flat file, DIRECTXA is used to make it accessible to CP
- User MAINT is responsible for maintaining the directory

Updating USER DIRECT

- Log on as user MAINT
- Edit USER DIRECT with XEDIT
- Run DISKMAP to check for overlapping disk allocations
- View USER DISKMAP to see if overlaps are acceptable
- Run `DIRECTXA USER DIRECT` to make the new directory available to z/VM

z/VM User Directory: Example

```
USER LINUX01 MYPASS 512M 1024M G
MACHINE ESA 2
IPL 190 PARM AUTOCR
CONSOLE 01F 3270 A
SPOOL 00C 2540 READER *
SPOOL 00D 2540 PUNCH A
SPECIAL 500 QDIO 3 SYSTEM MYLAN
LINK MAINT 190 190 RR
MDISK 191 3390 012 001 ONEBIT MW
MDISK 200 3390 050 100 TWOBIT MR
```

Questions

?