

Hardware

CSH5 Chapter 4

“Hardware Elements of Security”

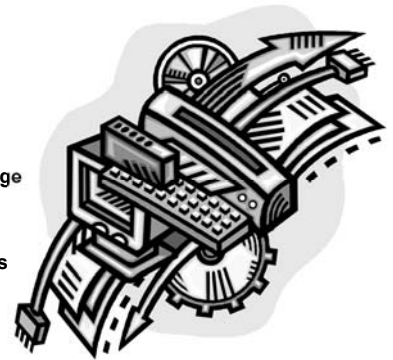
Sy Bosworth & Stephen Cobb

1

Copyright © 2011 M. E. Kabay. All rights reserved.

Topics

- Introduction
- Binary Design
- Parity
- Hardware Operations
- Interrupts
- Memory & Data Storage
- Time
- Natural Dangers
- Data Communications
- Cryptography
- Backup
- Recovery
- Microcomputers



2

Copyright © 2011 M. E. Kabay. All rights reserved.

Introduction

Other hardware-related chapters of CSH5:

- Ch 5 – Data Communications & Information Security
- Ch 6 – Network Topologies, Protocols, & Design
- Ch 22 – Physical Threats to the Information Infrastructure
- Ch 23 – Protecting the Information Infrastructure

3

Copyright © 2011 M. E. Kabay. All rights reserved.

Binary Design

- Von Neumann Architecture
 - ❑ John von Neumann, 1946
 - ❑ Apply binary representation to computer implementation
 - ❑ Electrical/electronic systems could handle high/low or on/off states to represent binary 0 and binary 1
 - ❑ Rapid switching = pulses
- Pulse characteristics
 - ❑ Ideally square waves
 - ❑ But cope with sine waves and other waveforms

4

Copyright © 2011 M. E. Kabay. All rights reserved.

Circuitry

- Original 1940s computers used vacuum tubes
 - ❑ Relatively large – room-sized machines with power of later calculator-wristwatches
 - ❑ Consumed power & ran hot
 - ❑ Short MTBF (mean time between failures)
- Solid-state transistors
 - ❑ Patented in 1925 (Lilienfeld) & 1934 (Heil) but never developed
 - ❑ William Shockley & colleagues at Bell Labs developed effective transistors starting in 1947



5

Copyright © 2011 M. E. Kabay. All rights reserved.

Coding

- Convention for representing data
- Early codes include
 - ❑ Baudot (hence “baud rate”)
 - ❑ Binary-coded decimal (BCD)
 - ❑ Extended BDC (EBCDIC, used by IBM)
 - ❑ American Standard Code for Information Interchange (ASCII)
- Bits → bytes (8 bits/byte) → words (n bytes/word)
- Prefixes for length of numerical codes (B = bytes & b = bits)
 - ❑ KB = kilobyte (1024 bytes) (aka kibibyte!)
 - ❑ MB = megabyte (1024 KB) (aka mebibyte)
 - ❑ GB = gigabyte (1024 MB) (aka gibibyte)
 - ❑ TB = terabyte (1024 GB) (aka tebibyte)



6

Copyright © 2011 M. E. Kabay. All rights reserved.

Error-Detecting Codes

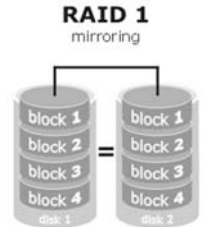
- Error-detection systems started with parity bits
- Write additional bit into hardware storage (e.g., disk, RAM, data-comm, tape...)
 - Even parity bit = 0 when sum of bits is even
 - Odd parity bit = 0 when sum of bits is odd
 - Recompute parity bit when reading data back
 - Check to see if computed parity bit = recorded parity bit
- Extensions led to error-correcting codes; e.g.,
 - Cyclical Redundancy Checks (CRCs)
 - Self-checking codes



Copyright © 2011 M. E. Kabay. All rights reserved.

Hardware Operations

- Fundamentals ops: Input, Output, Processing
- Typical hardware-implemented error-handling
 - Read-after write
 - Echo
 - Overflow errors
 - Validation
 - Replication (e.g., RAID-1 arrays of disks)



Copyright © 2011 M. E. Kabay. All rights reserved.

Interrupts

- Changes of state can allow operating system to examine its own integrity as well as integrity of data
- Types of interrupts
 - I/O
 - Supervisor calls
 - Program check
 - Machine check
 - External



For a detailed computer engineering review, see "Investigating Interrupts" by Garth Wilson <http://tinyurl.com/42dqcu> (← q not g)

Copyright © 2011 M. E. Kabay. All rights reserved.

Memory & Data Storage

Memory Hierarchy (of speed)

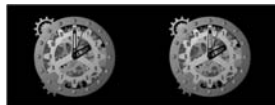
- CPU registers (architectural registers)
 - Nanosecond access time
- Main memory (primary memory, RAM)
 - Microsecond access time
- Secondary storage (disk, tape, flash memory ...)
 - Millisecond access time – on disks, mostly due to head positioning
- Hardware safeguards
 - Hardware-locking devices can prevent accidental write
 - Bad-sector compensation
 - Reformatting
 - SMART (Self-Monitoring, Analysis, and Reporting Technology)
 - Head-withdrawal systems for hard-drives



Copyright © 2011 M. E. Kabay. All rights reserved.

Time

- Synchronous processes
 - Operate according to strict rhythm
 - ✓ Intrinsic frequency of hardware
 - ✓ System clock cycles
 - ✓ Defined # cycles= tick
 - ✓ Defined # ticks may generate interrupt
 - Deviation from clock cycle may indicate error
- Asynchronous processes
 - No particular rhythm
 - E.g., keyboard inputs, packet streams



Copyright © 2011 M. E. Kabay. All rights reserved.

Natural Dangers

- Power failure
- Heat
- Humidity
- Water
- Dirt, dust
- Radiation

May cause downtime



See CSH5 Chapters 22 & 23

Copyright © 2011 M. E. Kabay. All rights reserved.

Data Communications

- DC hardware can be critical
- Terminals must be protected to prevent unauthorized access
- Wired facilities
 - ❑ Dial-up lines (increasingly rare)
 - ❑ Leased lines
 - ❑ DSL (Digital Subscriber Lines)
 - ❑ Cable
- Wireless



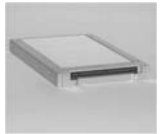
See CSH5 Chapter 5

13

Copyright © 2011 M. E. Kabay. All rights reserved.

Cryptography

- Essential tool for information assurance
- Increasingly available in hardware implementations
 - ❑ Encrypting disk drives
 - ❑ Encrypting data-communications equipment (e.g., STU-III)



ROCSAFE



Secure Telephone Unit III

See CSH5 Chapter 7

ROCSAFE
<http://tinyurl.com/qw36aa>

14

Copyright © 2011 M. E. Kabay. All rights reserved.

Backup

- All systems may fail
- Therefore all systems storing meaningful data should be *backed up*
- Definition: backup is *independent copy of data*
 - ❑ Thus must have *at least 2 instantiations* of data
 - ❑ Thus cannot backup and then destroy original: would have no backup
- Backup also includes operational components for business continuity
 - ❑ People
 - ❑ Hardware
 - ❑ Power

See CSH5 Chapter 57

See CSH5 Chapter 58

15

Copyright © 2011 M. E. Kabay. All rights reserved.

Recovery

- Effective recovery requires planning & testing
- Backups
 - ❑ Test backups at time of creation
 - ✓ Use verification mode
 - ✓ Reads data back and compares with original
 - ❑ Test backup restoration periodically
 - ❑ Keep in mind that backup media may deteriorate over time
 - ✓ Archives may become unreadable
 - ✓ Plan for re-recording if necessary

See CSH5 Chapters 58 & 59

16

Copyright © 2011 M. E. Kabay. All rights reserved.

Microcomputers

- General threats to microcomputers
 - ❑ Small size
 - ❑ Ease of access (e.g., laptops)
 - ❑ Widespread knowledge
 - ❑ Strong motivation to steal information
 - ❑ Lots of opportunity
- Specific threats *See also following slides*
 - ❑ Physical damage
 - ❑ Theft
 - ❑ Bad electrical power & static discharge
 - ❑ Data communications
 - ❑ Maintenance and repair



17

Copyright © 2011 M. E. Kabay. All rights reserved.

Physical Damage

- Susceptibility to shock
 - ❑ Disk drives in particular
- Damage from liquids and grease
 - ❑ Spilled beverages into keyboards
 - ❑ Dirty fingers on connectors
- Obstructed cooling vents
 - ❑ Dirt
 - ❑ Blockage by papers, books, other equipment



18

Copyright © 2011 M. E. Kabay. All rights reserved.

Theft

- Theft of laptops → loss of control over confidential data
 - ❑ Confidential data *must* be encrypted
 - ❑ Personally identifiable information (PII) in particular must be encrypted
 - ❑ Use whole-disk encryption for simplicity
- Computer lo-jack systems available



Bad Electrical Power & Static Discharge

- Reduce or eliminate use of multiple-access to power outlets
- Add voltage-regulators
 - ❑ Prevent spikes and brownouts
 - ❑ Many UPSs include voltage regulation
- Don't allow vacuum cleaners (etc) on same circuit as computer systems



See Kabay (2009) "Preparing for the Next Solar Max" <http://www.mekabay.com/infosecmgmt/solarmax.pdf>

Data Communications

- Explosion of interconnectivity
 - ❑ <1980 almost all computer networks were local
 - ✓ Simple terminals hardwired to mainframes
 - ✓ Smart terminals with some local processing
 - ❑ In 1980s LANs interconnected PCs locally
 - ✓ WANs and MANs implemented internetworking
 - ✓ Internet grew to 1.1M nodes by 1991
 - ❑ 1990s saw explosion in size of Internet
 - ✓ .com TLD (top-level domain) opened ~1993
 - ✓ WWW established early 1990s

Maintenance and Repair

- Organizations must establish official program of maintenance and repair for PCs
 - ❑ On-site by employees
 - ❑ On-site by contractors
 - ❑ On-call repair
 - ❑ Carry-in service to repair centers
 - ❑ Remote repair using shipping
- Have loaners on standby for immediate replacement of damaged units

Consider security implications

DISCUSSION