

# CS574

# Computer Security

San Diego State University

Spring 2008

Lecture #2

# Today's Structure

- Administrivia
- Questions
- Recent News
- Lectures
- Crashers

# Administrivia

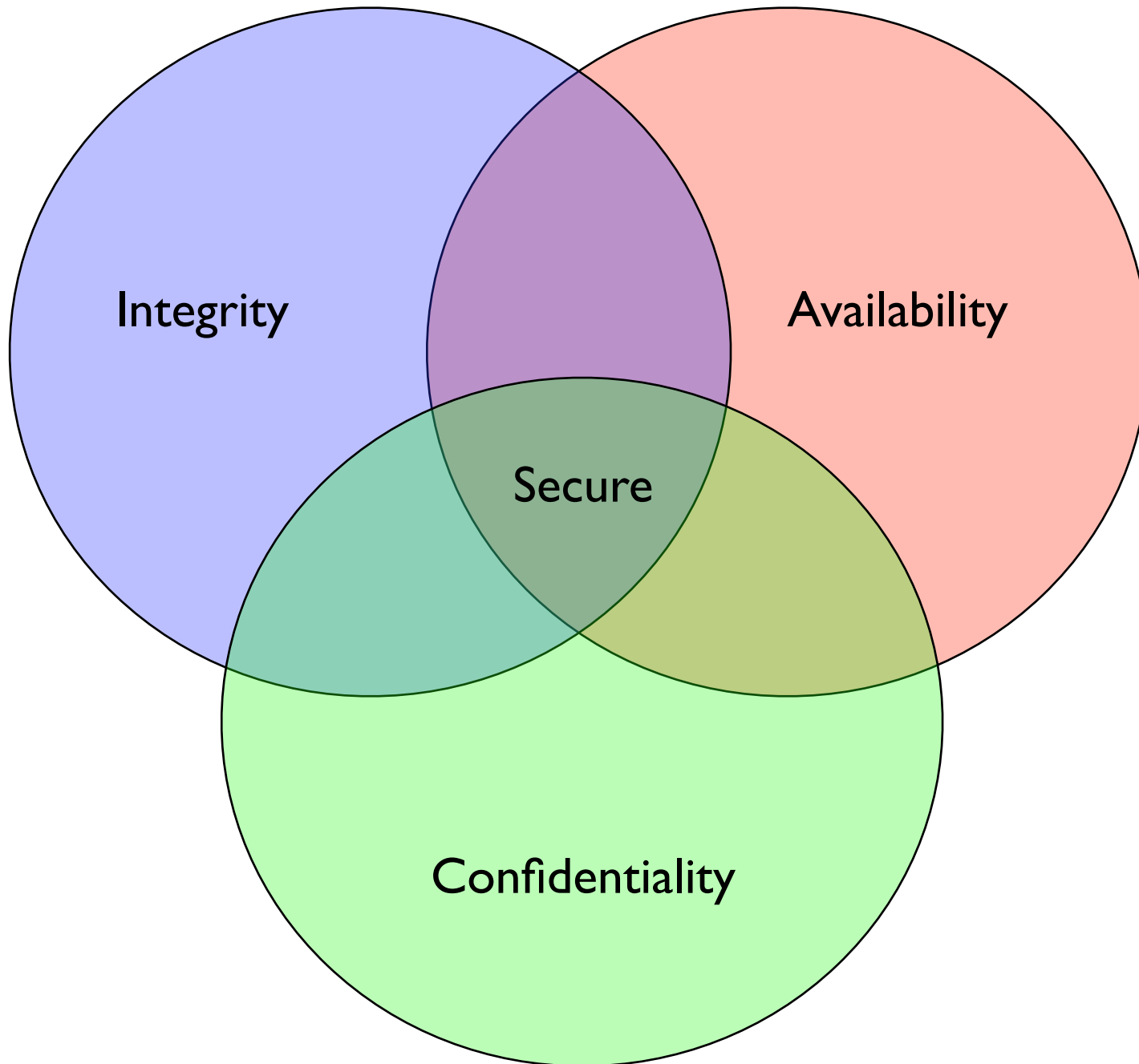
- Crashing
  - Seats Free
  - Crash List
  - Transcripts
- Roll

**Questions?**

# Recent News

- Drive-by Pharming
- Compromised Servers
- Banking Fraud
- *Government involvement*
- *others?*

# Lecture



# Physical Threats: Disasters

- Fire & Fire Suppression
- Floods
- Power Disruption
- Temperature
- Storms

# Physical Threats: Vandals

- Targets - hardware / media / people
- Theft
- Destruction

# Physical Threats: Unauthorized Access

- Isolated Terminals
- Kiosks
- Taps
- Dumpster Diving
- Piggy-Backing

# Controls: Contingency Planning

- Something *will* go wrong:  
Murphy's Law / Finagle's First Law
- Plan ahead to minimize surprise
- Avoid solving only the last problem

# Controls:

# Backups

- Assumption is that it's the data that's important; machines are basically all the same
- Types: Full, Differential, Incremental, Specific
- Schedule: Daily, Weekly, Monthly, Yearly, ad-hoc
- Retention Period & Location
- Indexing
- Media Types

# Controls: Recovery Sites

- Assumption is that it's the data and access that's important, not hardware or location
- Hot sites
- Cold sites

# Controls: Disposal

- Original and working documents
- Old media
- Old machines

# Controls: Access

- Locks
- Badges
- Guards
- Landscape
- Monitors & Motion Detectors

# Controls: EMSEC

- Emanation Security
- The problem
- A concern since the 1960s
- Details mostly classified

# EMSEC

- EMSEC - *Emanation Security*
- TEMPEST - *Interception of information via RF emissions*
- HIJACK - *Interception of information via contaminated electrical signal*
- NONSTOP - *Interception of information via (accidentally) modulated RF carrier*

# EMSEC

## Video Monitoring

- CRTs
- LCDs
- Direct Observation
- Indirect Observation

# EMSEC

## Other Monitoring

- Keyboards
- Printers
- Power Consumption
- LEDs

# EMSEC Controls

- Shielding equipment
- Shielding environment
- Adding Noise
- “Soft Tempest”

# Lecture References

- Pfleeger, *Security in Computers*, 3rd & 4th edition
- Various documents, <http://www.infosyssec.org/> (defunct?, accessed September 2005)
- Kuhn, M.G., “Compromising emanations: eavesdropping risks of computer displays”
- Kuhn, M.G. & Anderson, R. J., “Soft Tempest: Hidden Data Transmission Using Electromagnetic Emanations”
- Anderson, R.J. & Kuhn, M.G., “Soft Tempest - An Opportunity for NATO”
- The Complete, Unofficial TEMPEST Information Page,  
<http://www.eskimo.com/~joelm/tempest.html> (still available, January 2008)
- Grady Ward, “TEMPEST in a Teapot”, cypherpunks list  
(still available January 2008 at <http://cypherpunks.venona.com/date/1993/03/msg00492.html>)

**End Lecture**

# Reading

(For the next few classes)

- Pfleeger, Chapter 2
- Pfleeger, Chapter 12
- Snake-Oil FAQ

<http://www.interhack.net/people/cmcurtin/snake-oil-faq.html>

**Finis**