# Cyber Lessons, Learned and Unlearned

Eugene H. Spafford
spaf@purdue.edu

PURDUE UNIVERSITY

CERIAS

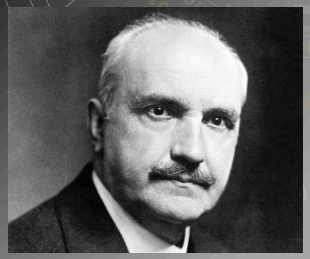
## All these threats & problems

We haven't seen these attacks before. Who could have defended against them?

- Wide-scale ransomware
- Massive supply chain attacks
- APT
- IoT attacks

"Those who cannot remember the past are condemned to repeat it"

– George Santayana, as stated in his work, The Life of Reason





## Cybersecurity isn't new

- The Ware Report — 1967
- Project MULTICS — 1969
- The Anderson Report — 1970
- Trusted Computer System Evaluation Criteria (Orange Book) — 1983

## What We Learned

- Software is fallible — need hardware support
- Need strong control over access
- Divide privilege

- Fast but bad security is still bad security!!



## However…

- Commercial interests ignored (or never learned) the lessons of security.

- Why? It sells more systems to put in weak or no protections.
- As a result, we are stuck with poor designs with weak features.

# Additionally…

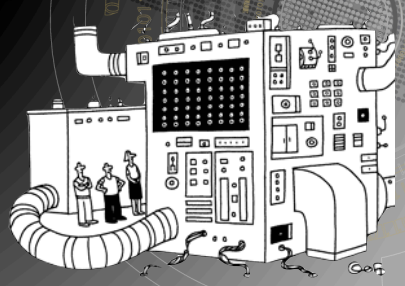
- Correctness means it does what we specify it will do
- Security is that it will do no more than what we specify
- But we gave up on specifying software (generally) decades ago!



# A Consequence of "Design"

***A program that has not been specified cannot be incorrect; it can only be surprising.***

Proving a Computer System Secure, W. D. Young, W.E. Boebert and R.Y. Kain, The Scientific Honeyweller (July, 1985), vol. 6, no. 2, pp. 18-27.



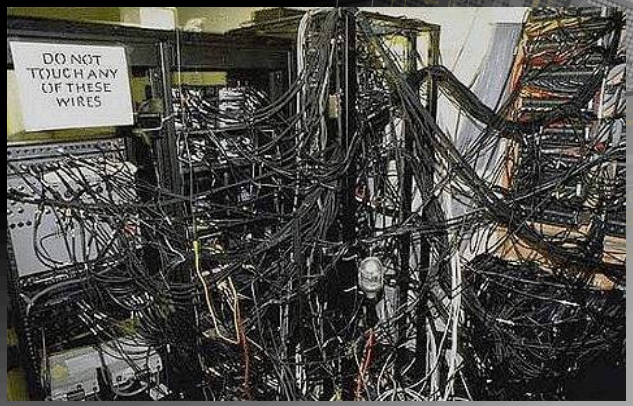
"It was just going to be a laser printer before we started adding features."

# Complexity & Design

- We can't define and design software well enough
- Complexity is killing us
- Legacy is a huge part of the problem
- We are stuck in a loop, fixing broken things that are fundamentally unsound
- Leads us to avoid investigating fundamental issues



# Metaphor for Current Software



# Richard Danzig

- Ptolemaic view of computing — we continue to patch systems—it works
- Copernican view is not appreciated because it costs money…and may not serve government interests
- However, current system is losing in facing future. Inside the OODA loop (John Boyd)



# Codified by Saltzer & Schroeder

- Economy of mechanism
- Fail-safe defaults
- Complete mediation
- Open design
- Separation of privilege
- Least privilege
- Least common mechanism
- Psychological acceptability

*The Protection of Information in Computer Systems, 1973*
*ACM SOSP*

# Think about these

- Economy of mechanism
- Fail-safe defaults
- Complete mediation
- Open design
- Separation of privilege
- Least privilege
- Least common mechanism
- Psychological acceptability

Does any system in common use adhere to these?

Windows?
Linux?
Android?



# Least Common Mechanism

- Windows registry?
- Shared libraries?
- Supply chain (SolarWinds) attacks?
- Web servers with DB, language interpreters, and animation built in?

## Complete Mediation

- Never done in standard systems… that is why “Zero Trust” is now a meme.
- Part of why supply chain attacks work



## Least Privilege

- Admin or super user is an “all-in” set of privileges.
- SE Linux is a worked example of reduced privileges — why isn’t it more widely used?

## And so on….

- Commercial interests ignored (or never learned) the lessons of security.
- Why? It sells more systems to put in weak or no protections.
- As a result, we are stuck with poor designs with weak features.



## Additional observation

- Without computers, we would have no cyber abuse.
- And without people, we would have no cyber abuse.
- Thus, focusing on the technology is only part of the solution.
- We need to change the way we look at the field.

# Cyber Security Should Include

- Psychology
- Human factors
- Economics
- Education
- Risk management
- Organizational management
- Criminology
- Computer architecture
- Physical plant protection
- Disaster recovery/ continuity
- … and more

(This is how we approach it at CERIAS)



# So, what next?

- More extortion-ware. Imagine “smart city” or national critical infrastructure extortion
- Because we do not provide fully mediated access and appropriate separation of privilege

## Coming

- More ICS, OT/IT threats because these are being built to be fast and cheap, not secure

– Complete mediation, separation of privilege, least common mechanism, failsafe defaults — all largely ignored.



## Coming

- More attacks on supply chains

– Least privilege, complete mediation

## Coming

- Attacks against cloud services and providers, including DDOS

– Least common mechanism, complete mediation, fail safe defaults



Security should not be “No, you can’t do that.”

It should be “Let me show you how to do that safely.”

## We Need To Value Security

1. Instead of cheapest, build better
2. Ignore compatibility unless strictly needed
3. Pay attention to known good practice
4. Build solutions that work well for specific purposes, rather than systems okay for many



*Thank you!*