Metaphorical Cybersecurity and Building Codes

Carl Landwehr
GREPSEC
May19, 2013

But first…

Federal labs as another employment option

Keep up relationships – you will meet people over and over
    Professional contacts outside your organization can help a lot

Respect your own work

Enemies are a luxury

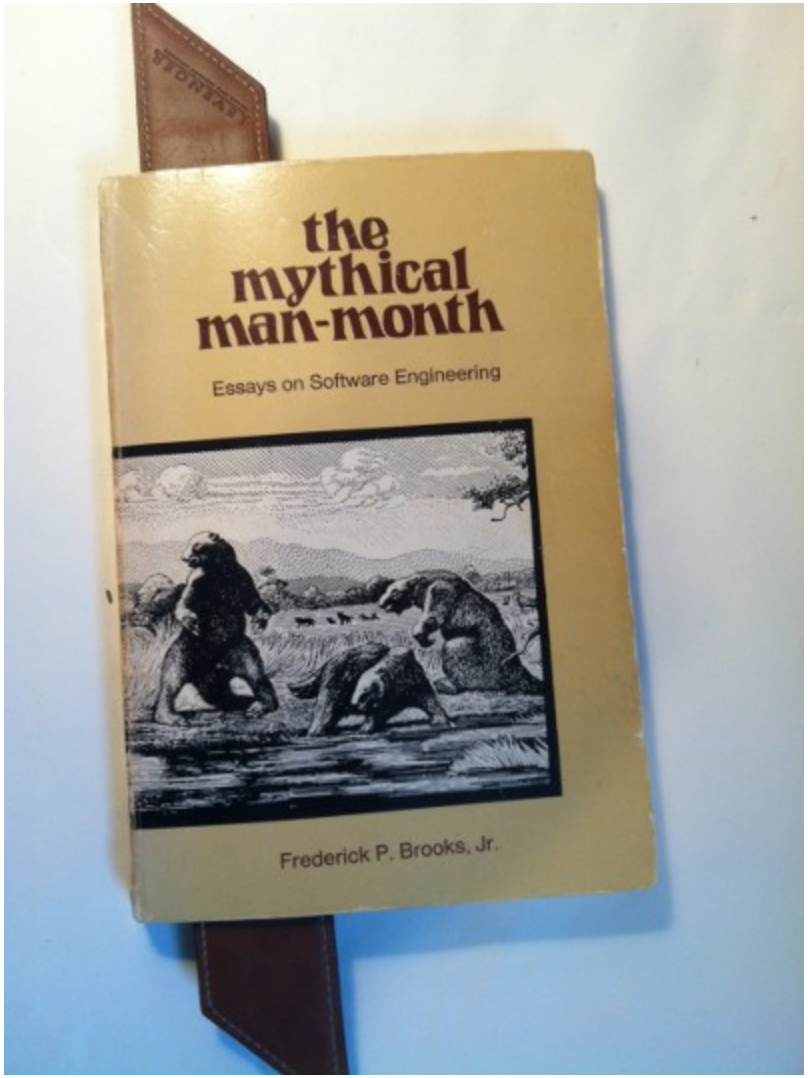
Today’s Reading

F. P. Brooks, The Mythical Man-Month, Addison Wesley, 1975, p.7

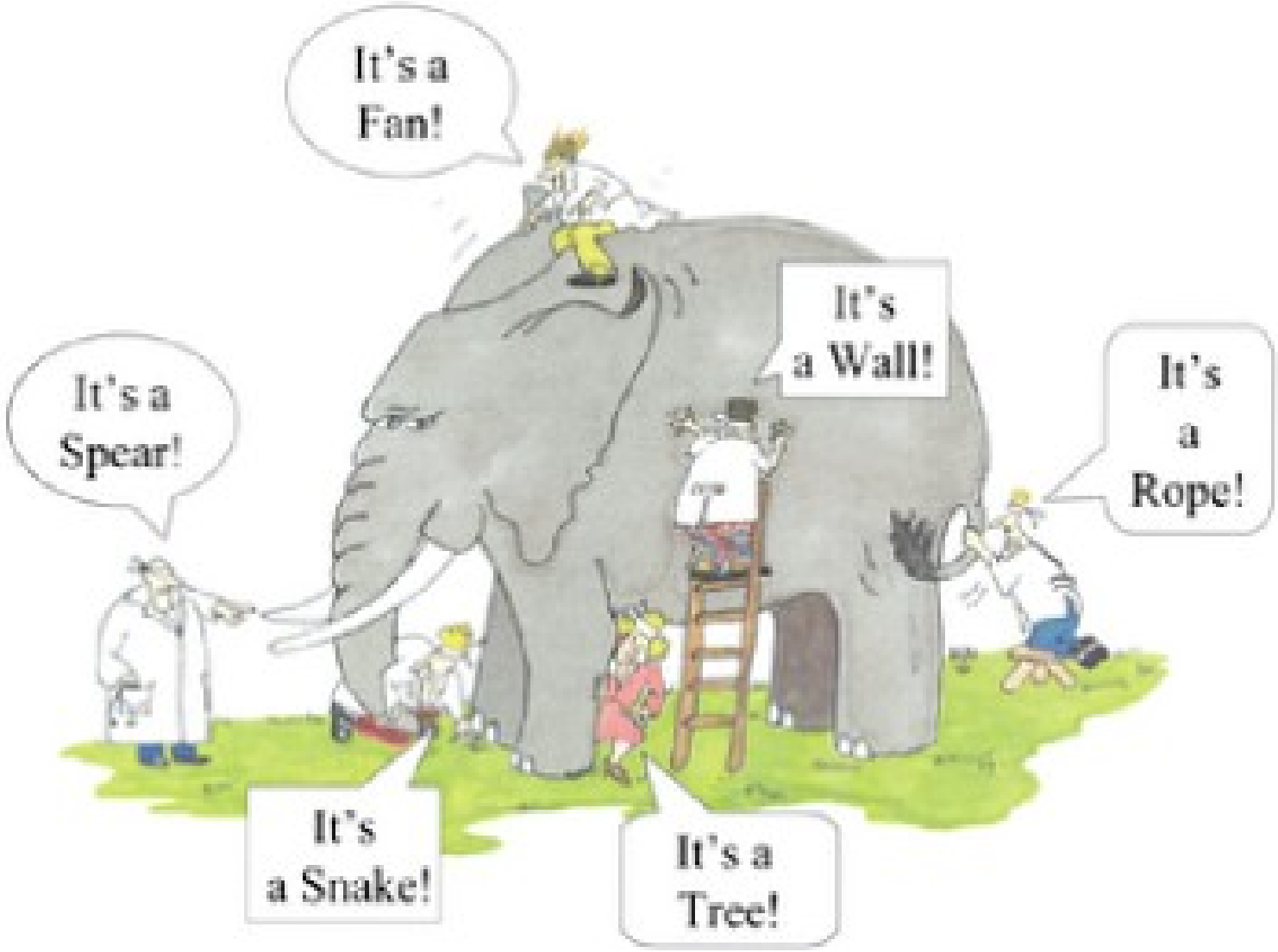
"... The programmer, like the poet, works only slightly removed from pure thought-stuff. he builds his castles in the air from air, creating by exertion of the imagination. Few media of creation are so flexible, so easy to polish and rework, so readily capable of realizing grand conceptual structures. ...

"Yet the program construct, unlike the poet's words, is real in the sense that it moves and works, producing visible outputs separate from the construct itself. It prints results, draws pictures, produces sounds, moves arms. The magic of myth and legend has come true in our time. One types the correct incantation on a keyboard, and a display screen comes to life, showing things that never were nor could be.

"Programming then is fun because it gratifies creative longings built deep within us and delights sensibilities we have in common with all.”



Metaphor

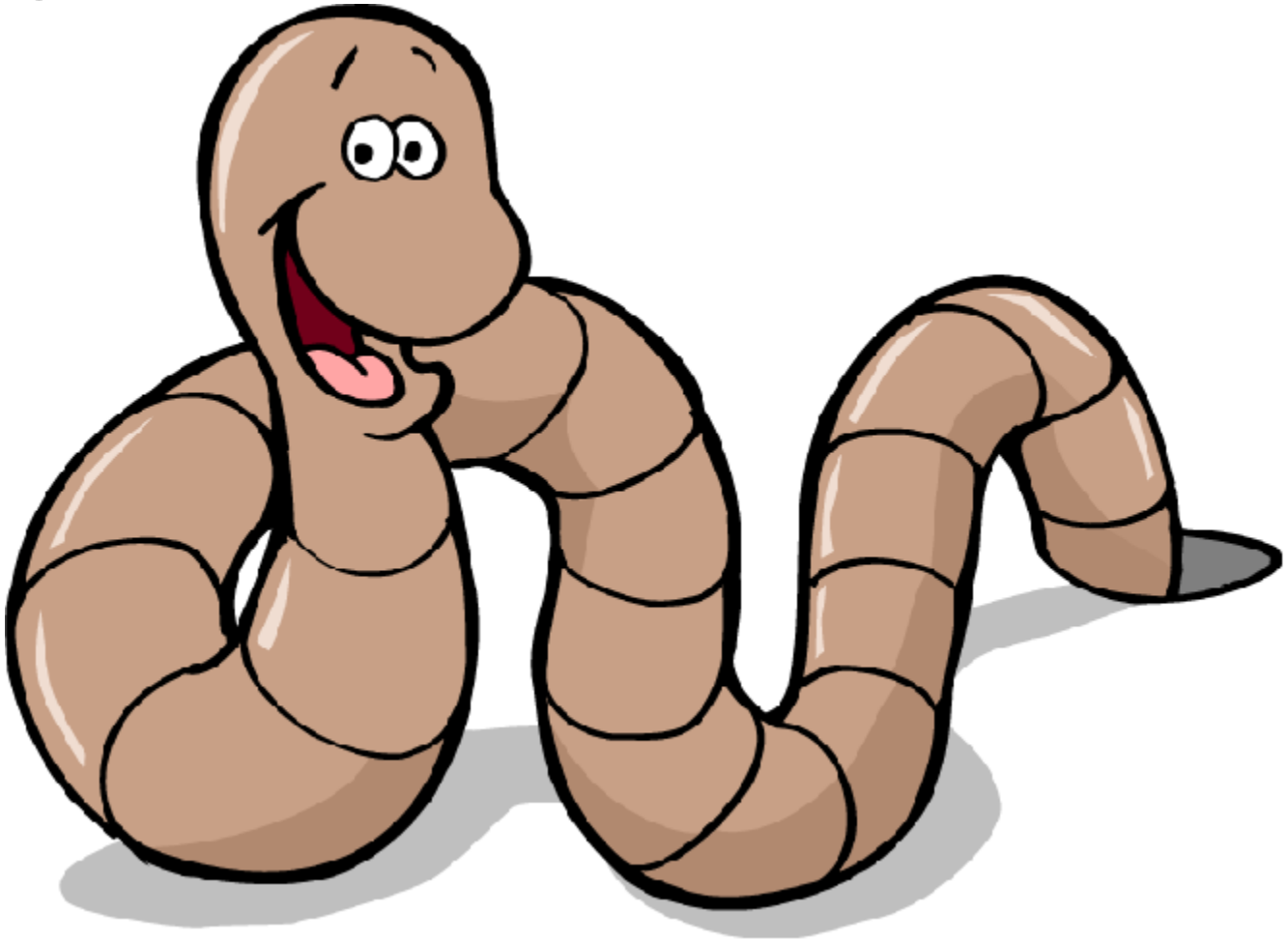


What makes a good metaphor?

Source domain target domain
Source domain (at least) widely understood
Captures an essential aspect of the target
Hides irrelevant/uninteresting detail
Reasoning in the source domain carries over reasonably well to the target domain, i.e., the mapping preserves essential functions

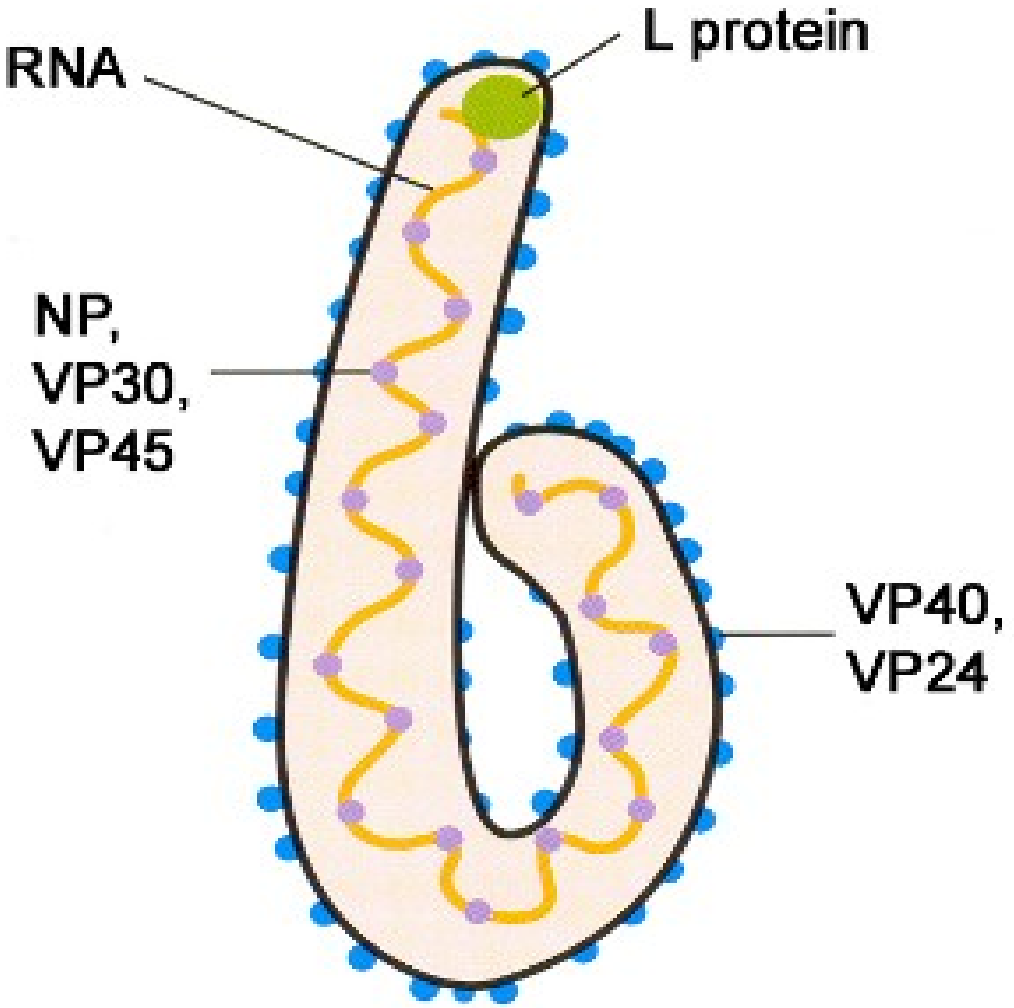
Trojan Horse

Worm



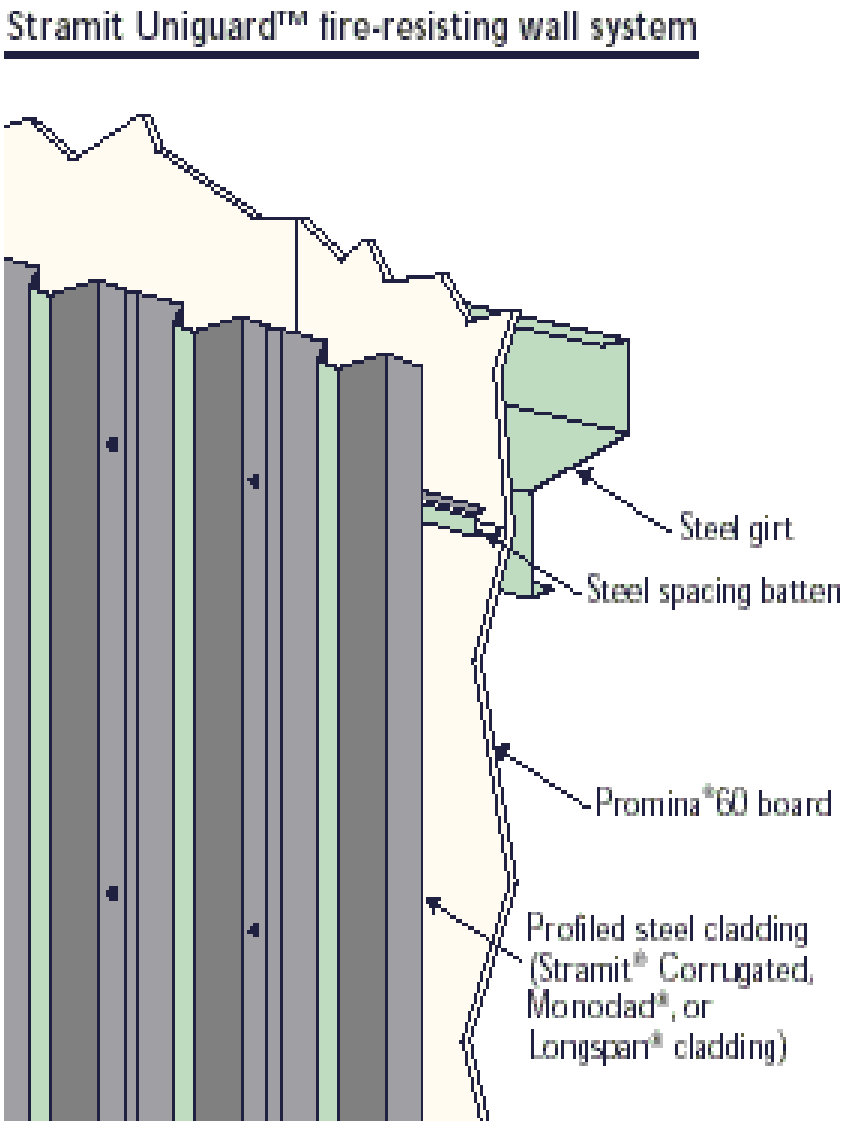
http://www.paratiritis-news.com/wp-content/uploads/2012/02/worm.gif

Virus



http://www.primehealthchannel.com/wp-content/uploads/2011/01/Ebola-Virus.gif

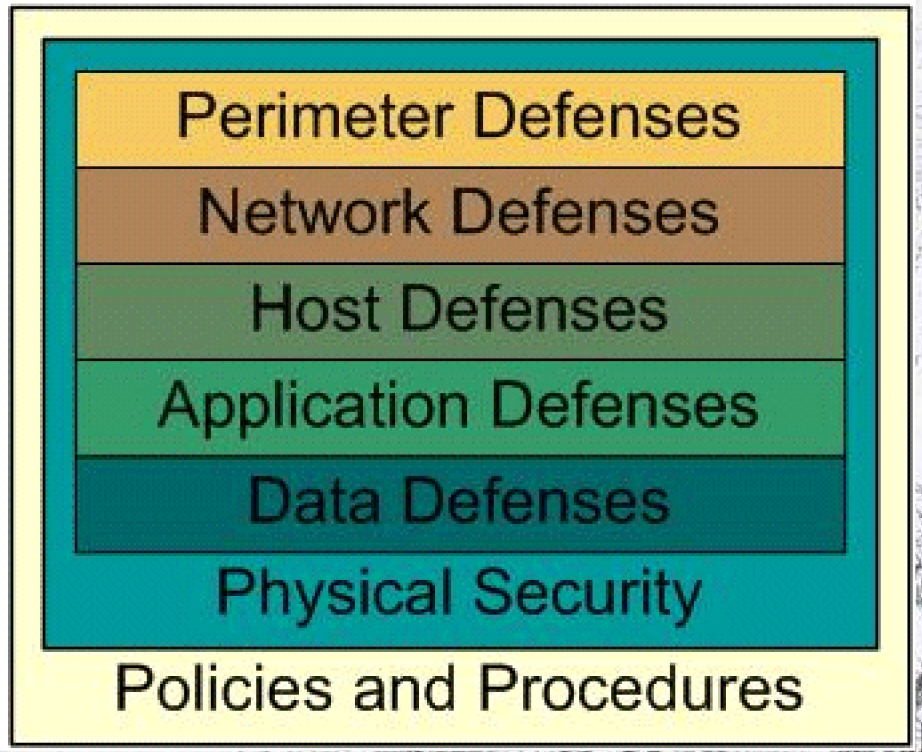
Firewall:1


Stramit Uniguard™ fire-resisting wall system
Steel girt
Steel spacing batten
Promina®60 board
Profiled steel cladding
(Stramit® Corrugated,
Monoclad®, or
Longspan® cladding)

Firewall: 2

Firedoor

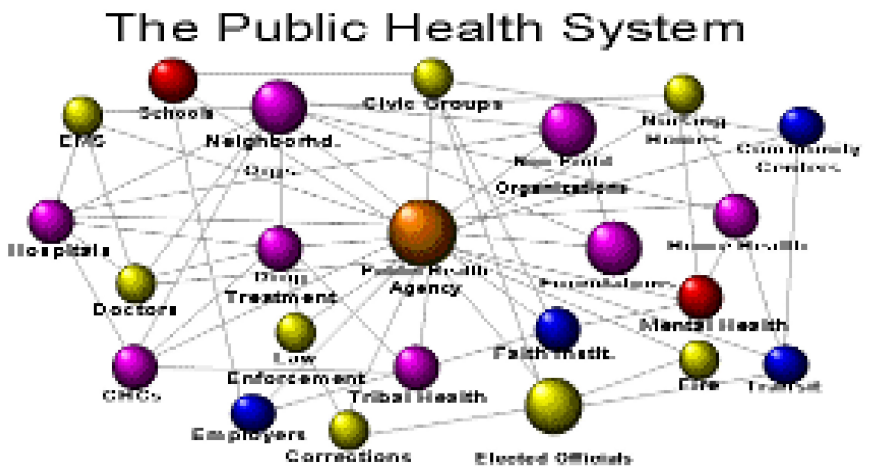
“Defense in Depth”



Which way is “deeper”?
Does each layer really encapsulate the next?
Does the attacker exhaust resources in crossing layers?

Moving Target Defense

Cybersecurity as Public Health



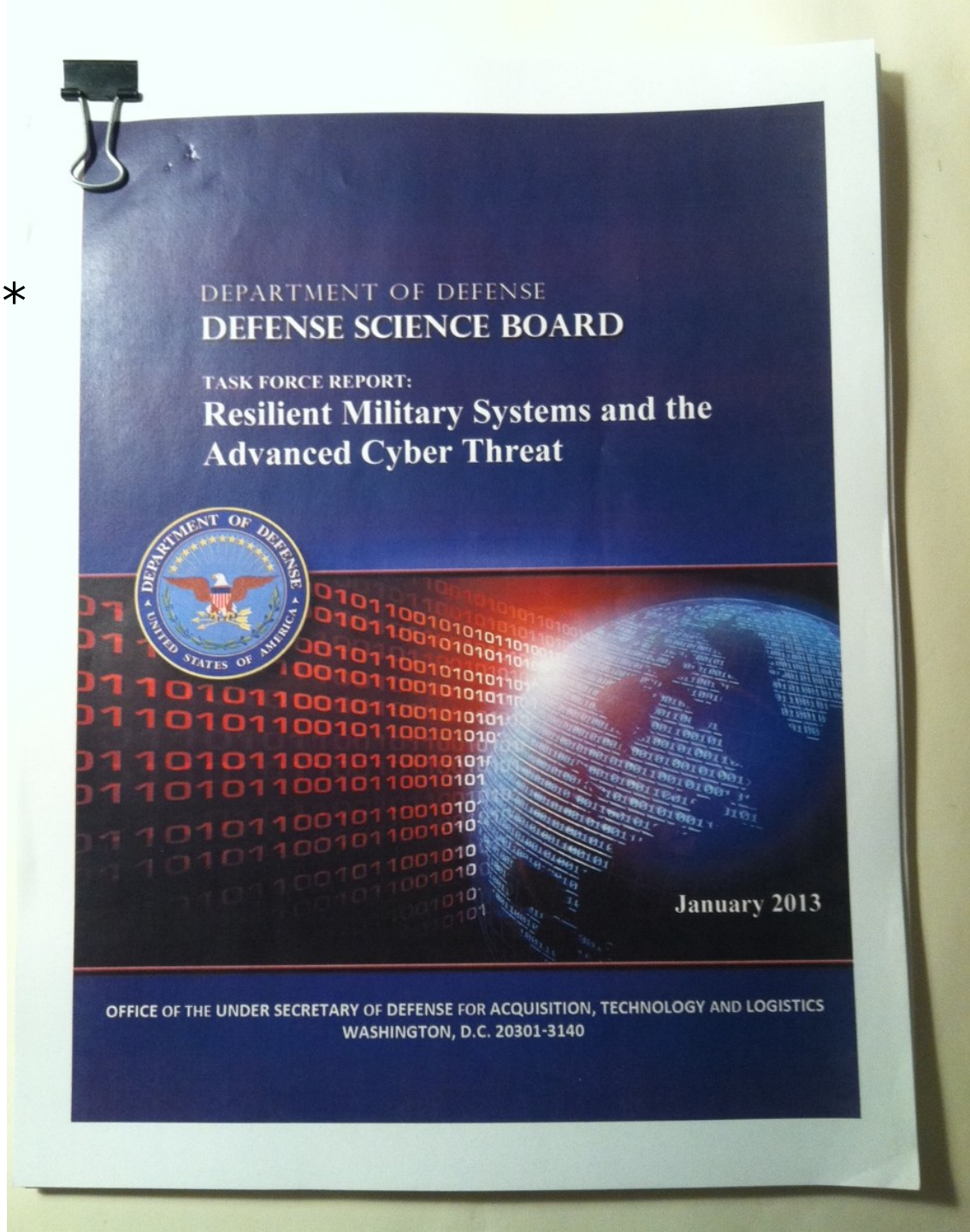
Recent Developments

Defense Science Board says our military systems* are not resilient to cyber attacks

Recommendations include: “Establish an enterprise security architecture, including appropriate ‘Building Codes and Standards’”

*except Nuclear Command and Control1

1. Maybe



Building Code

229. If a builder build a house for some one, and does not construct it properly, and the house which he built fall in and kill its owner, then that builder shall be put to death.

About 1772 BCE

(as translated by L. W. King, available at:

http://eawc.evansville.edu/anthology/hammurabi.htm

Disasters shape building codes

Disasters shape building codes

London fire of 1666 → 1667 Rebuilding Act:

- Includes: “That all the outsides of buildings be henceforth made of brick or stone” – Museum of London website

Santa Barbara Earthquake of 1925 →

- City of Santa Barbara revises building code to require that structures be designed to withstand horizontal forces – first seismic code requirement – MCEER website

Okeechobee Hurricane 1928 →

- “one lasting result of the 1928 storm was improved building codes” – Wikipedia

Kansas City Hyatt Skywalk collapse, 1981

- 114 dead, 216 injured. Construction deviated from design; issues of delegation of responsibility from professional engineers to contractors

9/11 attacks →

- 2004 New York adopts Local Law 26 with code revisions; Sept. 2008, Intl. Code Council adopts 23 changes to fire and building codes motivated by lessons from WTC collapse

Technology / Economics / Policy Shape Building Codes

Plumbing and heating codes

Uniform Plumbing Code, originated Los Angeles 1928, fourth edition 2012

National Standard Plumbing Code (US) first published 1933, updated annually by Plumbing,Heating, Cooling Contractors (PHCC) association

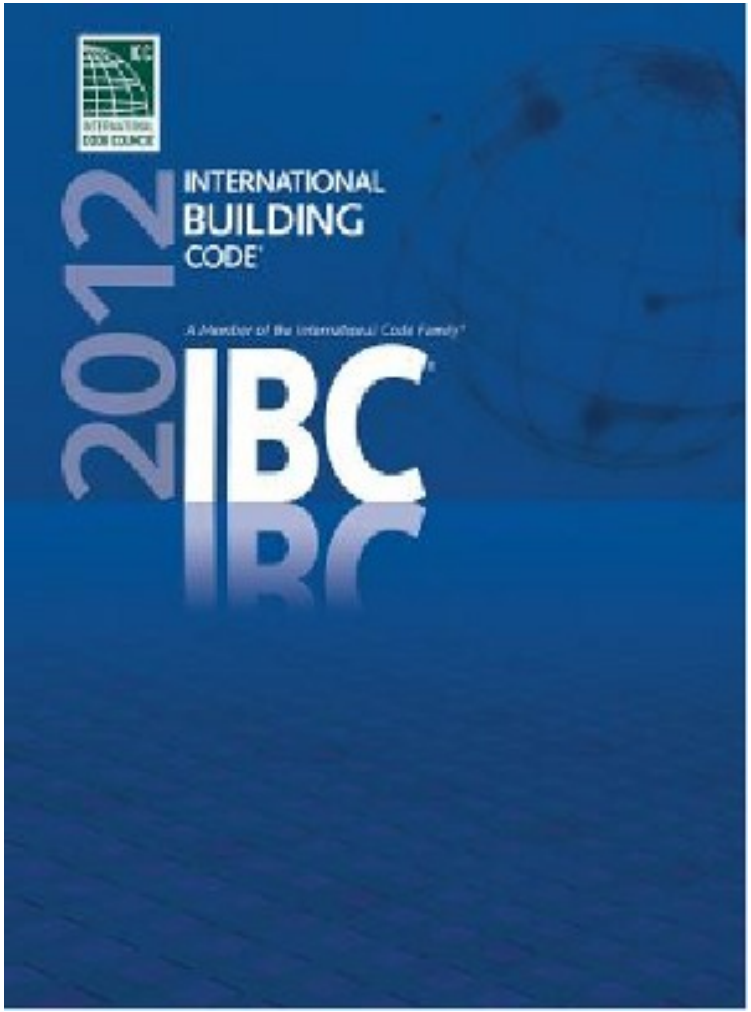
Codes being reshaped today to enable/control graywater use

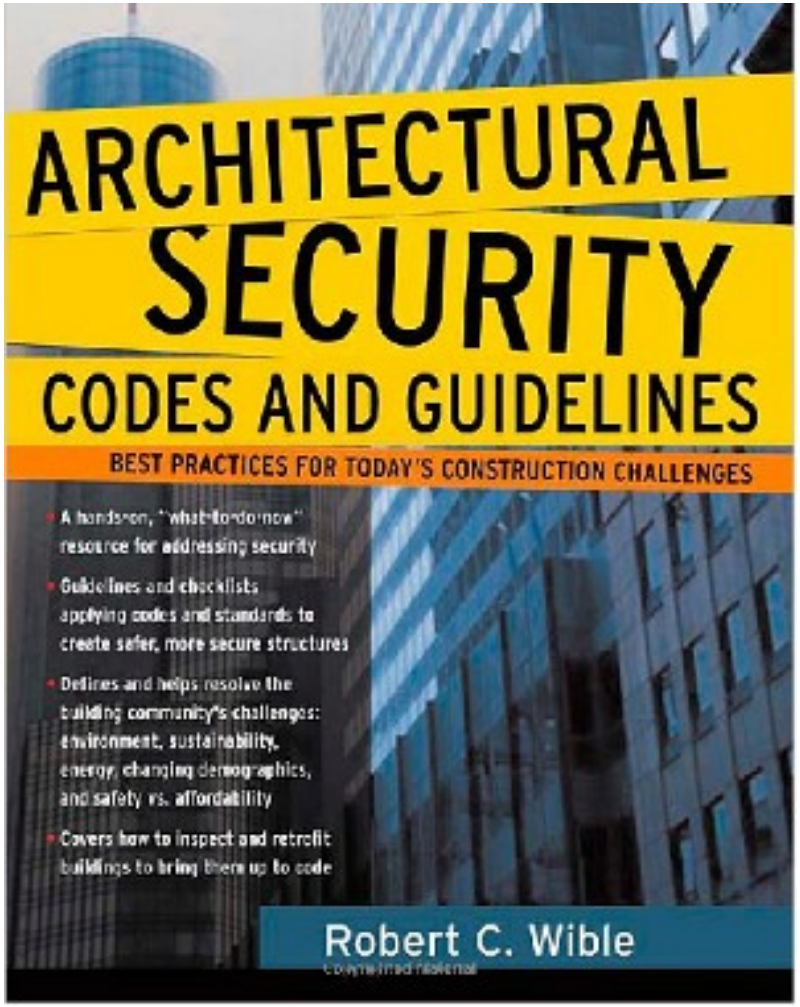
Electrical codes

National Electrical Code, maintained by the National Fire Protection Associaton (NFPA), updated every 3 years

These codes are generally “model” codes and have no force unless adopted by states or municipalities that have legal authority over construction

Codes for Buildings



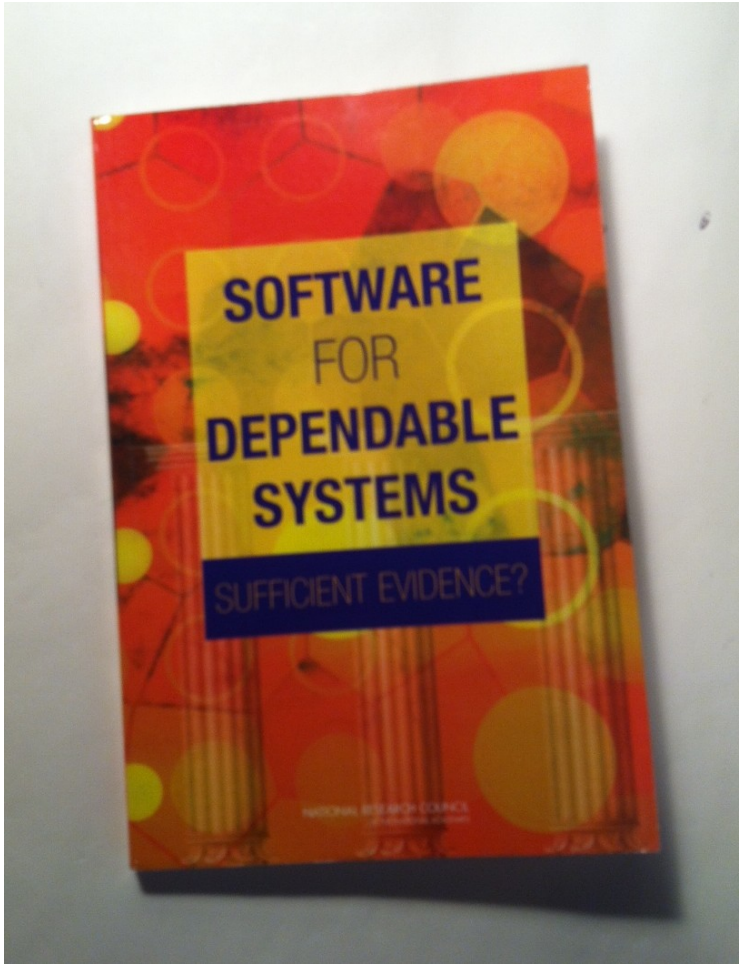


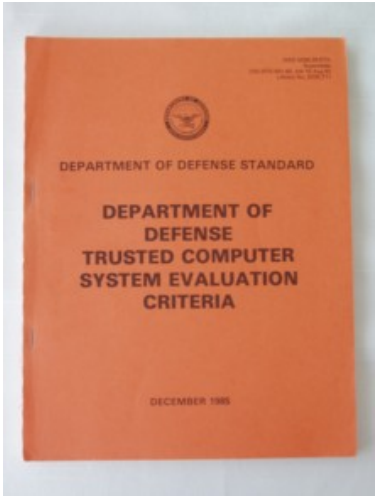
Building Code Characteristics

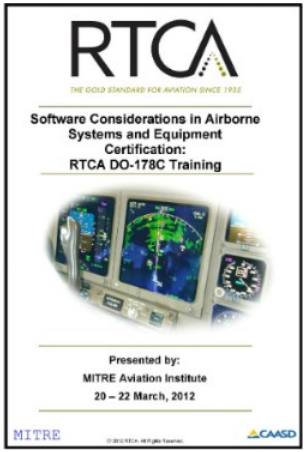
Can specify performance (withstand wind of 100 MPH) or construction (brick or stone facing)
Design approval
Inspection during construction
Approval before occupancy
Evolution to keep up with new technologies and risks

What about a building code for critical infrastructure software systems?

What can we require?
What can we inspect/test?
What do previous examples teach us?







From “Sufficient Evidence”

[About dependable software generally]:
“As is well known to software engineers…, by far the largest class of problems arises from errors made in the elicityng, recording, and analysis of requirements. A second large class arises from poor human factors design…”
[About security vulnerabilities]:
“Security vulnerabilities are to some extent an exception; the overwhelming majority of security vulnerabilities reported in software products – and exploited to attack [them] – are at the implementation level. The prevalence of code-related problems, however, is a direct consequence of higher=level decisions to use programming languages, design methods, and libraries that admit these problems. In principle, it is relatively easy to prevent implementation-level attacks but hard to retrofit existing programs.”

What might a building code for critical infrastructure software look like?

NSF SaTC PI meeting discussion group outcome, Nov. 2012, credits to Bill Scherlis, Sol Greenspan, and group members

Where the metaphor seems to work:

1. Engineering constraints: reduce options in both product structure and process model
2. Predictable quality improvement (intended result of (1))
3. Evidence of quality: things an inspector can see.
4. Support for response and responders. Build in conditions for emergencies (exit windows, e.g.).
5. Support for system evolution.

What might a building code for critical infrastructure software look like?

NSF SaTC PI meeting discussion group outcome, Nov. 2012 (cont'd)

Points of stress in the metaphor (i.e., risks in creating a code)

1. Rate of change in technology advancement in software development, risk of over-constraint
2. Scale and complexity. Software systems are more complex than buildings.
3. Diverse and interacting attributes that affect security.
4. Hardware: also complex, and opaque.
5. Economics drives software development – hard to apportion costs for compliance in relation to mission assurance provided

Modest Proposal

Develop a building code for securing critical infrastructure software that focuses on

- Programming language choices and characteristics
- Automated means of assurance
- System security architecture in relation to function
- Delivered software/system in preference to the development process

Who's interested?

The President, evidently:

For Immediate Release
February 12, 2013

Executive Order -- Improving Critical Infrastructure Cybersecurity

EXECUTIVE ORDER

- - - - - - -

IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY

And NIST, presumably:

Sec. 7. Baseline Framework to Reduce Cyber Risk to Critical Infrastructure. (a) The Secretary of Commerce shall direct the Director of the National Institute of Standards and Technology (the "Director") to lead the development of a framework to reduce cyber risks to critical infrastructure (the "Cybersecurity Framework"). The Cybersecurity Framework shall include a set of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks. The Cybersecurity

And maybe even industry…

Wall Street Journal, May 13, 2013, p. B10:

- FTC is suing Wyndham, alleging hotelier followed lax data-security practices that unnecessarily exposed customers' data to theft
- **Wyndham responds in court filing that the FTC brought the case without ever providing companies with any guidance on what security practices they should adopt.**

LAW JOURNAL.

Legal Tempest Over Cybersecurity

Hotelier Wyndham Mounts a Court Challenge to FTC's Authority to Police Corporate Data Practices

By Brody Kohnala

When hackers broke into computer systems at **Wyndham Worldwide** Corp. and several of its hotels, they allegedly stole payment-card numbers for hundreds of thousands of consumer accounts.

They also sparked a high-stakes legal battle over whether a federal agency can use its consumer-protection powers to police cybersecurity practices at American companies.

The Federal Trade Commission sued Wyndham and three subsidiaries in the wake of the data breaches, alleging that the hotelier followed lax data-secu-

The company said data-security standards should be decided in the political arena, where Congress is debating legislation and already has enacted security requirements for financial institutions, health-care providers and others.

"In light of the important economic and political considerations involved in establishing data-security standards for the private sector...it defies common sense to think that Congress would have delegated that responsibility to the FTC—particularly through a 1914 statute that does nothing more than forbid

Lexus ES 300h: A Smooth, Elegant Guilt-Eraser

Closing Thought

Dan Neil, Wall Street Journal, March 16, 2013, p. D11
"This quite-uncompromised car...[Lexus ES300h hybrid].. averages 40 mpg in mixed driving, according to the EPA. That's astounding... this yearling moose of a car gets about the same fuel economy as a Ford Fiesta...

“You know what's even more astounding? Recall the legions of entrenched industry forces who, two decades ago, swore on their professional lives that increased fuel-economy standards would drive up the cost of automobiles while making them boring and less safe. Yeah, that didn't happen at all.

"In fact, the opposite has happened. Cars have gotten more fuel efficient and more powerful, and quite measurably safer in every type of collision.”

Moral: Design constraints need not kill creativity and innovation. In fact they can be powerful motivators. We need to try some of that.