Critical Infrastructure vs Computer Science vs Software Engineering

Randy Bush <randy@psg.com>

Internet Initiative Japan & Arrcus

2019.08.28

You Have Heard of Impostor's Syndrome

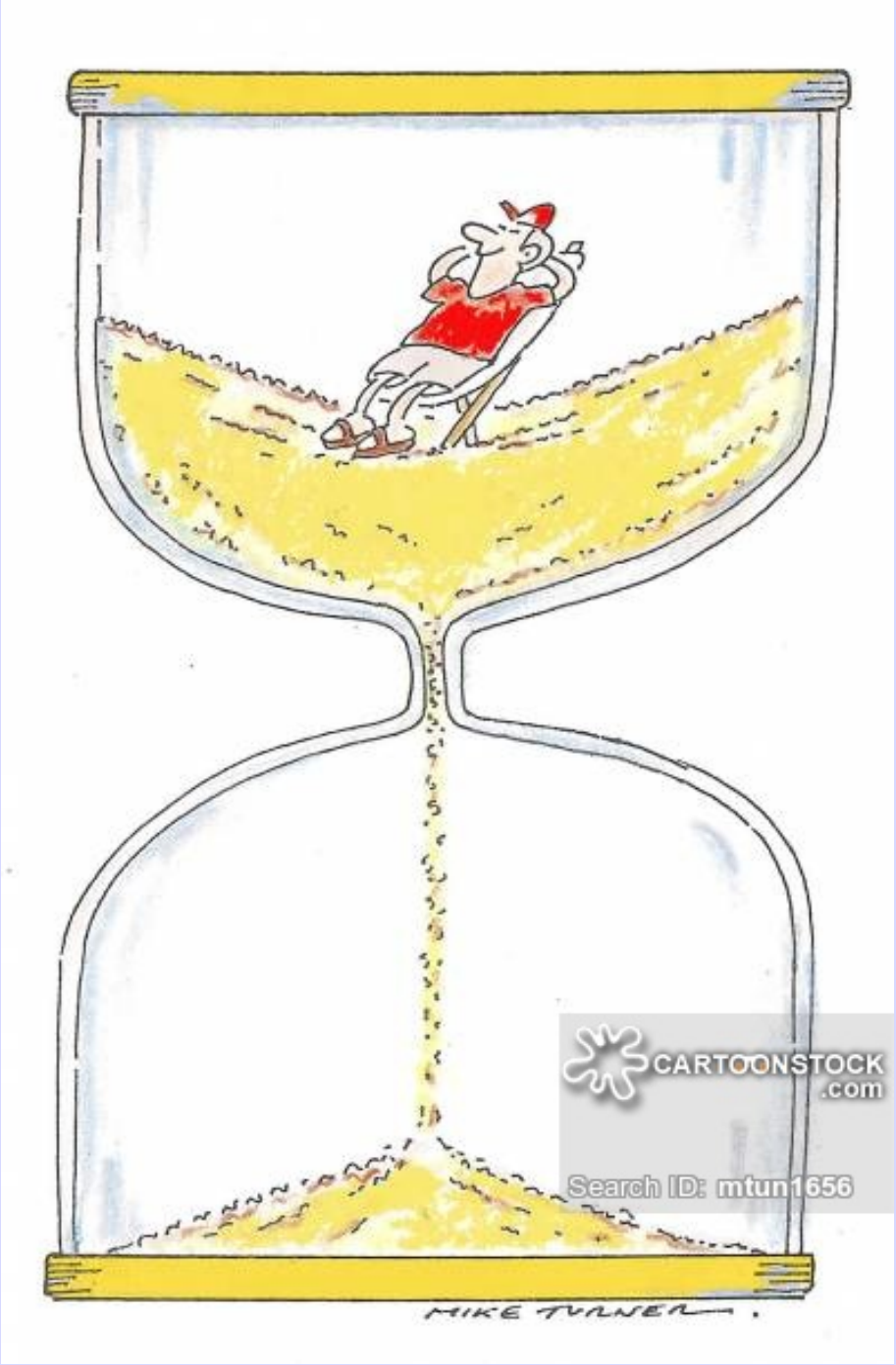
Well, I AM an Impostor

¥dayjob – IIJ – Research Tourist

$dayjob – Arrcus – a Vendor Protocol & Security Architecture Tourist

As a Tourist, Much of What I Have Seen Deeply Scares Me

In One Slide



A Confused Jumble Rant

- Critical Infrastructure
- The Internet is Hacks on Hacks, not Computer Science
- Software Engineering? What's that?
- Why Systems Fail
- The Internet is Death by a Thousand Cuts

In 2003, Tim Griffin and I Wrote a Position Paper, *Towards Networks as Formal Objects*

We Could Not Get it Published

https://archive.psg.com/030131.formal-nets.pdf

"The success of the end to end principle has led to a commonly held fallacy that the Internet core is simple and stupid. A corollary to this is that there is nothing interesting here for networking research.

"Our experience with the overwhelming difficulty of managing and operating core functionality tells us that exactly the opposite is true.

"At the heart of the problem is a *lack of network level models and abstractions*. The evolution of appropriate models and abstractions *requires a deep understanding of the data networking domain*.

If some of our better computer scientists are studying the Internet as a *behavioral phenomenon*, we are in very deep trouble.

I.e. the system is so complex that we can not reliably predict its behavior.

Most of the Protocols Were Designed on Serviettes. Really!

They are Proud of It!

But We Have Bet Civilisation On It!

What the Heck is Critical Internet Infrastructure?

Framing from ENISA

- **Critical Infrastructure**: an asset, system or part thereof located in Member States that is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact on a Member State as a result of the failure to maintain those functions.
- **Critical Information Infrastructure**: Information infrastructure (networks, hardware, software, etc.) critical to the functioning of a nation or country, like IT that supports health- or energy-sectors.

Critical Internet Infrastructure

The Internet as We Know It Could Soon be Over

Supply Chains for Food, Electricity, Fuel, etc. Can be Measured in Hours

We're Three Days from Mad Max

A Determined Nation State Attacker Could Bring the Global Internet Down in an Hour

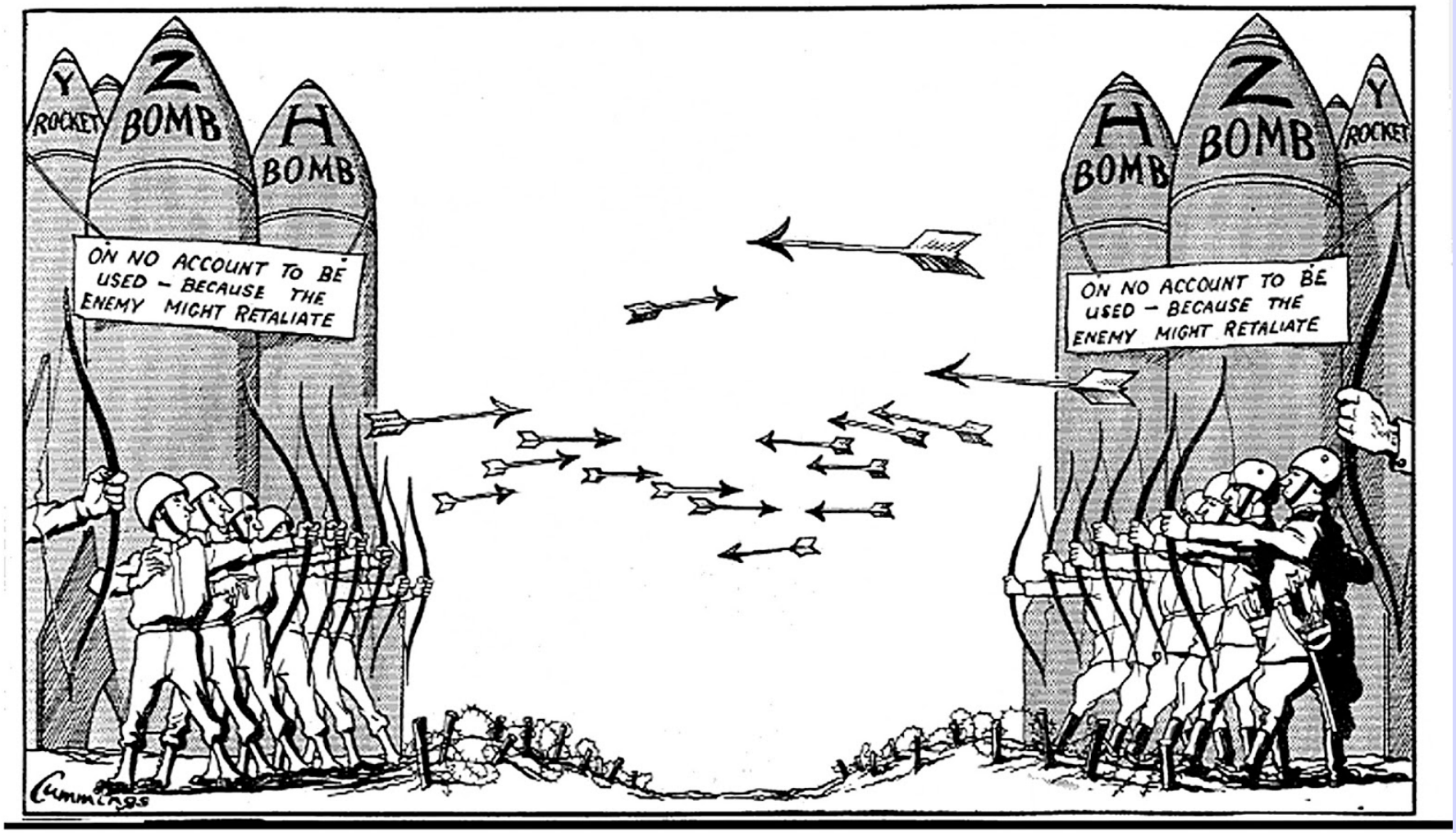
Heck, One of a Hundred Clueful Geeks Could do it

If Defense is Hard and Attack is Easy

The Incentive is to Escalate Attacks!

And the Steering Wheel is Ever More in the Hands of People with More Testosterone than Brains

Mutually Assured Destruction



XR

Why Have They Not Done This to the Internet?

Mutually Assured Shopping?

Critical Infrastructure is Military, Hospitals, Power/Energy, Business to Business

And it is Highly Vulnerable

Putting SCADA-Based Power Grid, Water, Electricity, etc. on the Internet is Insane!

So Where Are We Going?

We're from the Government and We're Here to Help

Like they Helped With the BGP 'Mis-Announcements' of Google, Facebook, Apple, and Microsoft

And
Pervasive Monitoring
Breaking TLS
Outlawing Crypto
Disconnecting the Net

The Governments, in their move to the Right, Surveillance, … Are REMOVING Safeguards

But in the CII, Enterprise, Military … World

Security and Integrity are a Disaster

It has been Breach after Breach, after …

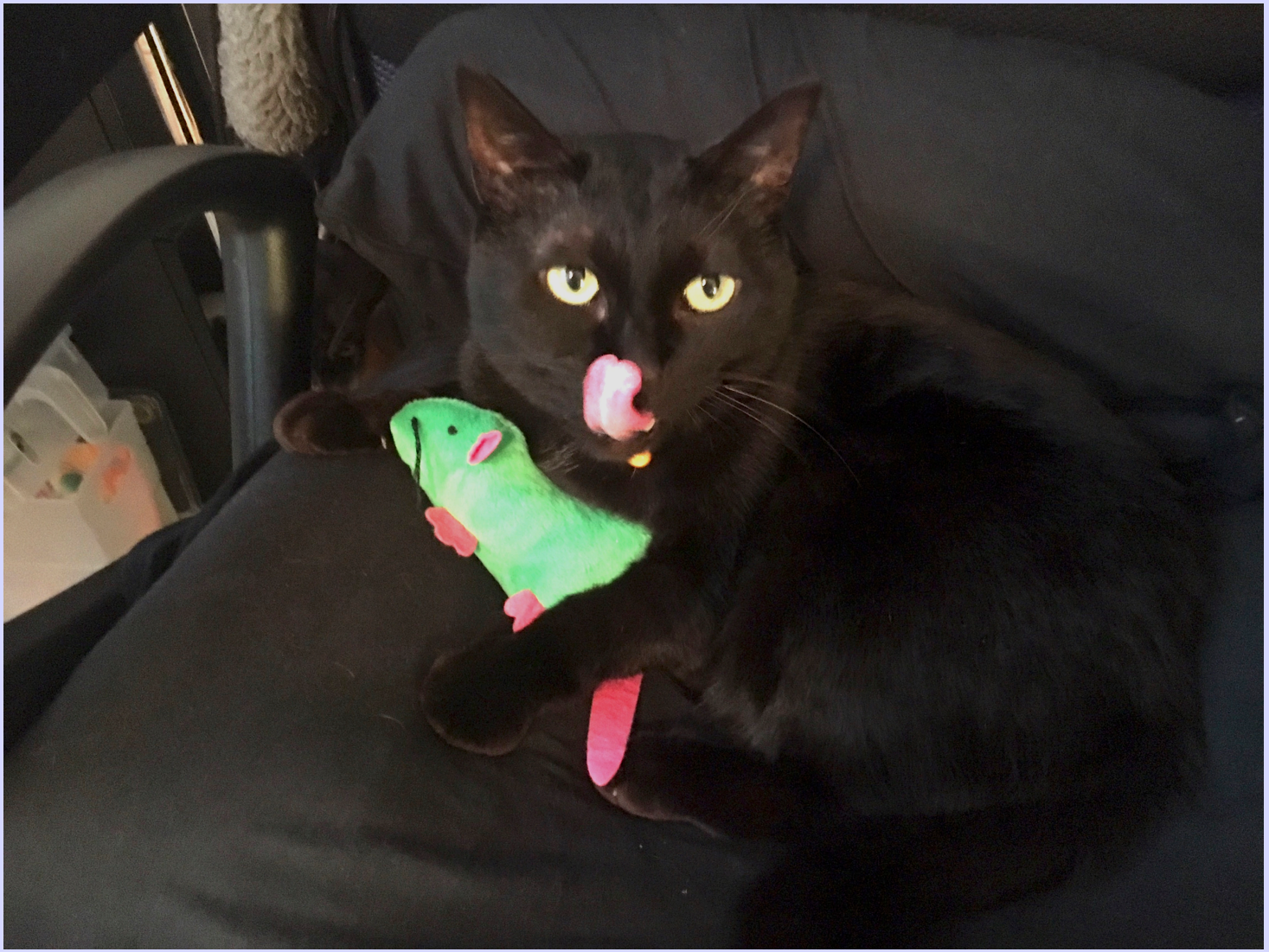
The Firewall Fantasy Still Dominates

All it Takes is One Bit of Malicious JavaScript in One Brokered Advert on One User's Laptop

US DoD Data Showed on Average 1/3 of Vulnerabilities in Government Systems Were in the Security Software

This is My Government

- Allowed the OPM hack where 21.5 million govt employees' details went to China
- Gave the NSA's TAO Tools to perps unknown, but Russians are suspected
- And those tools are being turned on the public by evildoers (RansomWare)
- These same governments wants us to trust them with our private keys



Flaws in Specs

Bugs are incorrect implementation

Flaws are bugs in the specification

And the specifications are not formal

If it was part of the "plan" it's an "event," if it is not then it's a "disaster"

On a Slightly More Positive Note

Network Configuration is a Bit Better

DevOps, Ansible, & Puppet are Delivering what SDN Promised

Central Policy but Distributed Protocols

Not the Danger of a Central Point of Failure Programming 10,000 Forwarding Tables

Yang / NETCONF/ RESTCONF (AKA SNMPng) May Up-level Configuration and Management a Bit

Without a Formal Model a Large Ansible Deployment is as Maintainable as a Large Perl Deployment

On the Other Hand

DNSsec, IPv6, & Routing Security are Barely Deployed

Centralized Configuration

Jupiter Rising

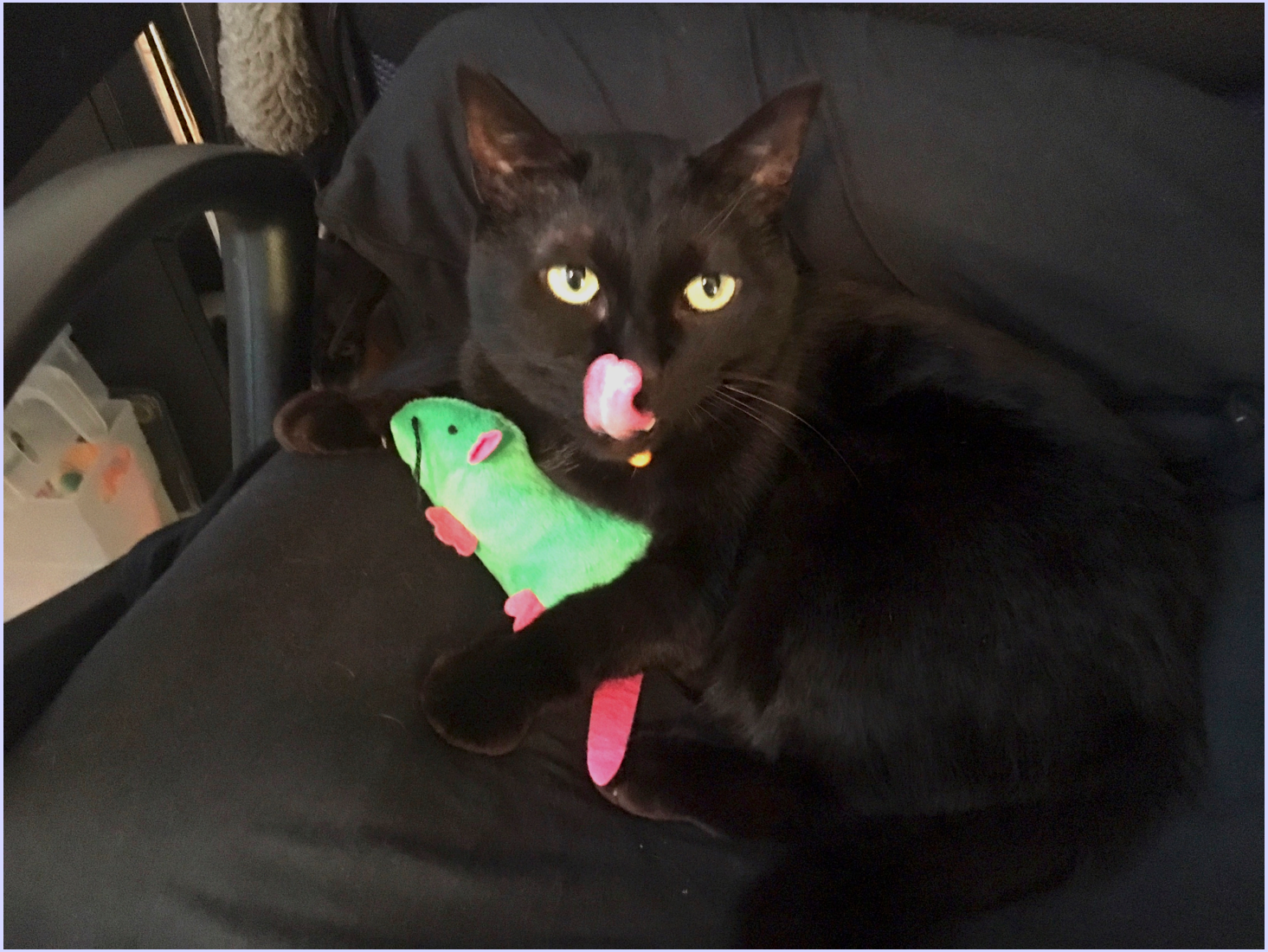
https://ai.google/research/pubs/pub43837

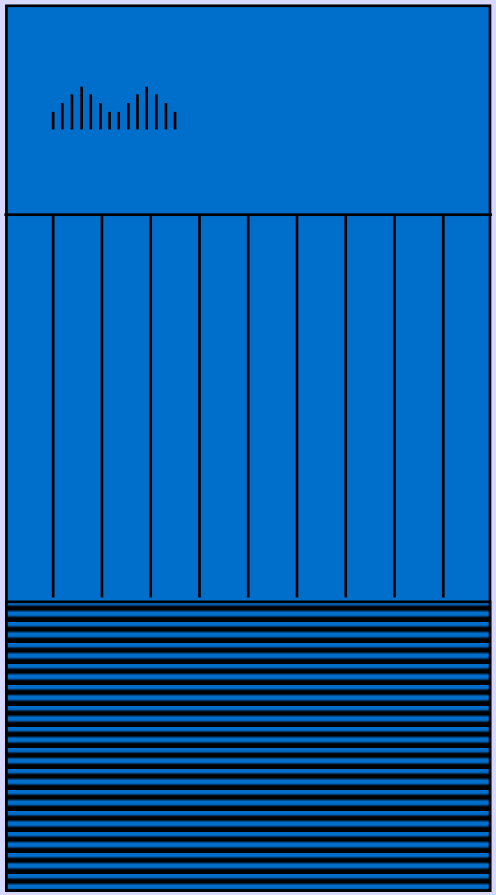
vs

Distributed Topology

BGP-SPF

Software Still Sucks!





This is a bit of Hardware and 10s of Millions of Lines of Code with NO FORMAL DEVELOPMENT METHODS

Carrier Class Reliability

- The famous 5ESS switch regularly has five nines in operation and has even hit six nines in the field
- We all think we want that in routers and other internet boxes
- Can we achieve this?

The Truth About Five Nines

- Almost half the code is a supervisory function which runs continually cleaning up **internal inconsistencies in the data structures**
- Without this, the 5ESS crashes in a few hours
- Can you imagine this approach scaling to internet routing?

Why Systems Fail

- Most security holes are due to buggy software.
  - As of 1998, 85% of CERT advisories described problems not fixable with cryptography.
  - About half of all new holes are due to buffer overflows.
- "Patch and pray" is no way to run an Internet.
- Patches are often hard to install, and can cause their own problems (and holes).
  - *No* responsible administrator of a production machine will install *any* patch without extensive testing.

FlightRadar24

Flypocalypse (2015.8.15)

It Was Just a Quick Patch

Defense Strategies

- We're not going to get rid of buggy code.
  - We've been trying for far too long to have any realistic hope of success now.
- We can't do much about lack of diversity – the "network effect" is too strong.
- We can try to reduce central points of failure.
- We must learn how to compose secure components, and how to build secure distributed systems out of insecure pieces.

Major Control Systems

Non-linear interactions of these can produce seriously disastrous results

- Routing
- MPLS Control Plane: LDP and RSVP
- DNS
- RPKI (and NTP)
- CDNs shifting traffic
- Peer to Peer Traffic Engineering
- Automated Traffic Engineering
- Reactive Configuration of Network
- OpenFlow
- TCP Congestion Mechanisms
- Interaction with Human Behavior (e.g. redialing)

Forgetting the insane designs,

How would you even test for this?

Fat Finger Friday

The first Friday of each month, we take out one control system

- We will learn how to take it out, i.e. Vulnerability Analysis
- Minimal interventions to cause maximal affect
- We will pre-announce, so the world will think about defenses
- We can measure and analyse

That was not meant to make you feel comfortable

Resilience Mechanisms

- Metric: correlation in spikes in help desk calls
  - AMAZON: rate of sales drop
  - Airlines – even 'almost' accidents are investigated
- Airlines investigate non-critical events
  - Maybe partial causes
  - Correlated events are perhaps the problem – interactions
    - They investigate subcritical because want to avoid the correlated cases
- What other systems should we [not] look at
  - Power?
  - Old telcos?

Resilience Mechanisms Can Be Our Enemy

- Resilience mechanisms are designed with particular failure modes in mind. When circumstances fall outside those boundaries, their [re]actions can interact with control systems in unanticipated ways.

- E.g. SONET restoration under Layer Three healing under CDN traffic shifting.

Assume 42 Slides on Formal Specification Model-Based Development, and Software Engineering

Software Engineering

- Formal Methods would be useful
- In devices
- In protocols
- Software Engineering is rare in the hardware vendor culture, "What's Valgrind?" And that is not even SE
- It is starting to be exercised in the OS and Applications Vendors

Microsoft Attacked Their Horrible Security Problem

Now One of the Most Secure Platforms

Complexity – the Enemy of Analysis, Reliability, Repairability, Scalability

Everything, Unless You are Paid by the Hour

Complexity is the Arch-Enemy of Scaling, Hence of the Bottom Line

- Telco culture started to glorify complexity as a competitive tactic in the '70s
- But look what it did to Operational Expense
- Land-lines are dead. Mobile is losing margin and being eaten by Over The Top services
- ISPs are all in a commodity market and buy from the same vendors as the competition

But Where is CII?

- Let's assume that public agencies such as ENISA can easily identify Critical Infrastructure
- How do they figure out how it connects to the Internet so they can identify Critical Internet Infrastructure?
- And how do they discover inter-ISP connectivity?

Topology is Hard

- Critical Infrastructure does not want to disclose connectivity as it may make them more vulnerable
- Providers view interconnection as NDA
- Research into Internet topology is primitive and error prone
- Public data are weak despite braggadocio

10 Lessons from 10 Years of Measuring and Modeling the Internet's Autonomous Systems

(synopsis: you can't do this reliably)

IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, VOL. 29, NO. 9, OCTOBER 2011

And Then What?

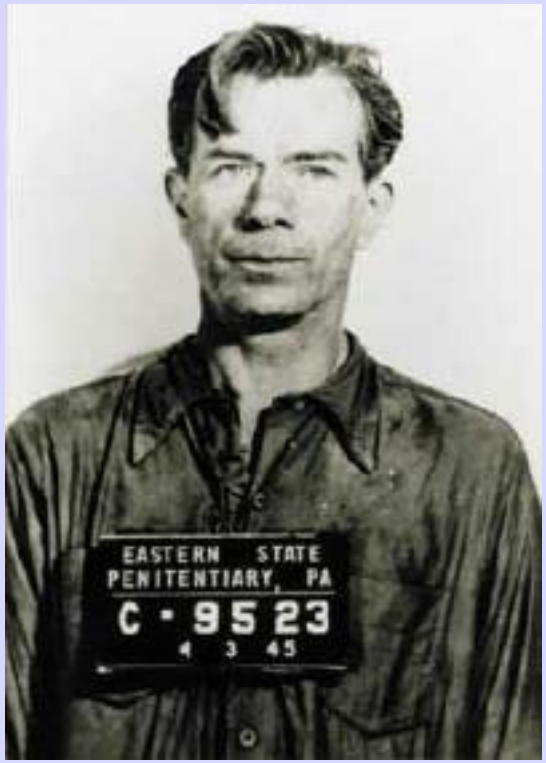
- Are we going to regulate how Critical Infrastructure connects to the Internet?
- Are we going to regulate how Internet providers inter-connect?
- Are we going to regulate a provider's infrastructure?

How About we Regulate use of Formal Methods?

CII is Reluctant to Disclose Vulnerabilities, Attacks,…

So We Have Bad Metrics

Willie Sutton



American Bank Robber 1920s-1950s

When asked why he robbed banks, said

"Because that's where the money is."

<doh>

Due to the *Willie Sutton Effect*, Crypto Currencies Have Been a Major Target

My Favorite

BGP Hijacking Used to Grab Bitcoins

Hijacking Bitcoin: Routing Attacks on Cryptocurrencies

Maria Apostolaki, Aviv Zohar, Laurent Vanbever

https://btc-hijack.ethz.ch/files/btc_hijack.pdf

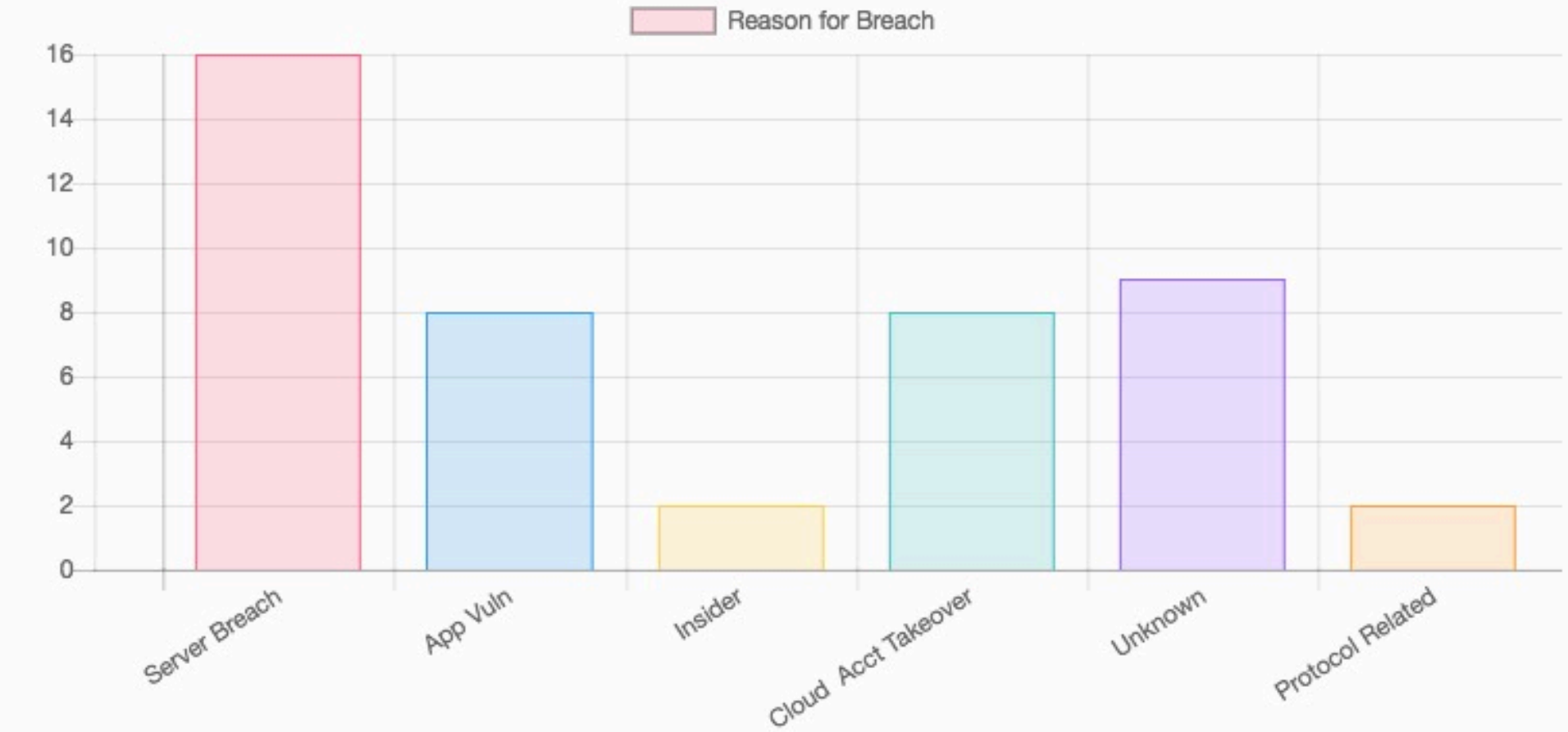
Blockchain Graveyard

- A Litany of Failures Worth Study
  - OpSec
  - Social Engineering
  - Insiders
  - Broken Software
  - Takeover of Cloud Hosting

  I loved "We planned to get the stolen property returned, and thought that was the end of it."

ROOT CAUSE ESTIMATES

The data below is roughly gleaned from publicly available data about **45** incidents. This should assist estimation during threat modeling.



IoT is a Disaster Which is NOT Waiting to Happen

The "S" in IOT Stands for Security

We Seem Unable to Contain the Problem

Computer Science Joke

- With enough complexity we strongly suspect that we can operate an approximate internet in polynomial time and dollars
- We are working on a proof that operating the internet can be made to be NP hard
- If we just keep hacking and it will all work out; just like climate change

But Seriously

How Do We Get Out of This Mess?

"Clean Slate Approach" Has Failed for 20 Years

Massive Installed Base

Changing the Engines on a 747 In Flight

There are Decades of Great Software Engineering Methods

Use Them!!!!

How can we Insert Formal Methods?

Jack the House Up & Build a Real Foundation

Tim Griffin (and students) Algebra for Routing Policy

Matt Roughan (and students) Formal Design and Verification of L2/L3

Until the Revolution, Eternal Vigilance

Thanks To

Internet Initiative Japan

Arrcus

A Cisco Research Grant

And a Large American Telco
which did Not Listen