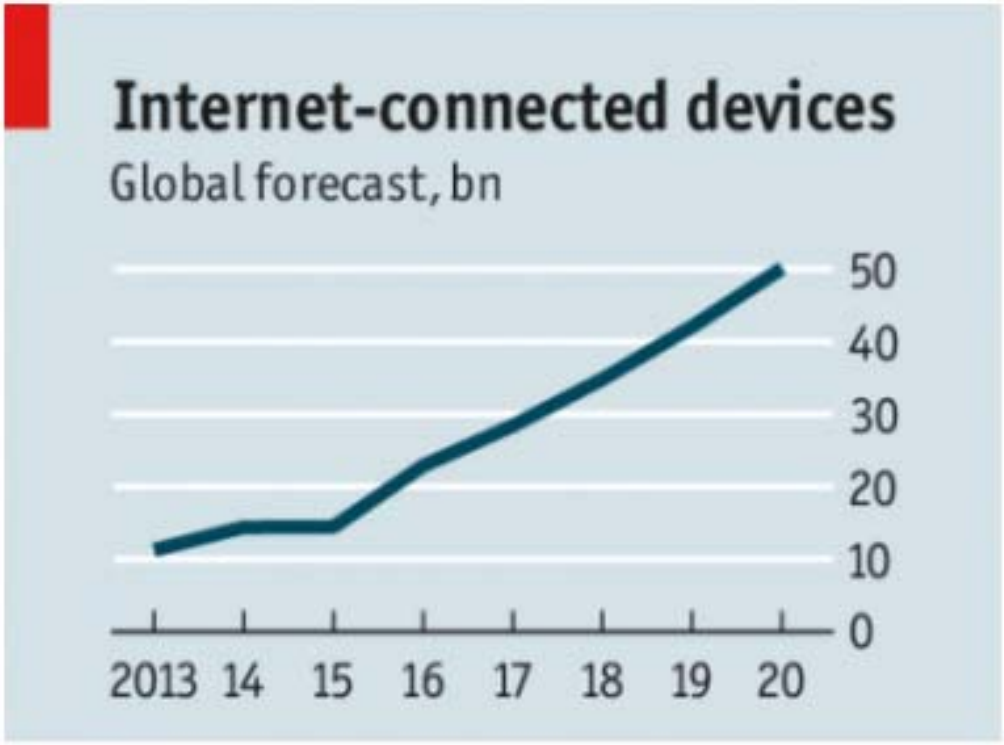
Some thoughts about IoT and IoT security

Peter L. Levin
peter@amida.com
@pllevin
October 22, 2017

Hardware sabotage

“The most monumental non-nuclear explosion ever seen from space” was reportedly caused by the US in a Soviet commercial gas pipeline.

An Israeli bombing raid on a suspected Syrian nuclear facility was due to a “kill switch” that turned off surveillance radar.

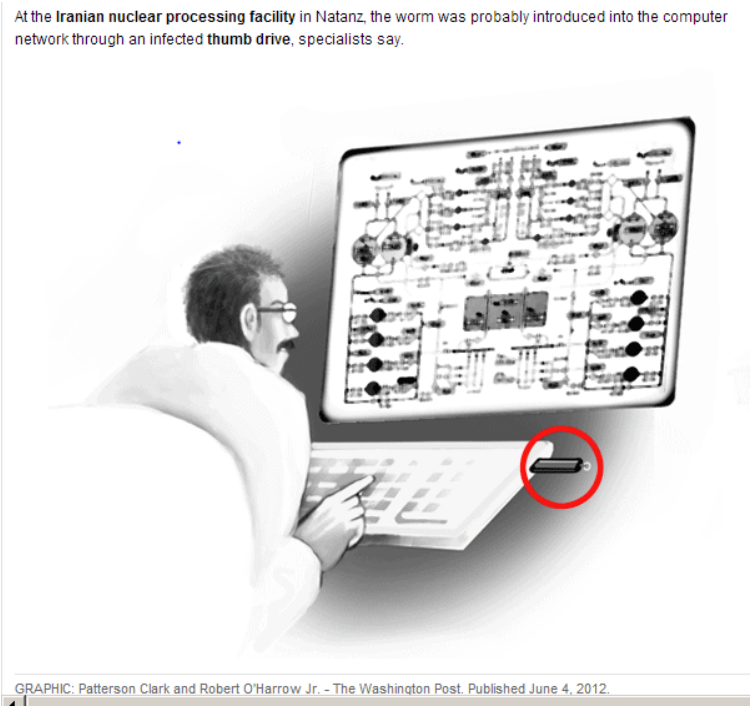


The Economist, Jul 12 2014

What if the target is
a very specific thing,
in a very specific place,
(and it isn't connected to the internet)?

For example: a centrifuge

- Controls mechanical devices while reporting normal operation
- 20 zero-day exploits
  - Looking for specific target
- “Natanz personnel could have unknowingly transported Stuxnet after using infected personal computers.“



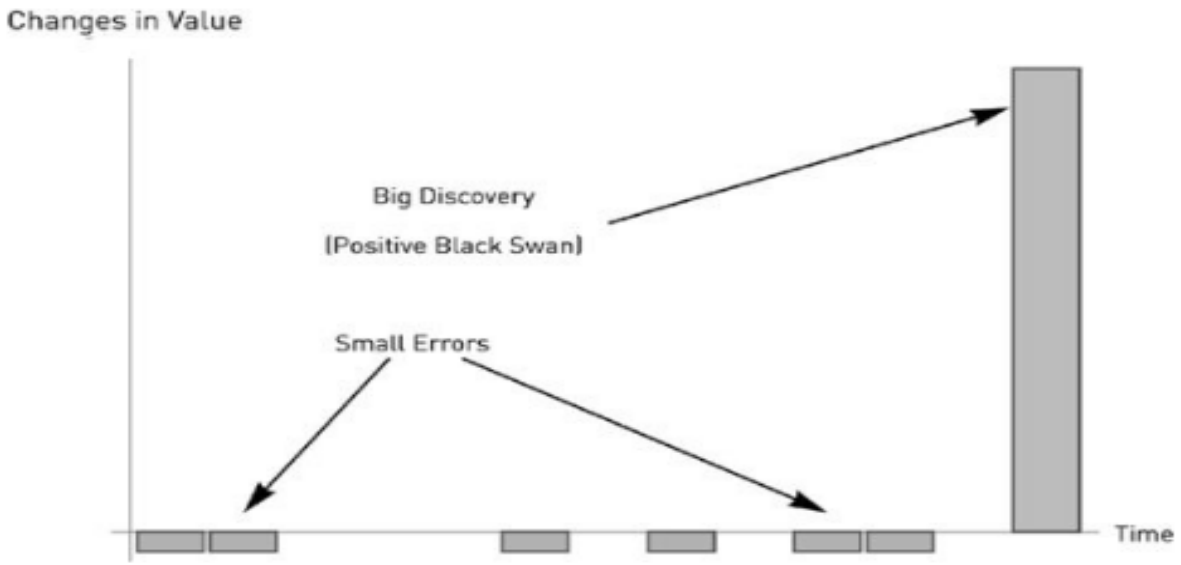
http://isis-online.org/uploads/isis-reports/documents/stuxnet_FEP_22Dec2010.pdf

Two basic approaches to cyber mischief

“see what happens” approach

“target object” approach

Cast in an “anti-fragile” frame of reference



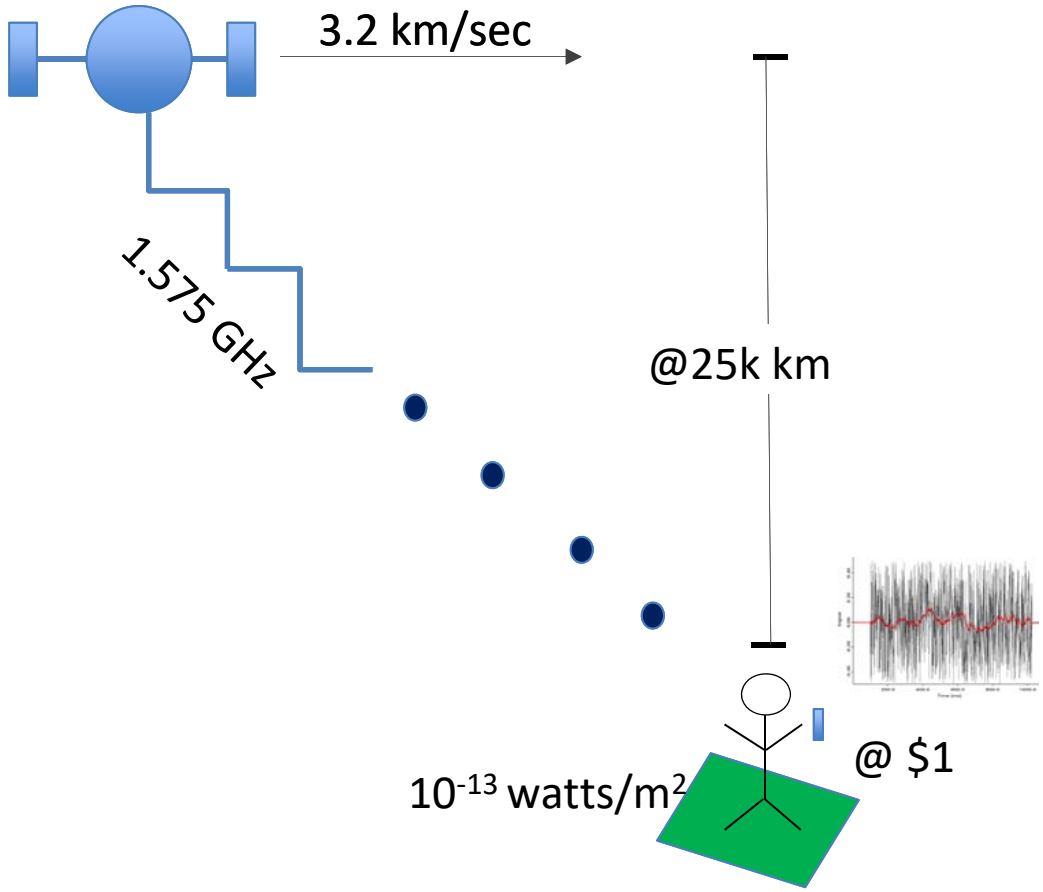
The mechanism of option-like trial and error (the fail-fast model) . . . [results in] low-cost mistakes, with known maximum losses, and large potential payoff.

Antifragile: Things That Gain from Disorder by Nassim N. Taleb (2012)

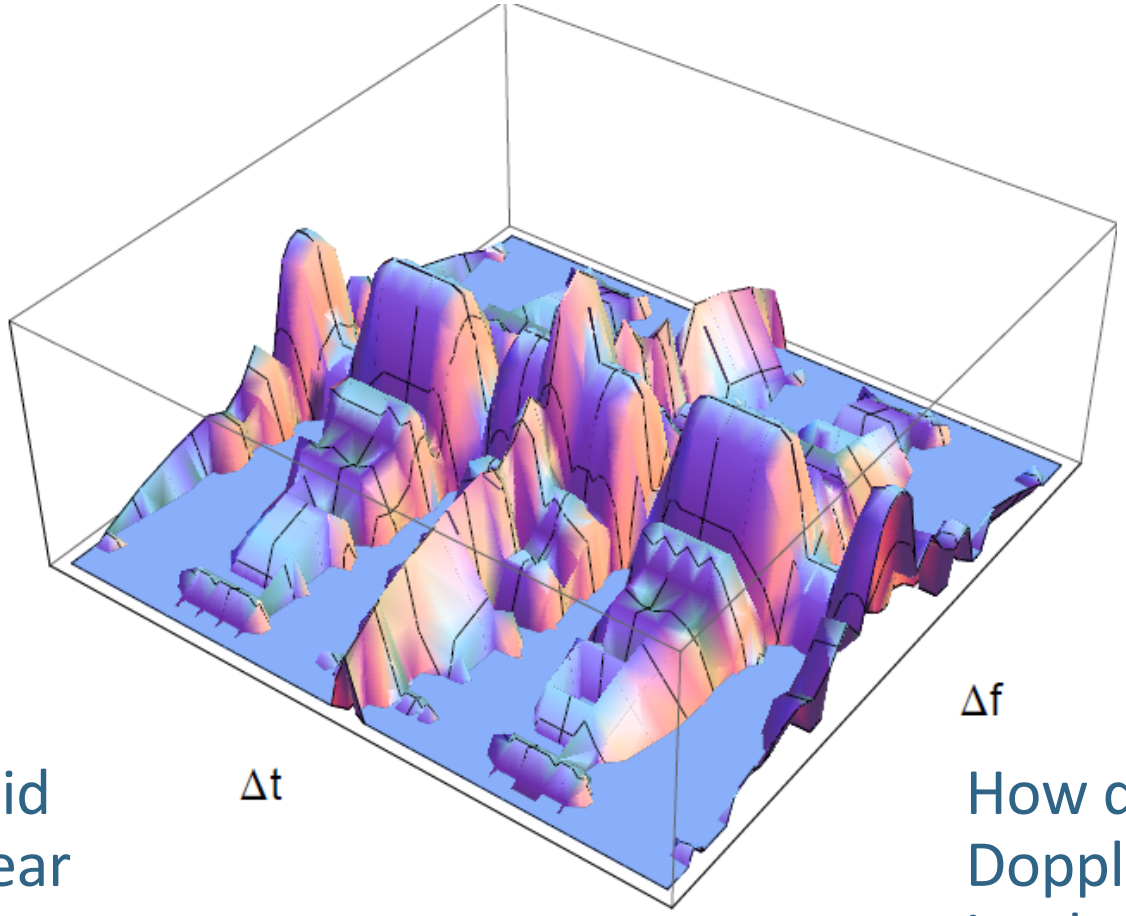
Related topic: detection of small signals. How can we hear the satellite's beacon when it is 6db below the electromagnetic noise floor?

Fundamentals of GPS:

- a cesium clock
- a 100 watt transmitter
- a space rocket
- a handheld receiver
- a very clever signal



Answer: Pattern matching



How long did it take to hear the signal?

How does Doppler perturb its shape?

Snapshot of an ambiguity function created by Prof Per Enge, Stanford University

These are big data problems:
looking for signatures and patterns.

This assumes that you know what you're looking for —
that there's a source for you to hear,
and that you can hear it somehow.

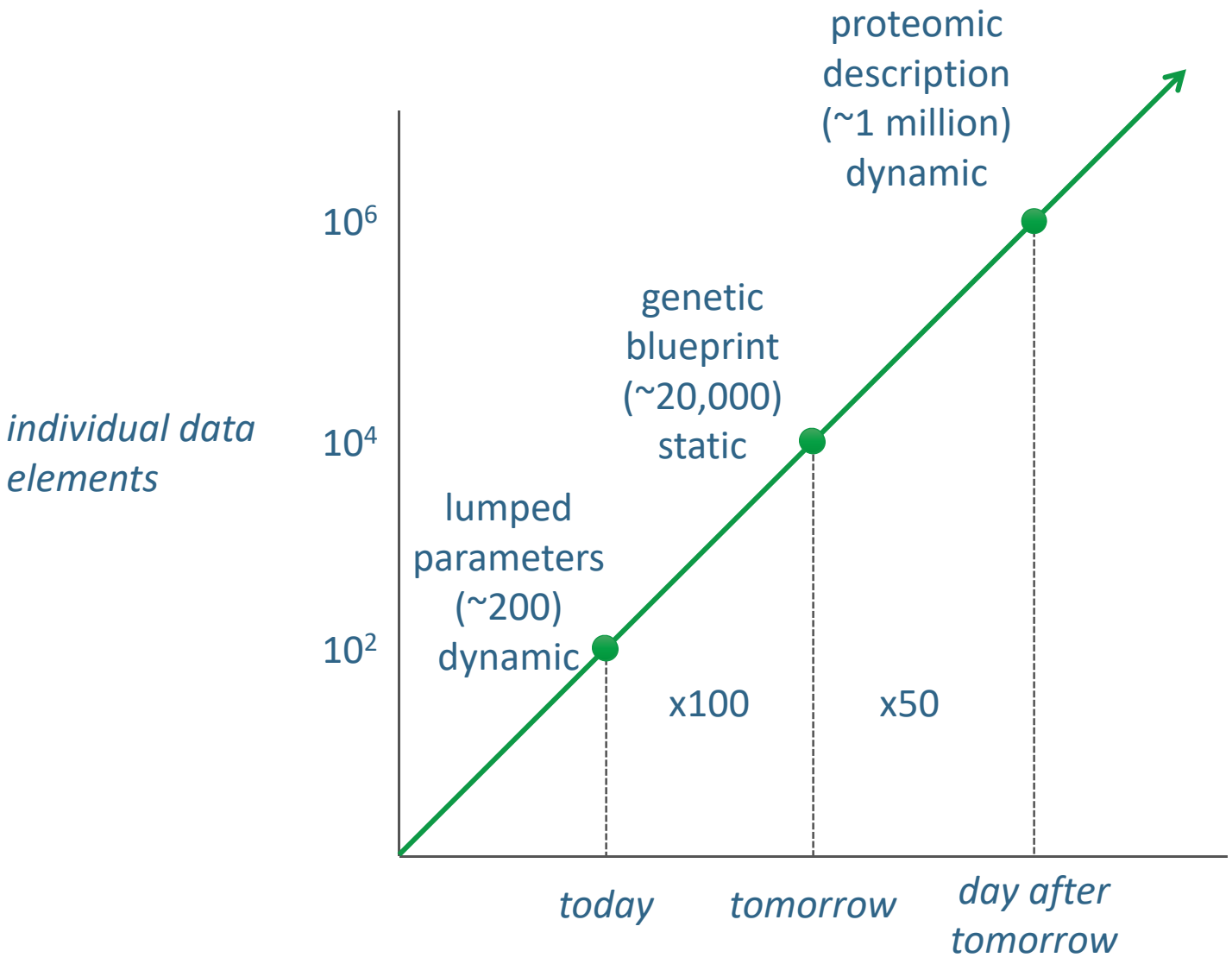
The situation today:

We can capture more data (networked things are everywhere)

and

we can process it more effectively (better compute).

A *really* big data problem



Scope of health data

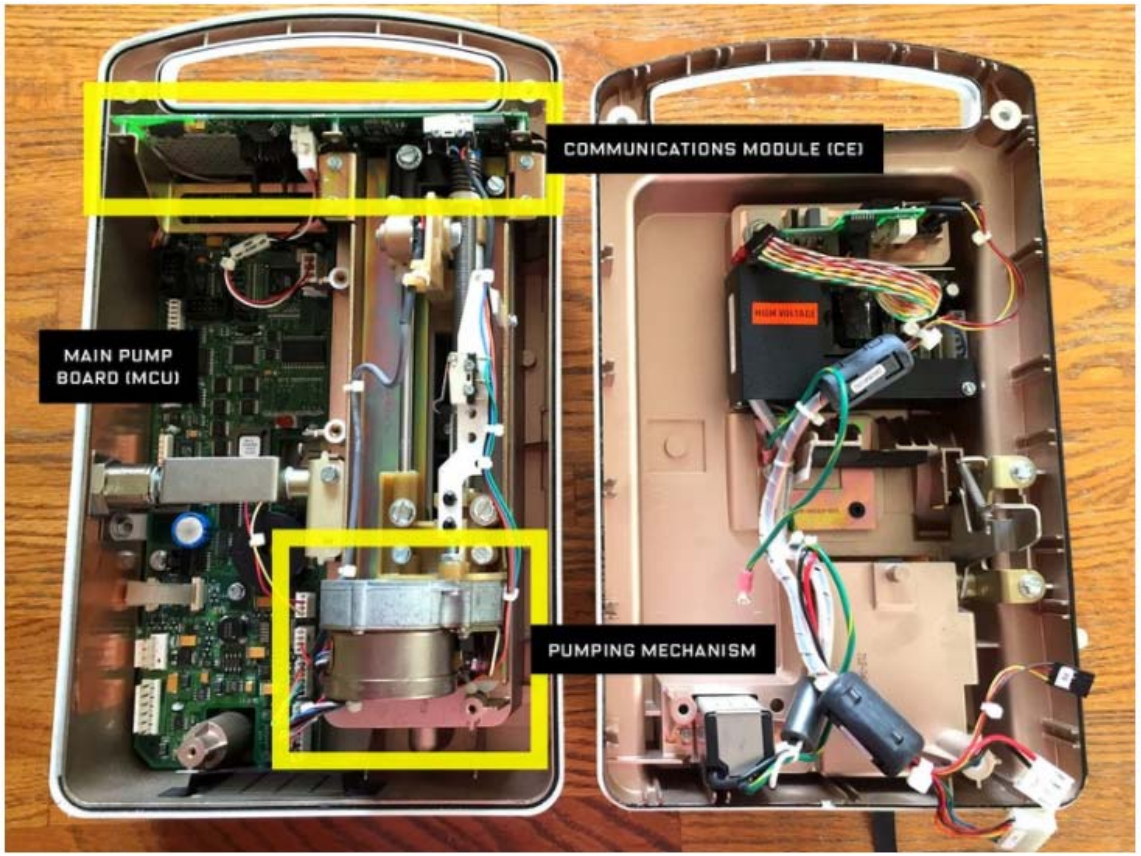
Size of one proteomic snapshot for a single patient:	**10^{-2} terabytes**
Amount of (non-image) data contained in the AHLTA electronic health record for 9.7 million patients today:	**10^{2} terabytes**
Storage space required for a single proteomic snapshot data for those 9.7 million AHLTA patients:	**10^{5} terabytes**
If every US patient who visited a doctors office last year had a proteomic snapshot:	**10^{6} terabytes**
If everyone in the world took a proteomic snapshot every day for a year:	**10^{9} terabytes**
Amount of data that will pass over the internet in 2018:	**10^{9} terabytes**

Managing complexity is hazardous business

- 13,000 diagnoses
- 6,000 drugs
- 4,000 medical procedures
- 1.5 million adverse reactions or Rx errors
- 100,000 deaths per year from medical errors (2009)

Some of the “things” we are inter-networking are in the operating room, in the ambulance (or car), in the medical home, and in your body. It would be good if their messages were both secure and right.

“Drug pump’s security flaw lets hackers raise dose limits”



Wired April 9, 2015; photo by Billy Rios

Perfect protection requires total surveillance[1]

Any alternative is strategically asymmetric

- Offenders only need a new method of attack
- Defenders suffer the cumulative cost off all known modes

Practical enterprise security has "no immitigable surprise"

- Is it realistic (or cost effective) to make failure impossible?
- Rehearsed and reliable recovery may be more attractive

[1] Dan Geer "Tradeoffs in Cyber Security"

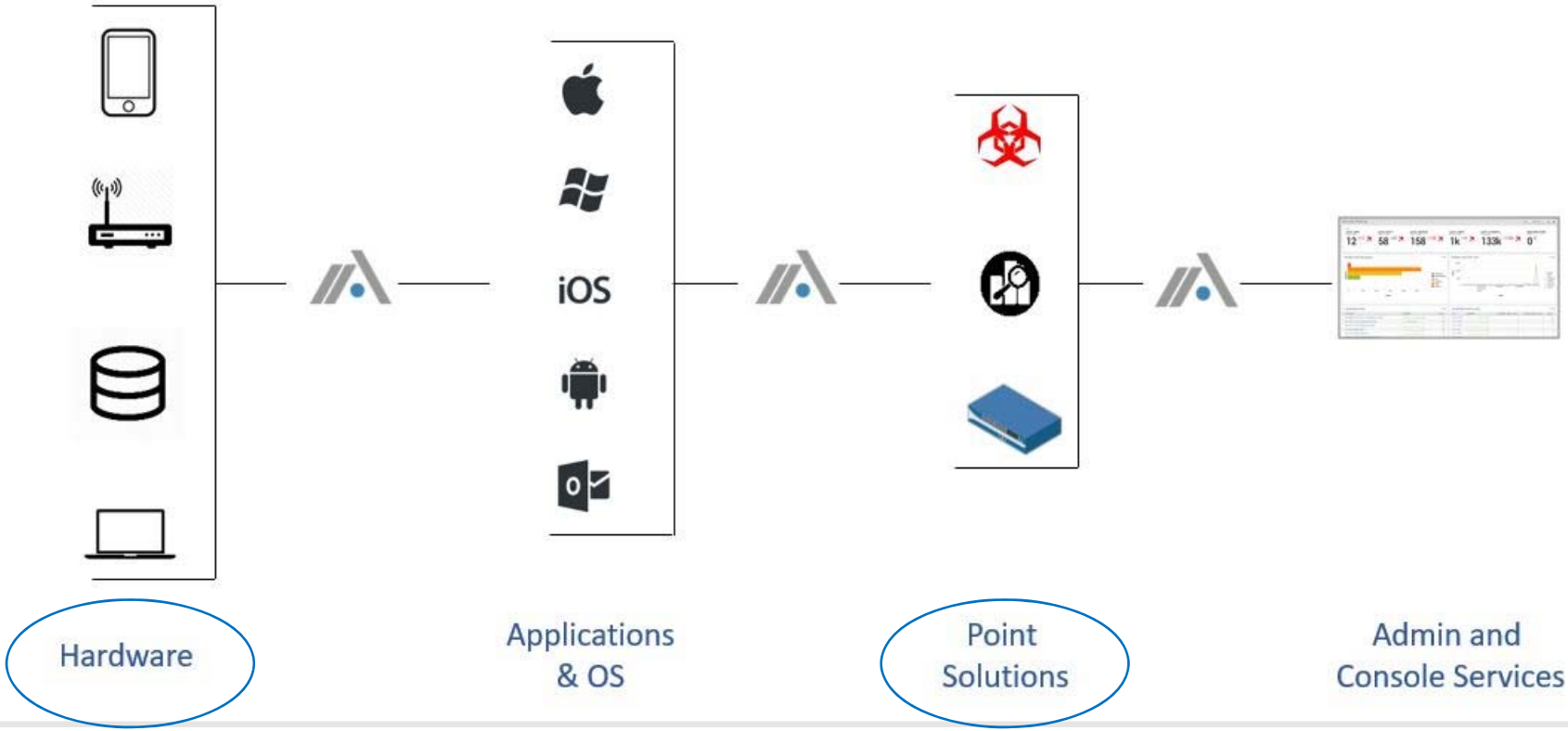
Security is a subset of reliability*

Real-world reliability vs digital security reliability

- Seven nines: aircraft landing
- Six nines: mature manufacturing quality assurance
- Five nines: PSTN availability (after 100 years)
- Four nines: domestic electric energy transmission
- Three nines: maximum possible desktop uptime
- Two nines: credit-card number protection
- One nine: internet traffic not broadly related to attack
- Zero nines: "[a]bility of stock antivirus to find new malware"

*from the article of that name by Geer and Conway, IEEE Security and Privacy, Dec 08

Two examples from cybersecurity

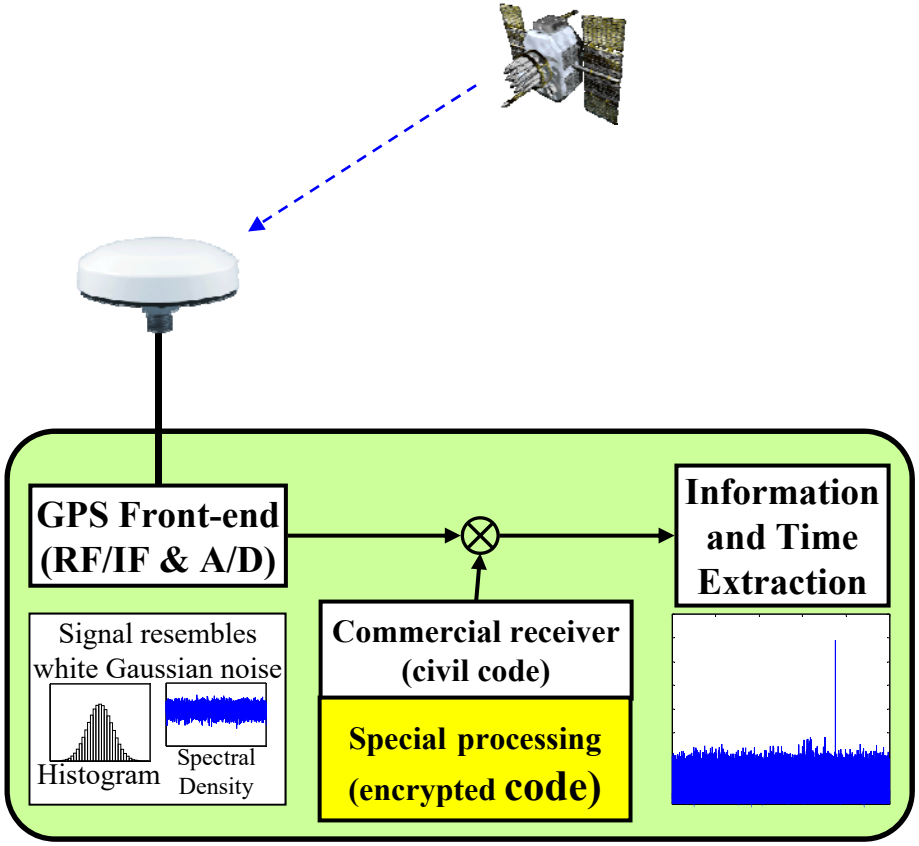


Point solution: location authentication

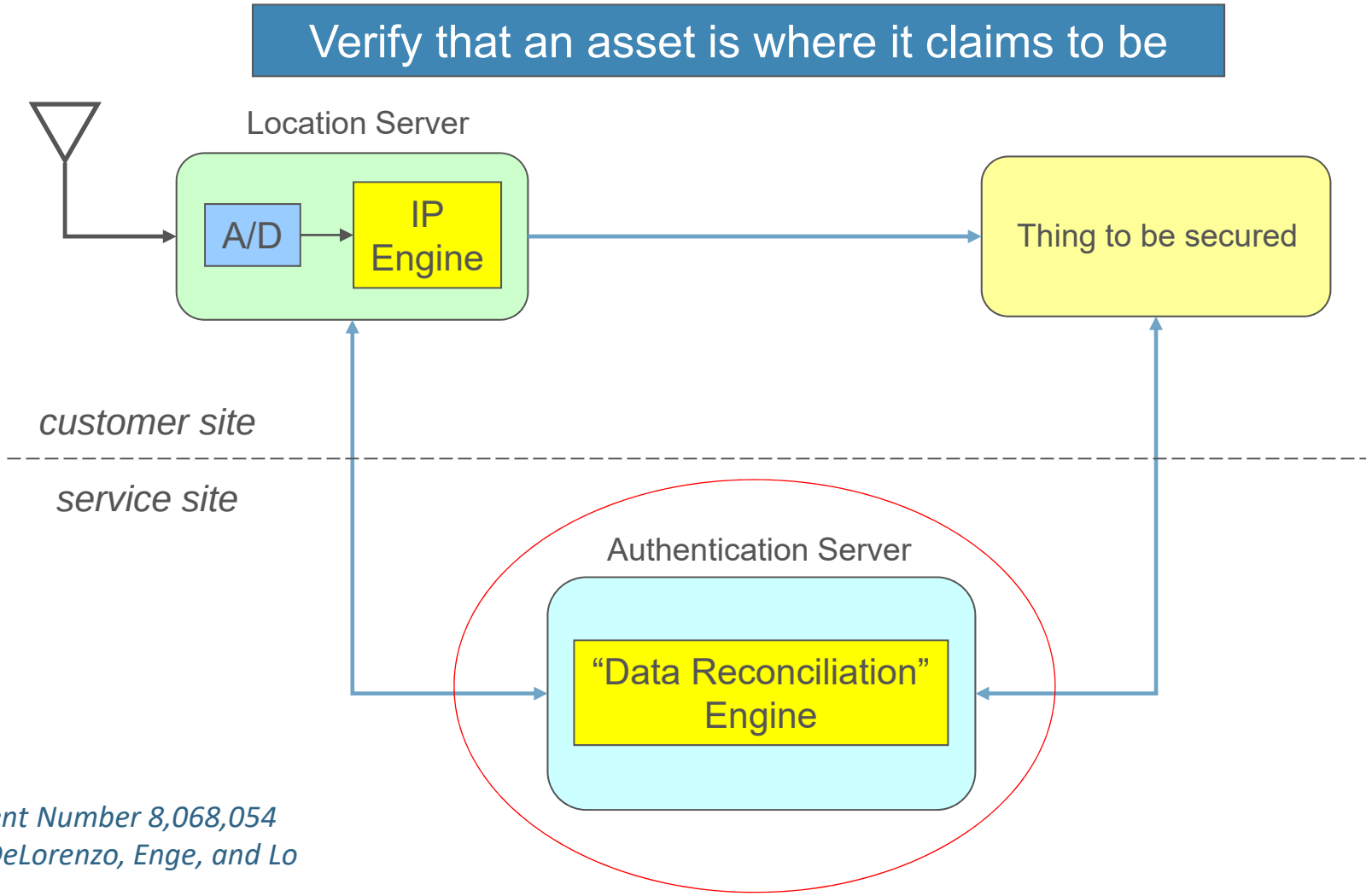
We determined the provenance of the signal without knowing the encryption code

We used these signals to:

- Transmit information securely across open networks
- Determine position and time with high integrity

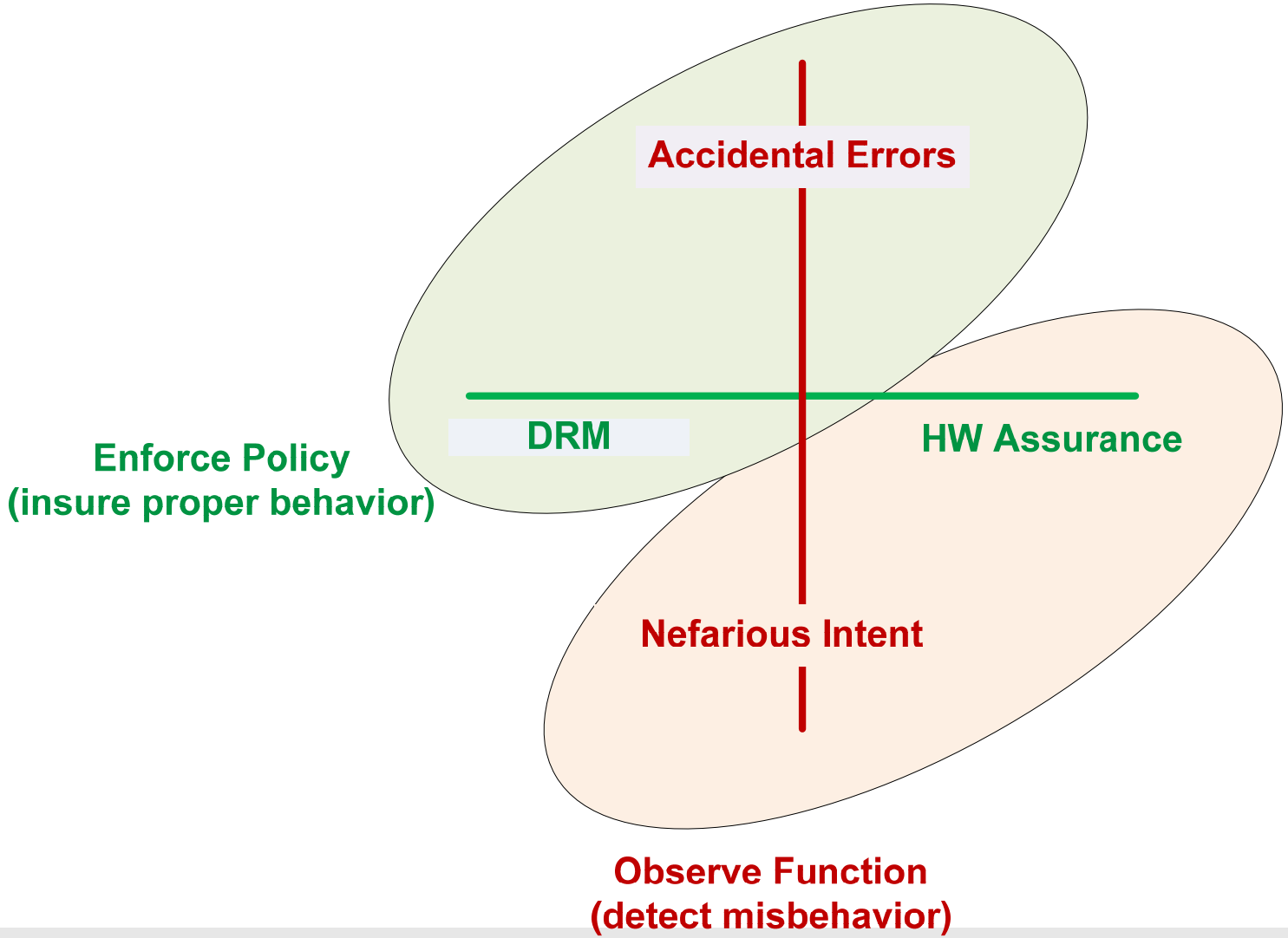


Location-based protection



US Patent Number 8,068,054
Levin, DeLorenzo, Enge, and Lo

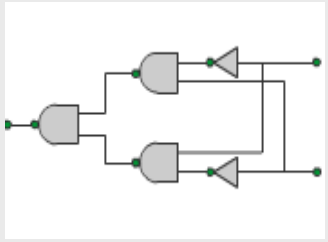
Hardware's axis of evil



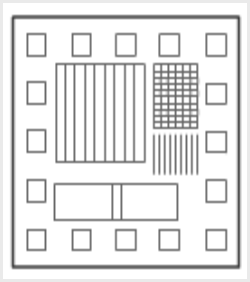
Chip-making in four easy steps

Functional Specification

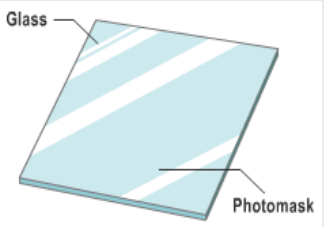
Logic Circuit Design

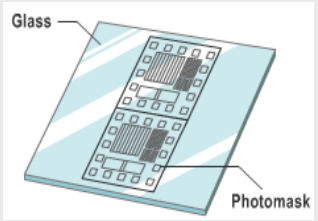


RTL & Layout Design

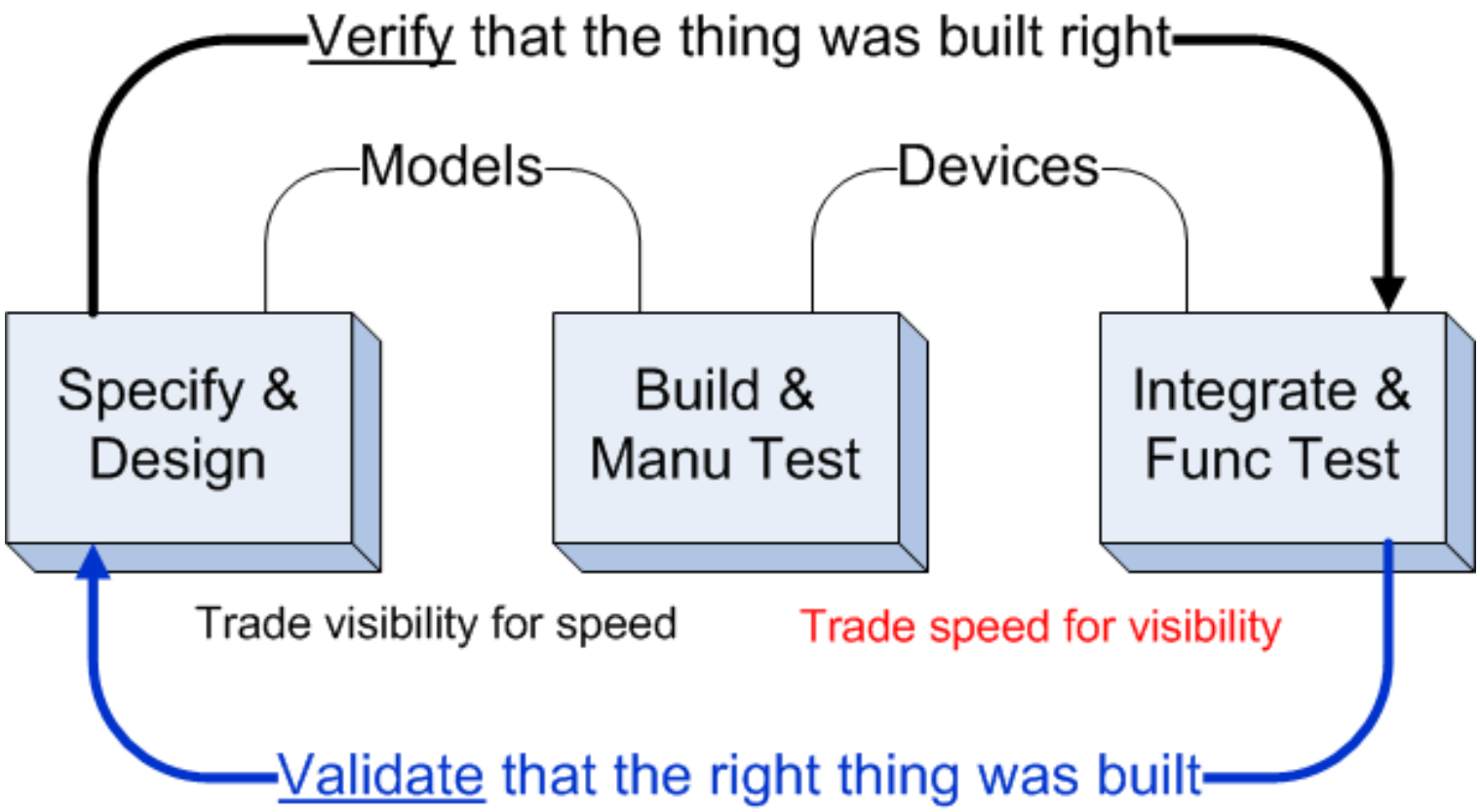


Mask Creation





“Your hands can’t hit what you’re eyes can’t see”

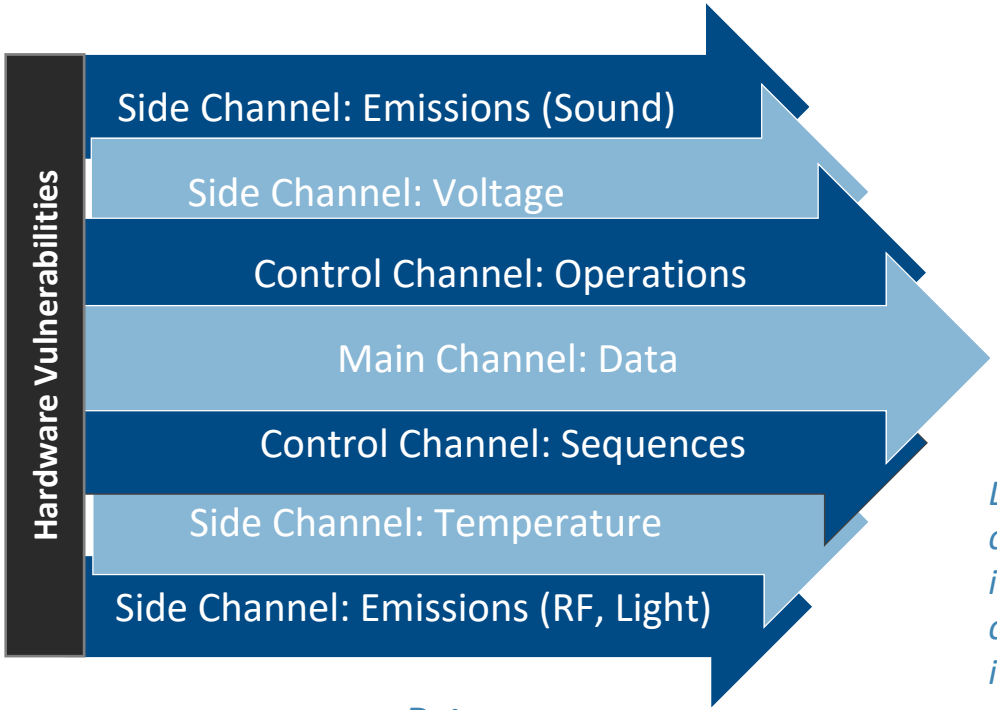


Why at-speed observability matters

Example: 5 billion transaction “boot scenario”

- SW simulation @ 0.01 MHz = 6 days
- HW acceleration @ 0.1MHz = 14 hours
- At-speed @ 500 MHz = 10 seconds

Control systems are inherently vulnerable



Data Sources

Detect anomaly; classify TTPs; identify infected components and impact of attack

Attack Details

- Detection Location, Type, Value, Corruption Field

Classification

- Data Leaker
- Behavior Modification
  - Denial of Service
  - Takeover
- Reliability

Localization

- Memory
- CPU
- Busses
- Input

Impact

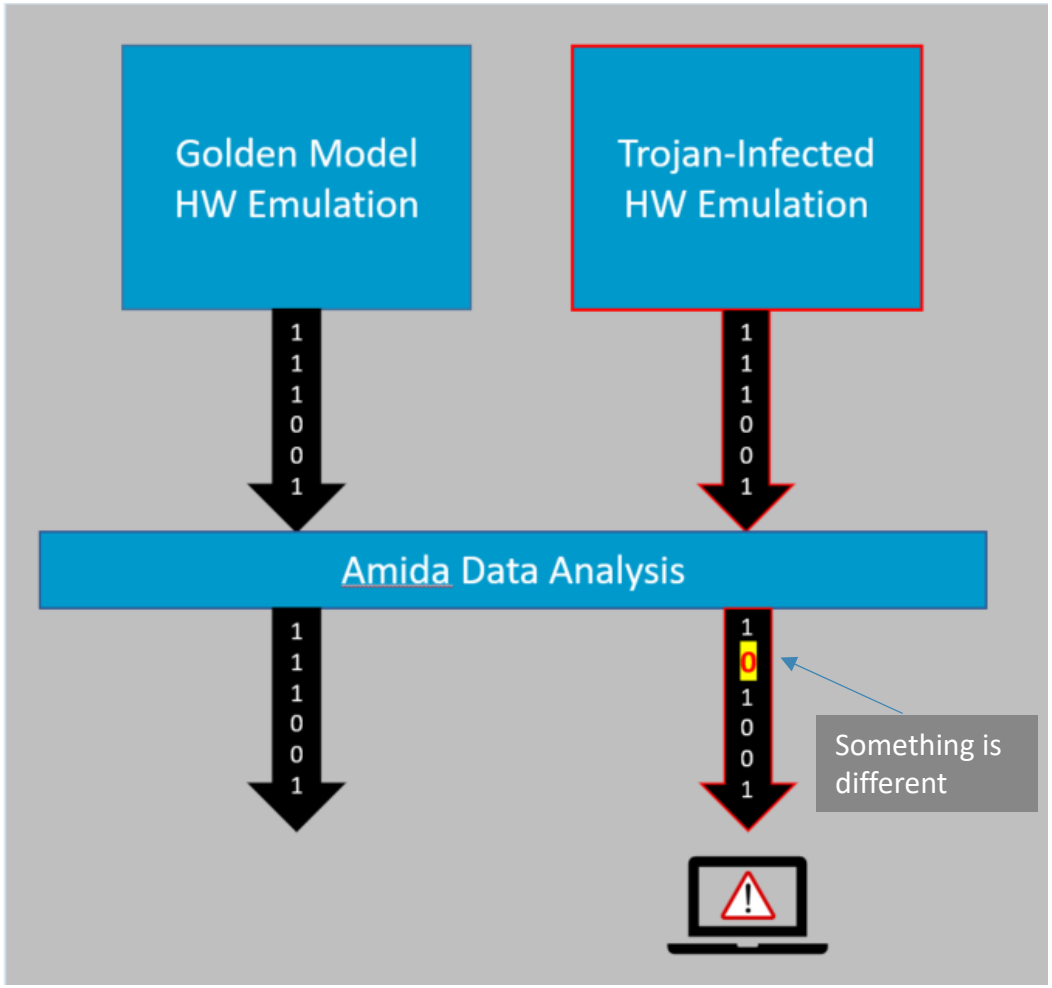
- Nuisance
- Damaging
- Destructive
- Catastrophic

Goal: Identify, classify, and localize the attack

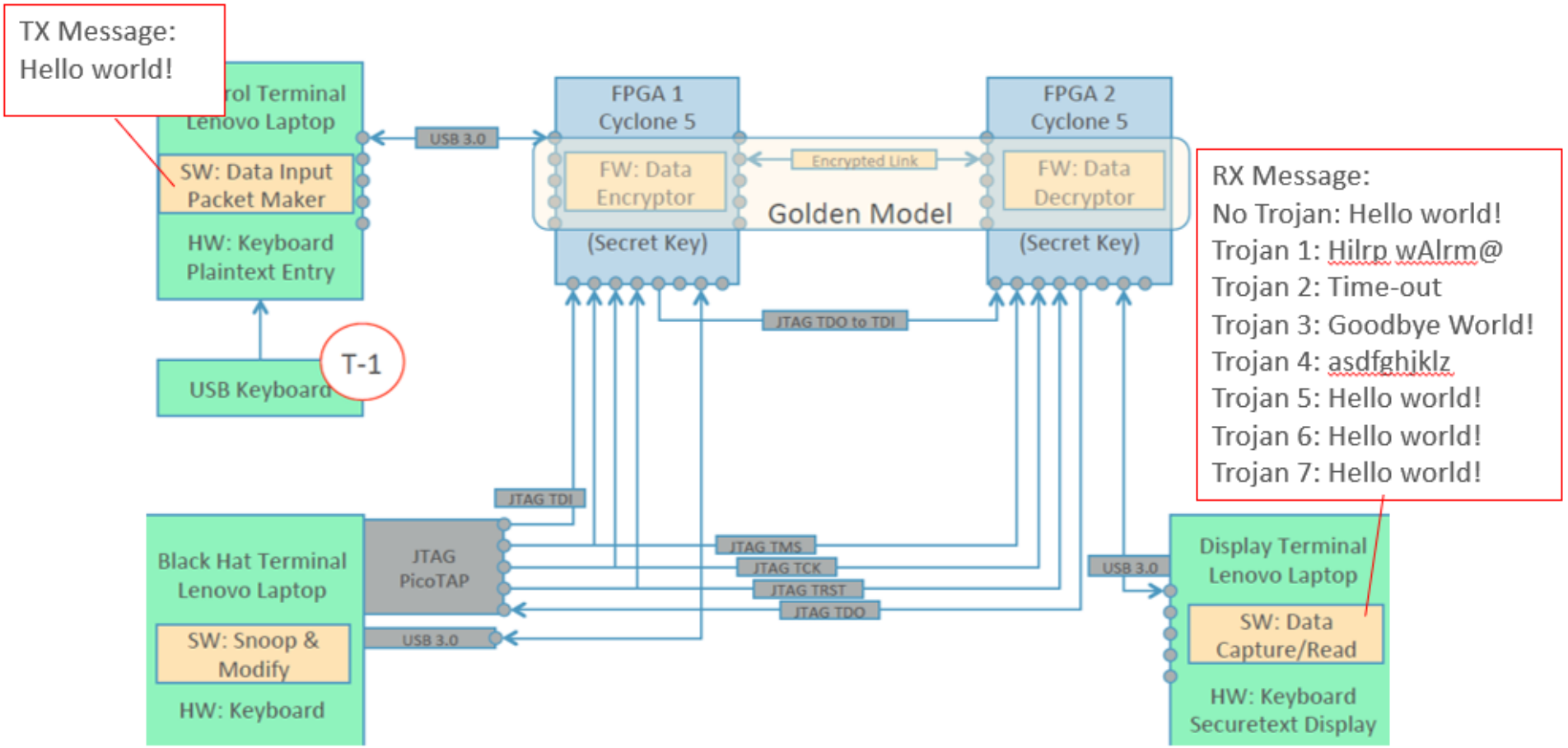
A proof of concept (for the Navy)

Basic idea

1. Emulate a system on FPGA boards
2. Insert Trojans into that system
3. Collect data from emulated system and detect anomalies
4. Figure out what change could have caused the difference



Detailed Hardware Emulation



Amida customizes, configures, and installs data integrity and interoperability components on an *open source* infrastructure platform

Lower total cost of ownership
no license fees and often faster to install and configure

No vendor-lock
any qualified developer can maintain the system

Better application security
more developers checking for vulnerabilities

Easier maintenance
access to the source code and platform service

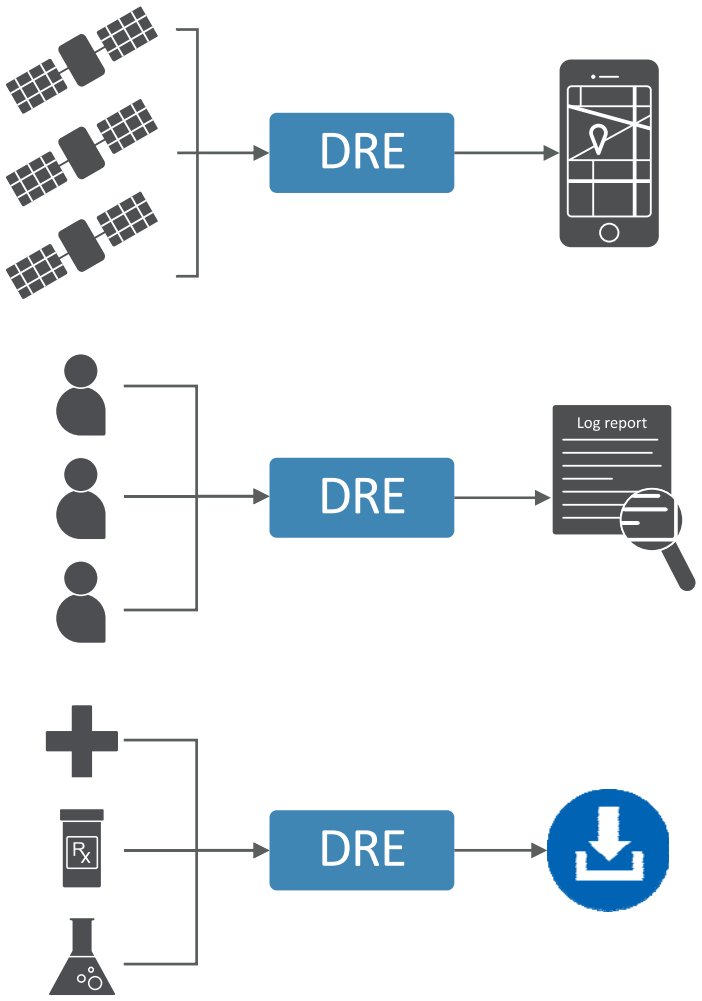
Data reconciliation is at the heart of cybersecurity

The basic questions:

- Where is the data coming from?
- How reliable or noisy is it?
- How do you know you're right?

IoT considerations:

- Hardware assurance
- Network and software security
- Special care for safety-of-life



Thank you

Peter L. Levin
Co-founder and CEO
peter@amida-tech.com