SAND2011-3427C

Demythifying Cybersecurity*

A glimpse of a secure cyber future

Edward B. Talbot

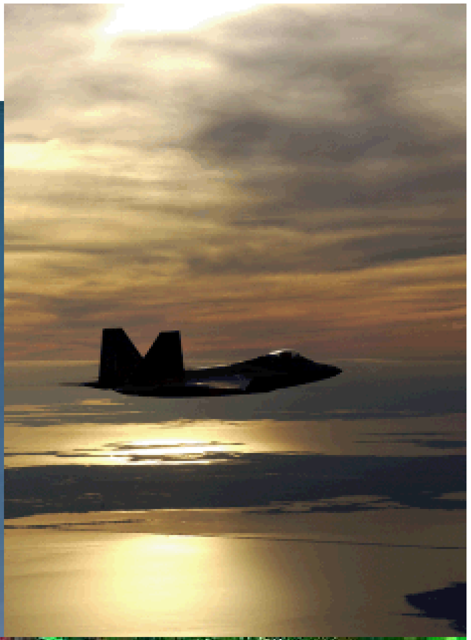
Tom M. Kroeger

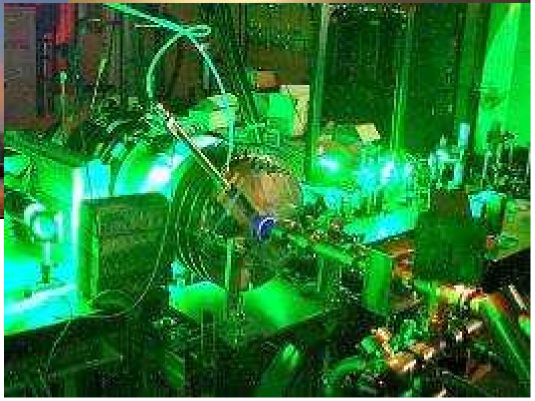
Sandia National Laboratories

Livermore, CA

* - http://doi.ieeecomputersociety.org/10.1109/MSP.2010.95

Sandia has been dedicated to national security since 1949





A Mission-Driven Laboratory:

- Design and development of nonnuclear portions of US nuclear weapons
- Production of advanced components
- Safety, security, use control
- Treaty verification, nonproliferation, and counterproliferation
- Advanced military technologies and applications
- Energy and environment
- Homeland security and countering weapons of mass destruction

On the Internet nobody knows you're a dog…

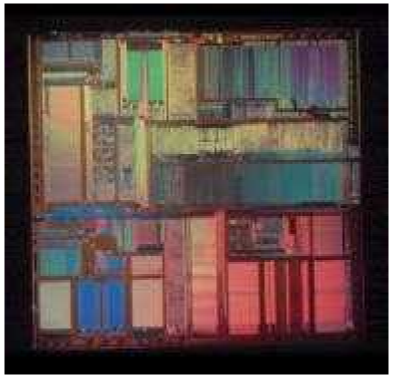
…or an adversary!

The problem: we can't trust our machines and we can't live without them.

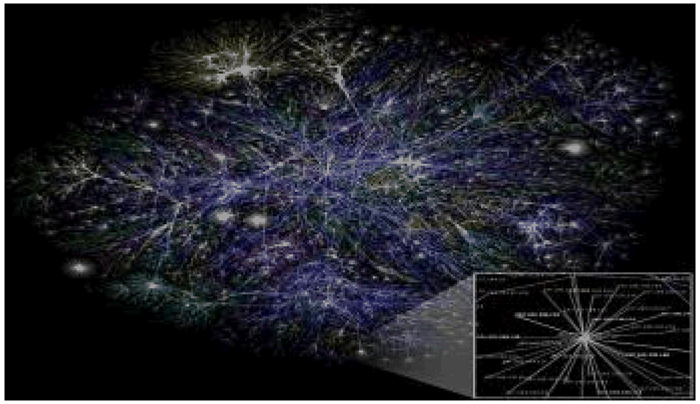
Information systems have become too complex and too interconnected at all scales to ensure that they do not contain vulnerabilities.

- Multi-scale: micro (3 lines of code) -> human -> macro (Internet)
- Multi-discipline: device physics -> electronics -> computer architecture -> software -> human factors
- Multi-medium: photons -> electrons -> RF

- Wafer
- Mask
- Programming
- Die



→



- Servers
- Routers
- Switches
- Fiber
- Firewalls
- Desktops
- Users

…we are behind and falling further behind.

Cybersecurity Manifesto

- The Situation
  - Current cyber security approaches are fundamentally broken.
  - Current cyber security strategies are reactive and asymmetric.
  - Vulnerabilities in current implementations are virtually limitless.
  - Threats are exploiting these vulnerabilities faster than we can detect and counter them.
  - Current cyber security implementations compound the problem by creating the illusion of security.

"We cannot solve our problems with the same thinking we used when we created them."

- Albert Einstein

“The great enemy of the truth is very often not the lie, deliberate, contrived and dishonest, but the myth, persistent, persuasive and unrealistic.”

- John F. Kennedy

- Some Myths
  - **Myth 1:** More layers of defense are better.
  - **Myth 2:** Burdensome security is good security.
  - **Myth 3:** Running my executables on my data on my system is secure because I control my system.
  - **Myth 4-…:** ???

We need to move cyber security from a craft/lore/myth to a scientific discipline.

Craft/Lore/Myth		Science	
Reactive	Trial-and-error Rules of Thumb Skill- / luck-based	Theory Experiment Modeling and Simulation	**Predictive**

An example

Alchemy	*Chemistry*
Earth, Air, Fire, Water	Periodic Table
Qualitative Assertions	***Quantitative Assertions***

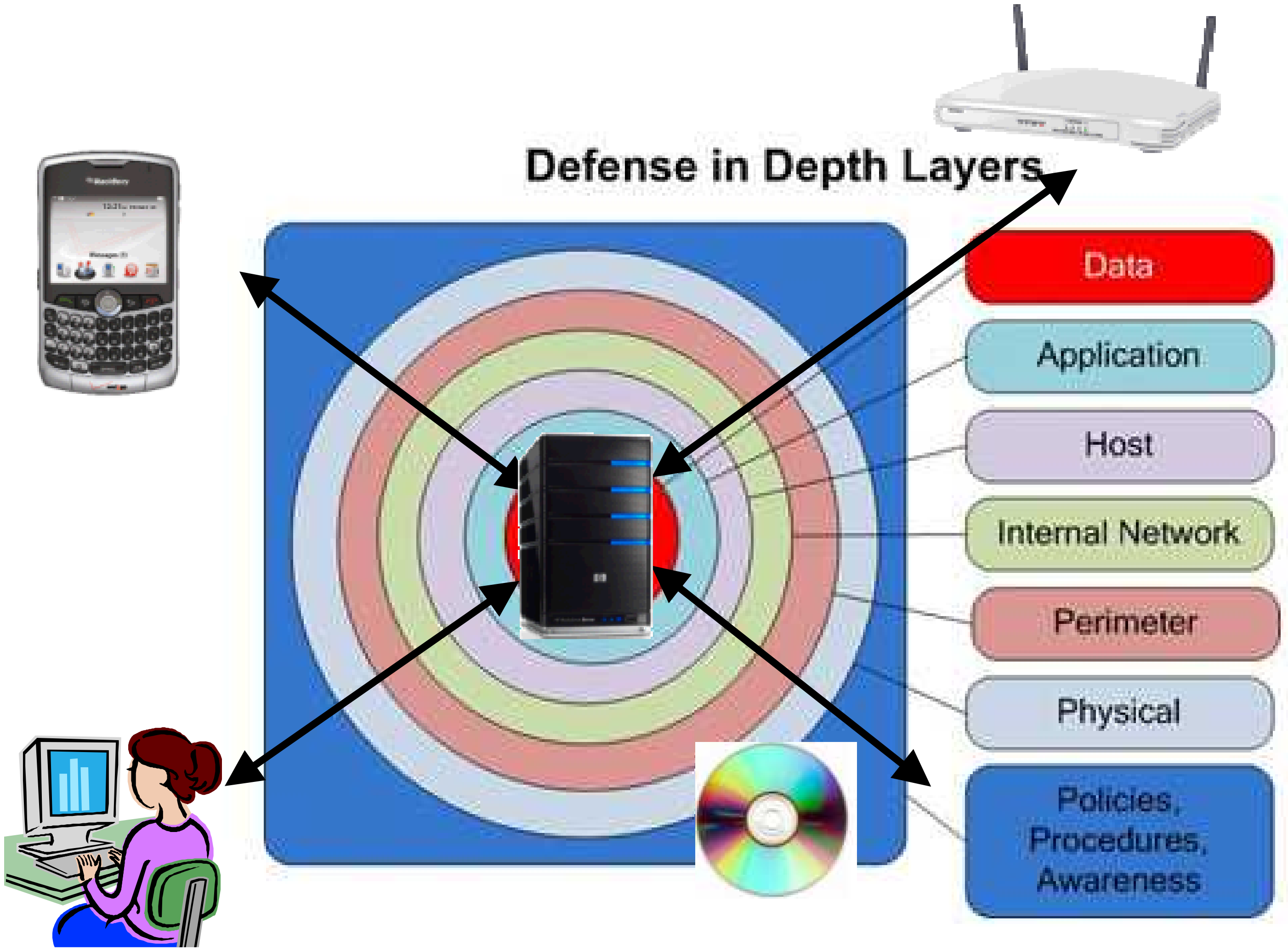
"The highest priority should be assigned to establishing research protocols to enable reproducible experiments…There is a science of cyber-security."

- Science of Cyber-Security, JASONs report dtd November 2010.

Myth 1: More layers of defense are better.

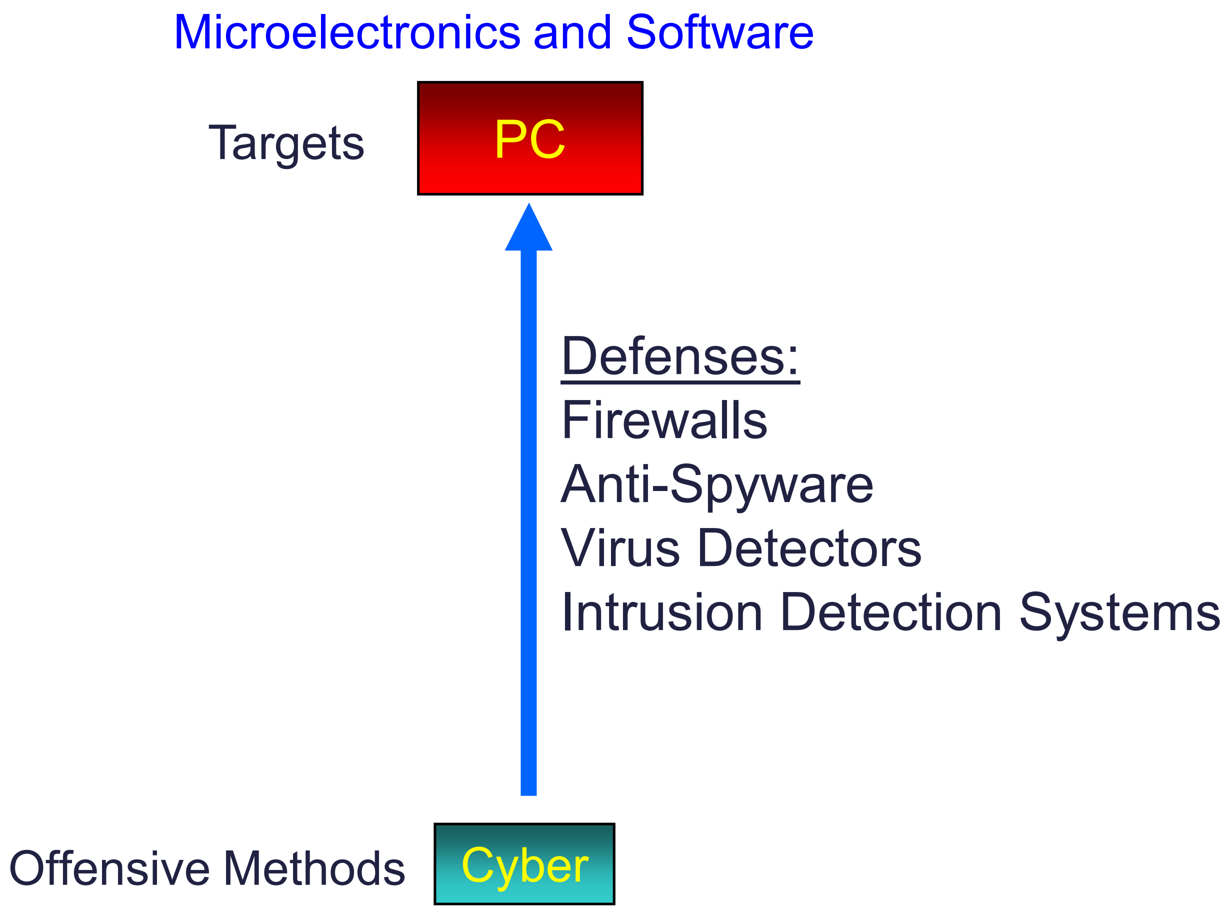
Layered defense is great for
physical assets

Myth 1: More layers of defense are better.

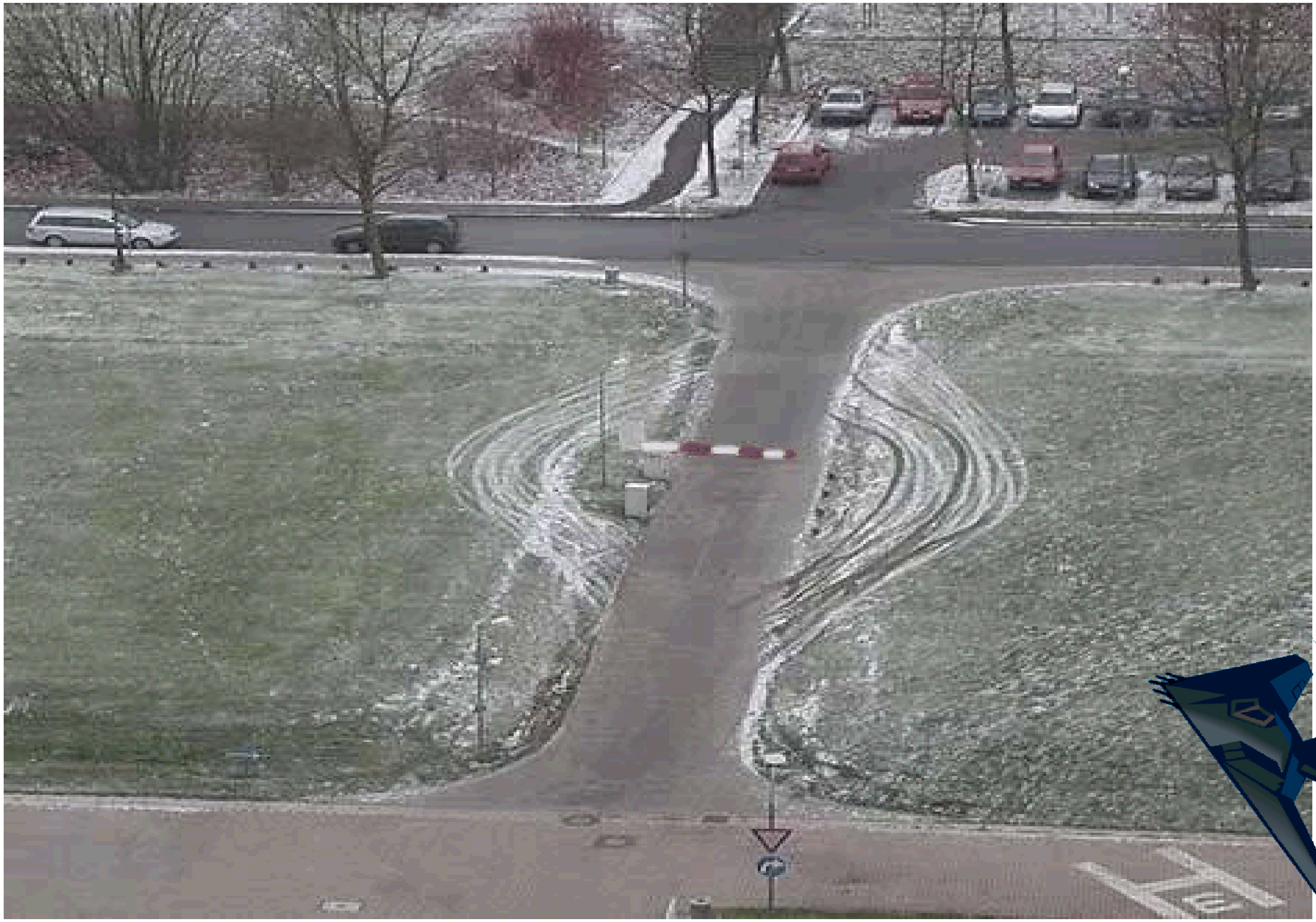


Layered defense creates the illusion of impenetrability

A common perception of the threat



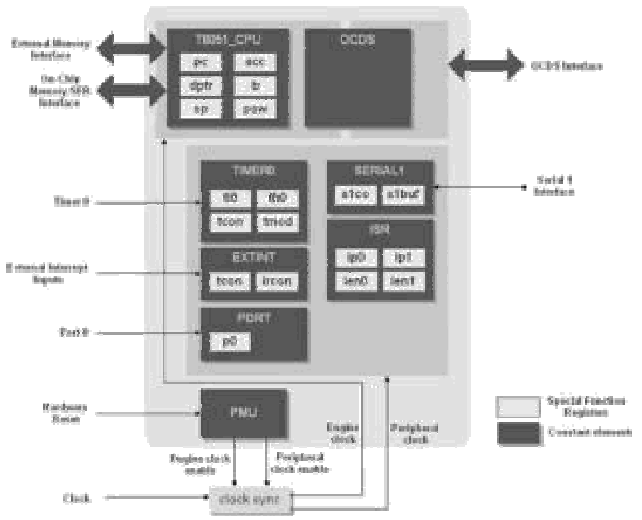
Many threats are not obvious



Myth 1: More layers of defense are better.

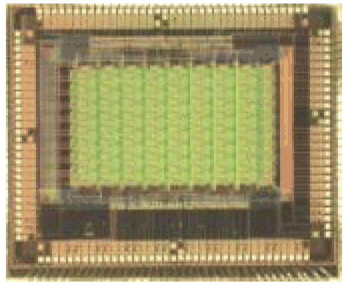
Response 1: Science-Based Cyber Security

VHDL

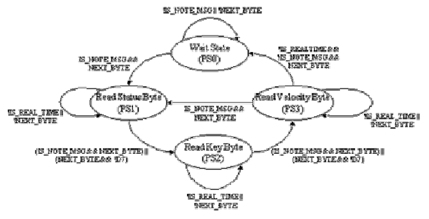


C compiler

FPGA – 500k logic elements



Lots of states, lots of flexibility, lots of trouble.



MIDI Parser State Diagram

Few states, testable, ***provable***.

“Direct-to-gates” compiler

Myth 1: More layers of defense are better.

Response 1: Science-Based Cyber Security

Myth 2: Burdensome security is good security.

- Increasing security burden
  - User-selected passwords to constrained passwords
  - 2 factor: constrained passwords *plus* HSPD-12 badge
  - 3 factor: constrained passwords *plus* HSPD-12 badge *plus* fingerprint
- Are we more secure?
  - Can we *PROVE* that we are more secure?
- Looking forward:
  - Identity 2.0: Human-BadgeΞMachine-Environment
  - Identity 3.0: HumanΞEnvironment

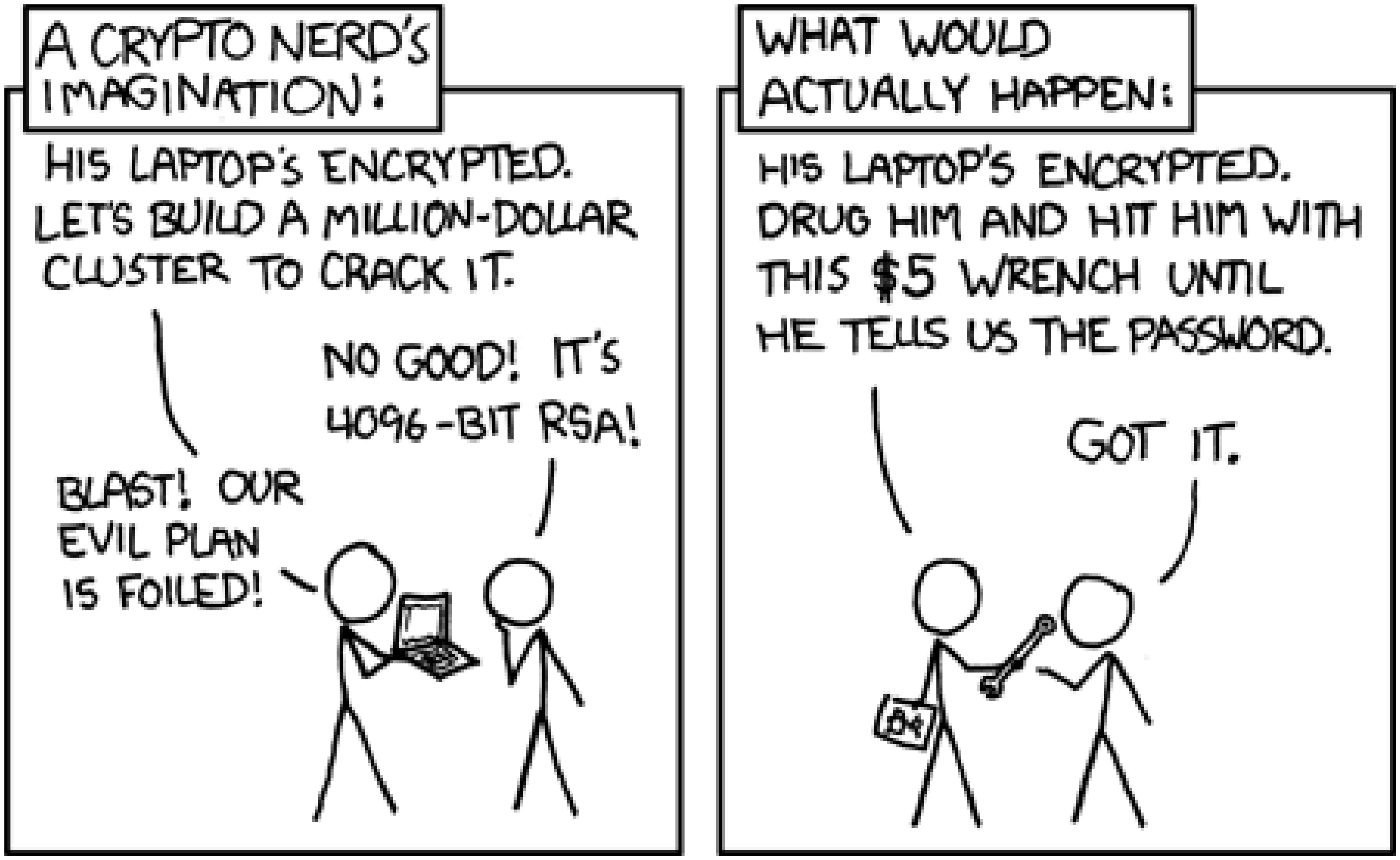
e.g. Strong Kerberos

+

+

Myth 2: Burdensome security is good security.

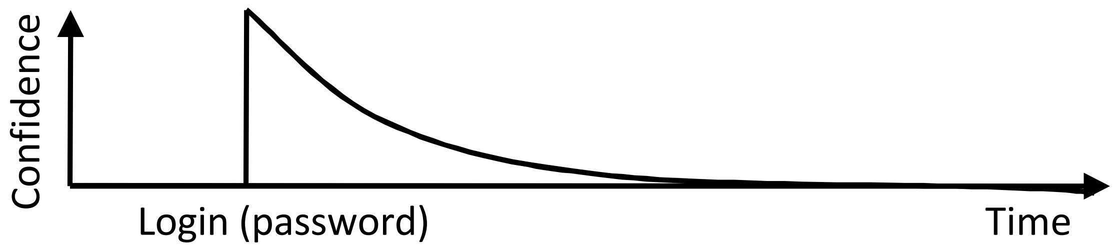
Rethinking our security approach.


A CRYPTO NERD'S IMAGINATION:
HIS LAPTOP'S ENCRYPTED. LET'S BUILD A MILLION-DOLLAR CLUSTER TO CRACK IT.
NO GOOD! IT'S 4096-BIT RSA!
BLAST! OUR EVIL PLAN IS FOILED!
WHAT WOULD ACTUALLY HAPPEN:
HIS LAPTOP'S ENCRYPTED. DRUG HIM AND HIT HIM WITH THIS $5 WRENCH UNTIL HE TELLS US THE PASSWORD.
GOT IT.

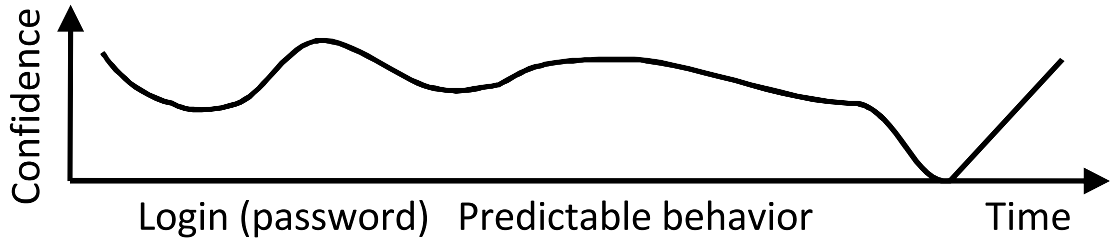
Myth 2: Burdensome security is good security.

Continuous, adaptive identity authentication

- **Event-based identity authentication** is momentary (event-based)



- **Continuous, adaptive identity authentication** is a continuous process
  - Probabilistic (not deterministic)
  - Approach: Multi-sensor fusion (example: Kalman filter using GPS, IMU, control laws, galvanic skin response, real-time DNA analysis, etc.)



Effective authentication requires unambiguous identity.

Myth 2: Burdensome security is good security.

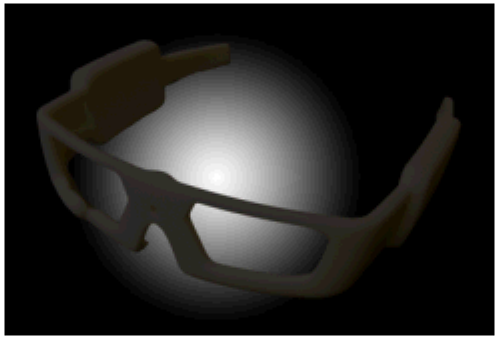
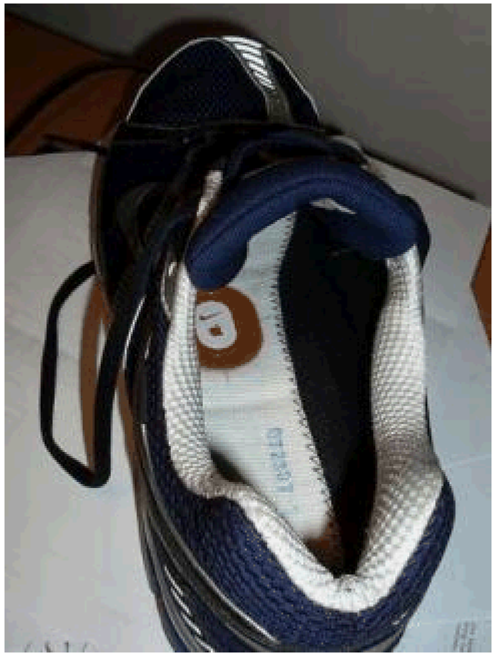
Continuous, adaptive authentication provides unambiguous identity regardless of dynamics.

If a control system can be built that enables this aircraft to return to base…

…a control system should be able to authenticate me despite changes in my dynamics

Myth 2: Burdensome security is good security.

“Cell phones show human movement predictable 93% of the time”*

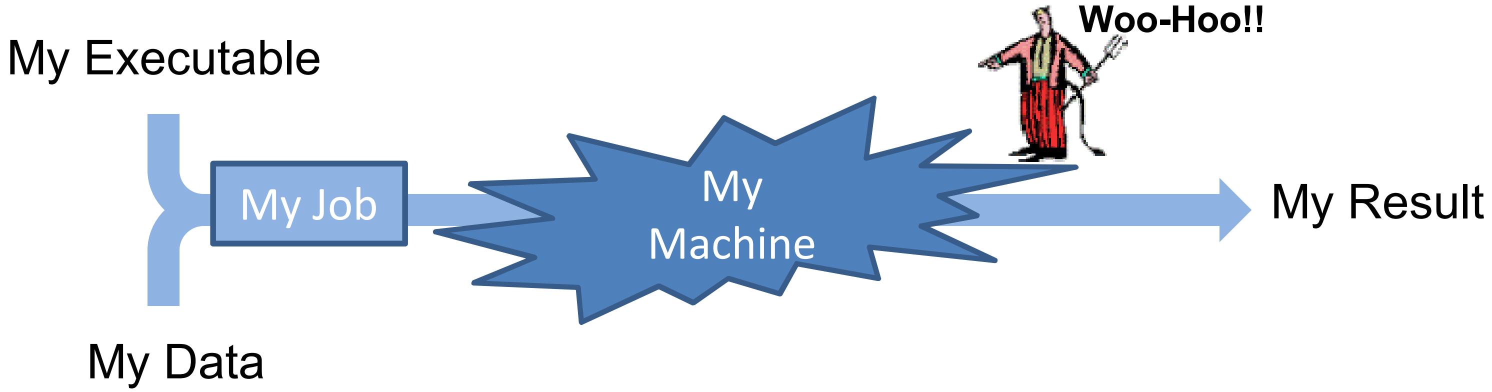
- INTEGRATION of existing sensors
  - ✓ Eyes
  - ✓ Gait (feet, waist)
  - ✓ GPS location
  - ✓ Voice
- to provide
  - ✓ Continuous
  - ✓ Real-time
  - ✓ Adaptive
  - ✓ Unambiguous
- identity authentication

* - http://arstechnica.com/science/news/2010/02/cell-phones-show-human-movement-predictable-93-of-the-time.ars

Myth 2: Burdensome security is good security.

Response 2: Unambiguous identity as certain and intuitive as in the physical world.

Myth 3: Running my executables on my data on my system is secure because I control my system.



Myth 3: Running my executables on my data on my system is secure because I control my system.

Cyber-attackers exploit complexity

- **The asymmetry:**
  - **Defense:** protect against every possible exploit (hard).
  - **Attack:** find one unprotected vulnerability (easy).
    - Linux kernel: 25 year old bug in the kernel was found two years ago.
    - Vista rewrite: 6 major vulnerabilities identified in the first 3 months.

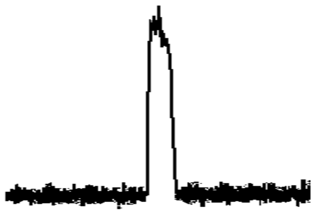
- **Response 3: Reverse the asymmetry**
  - **Defense:** easy.
  - **Attack:** hard

- **Approach:** tailor complexity for defense.

"We cannot solve our problems with the same thinking we used when we created them." ***- Albert Einstein***

Myth 3: Running my executables on my data on my system is secure because I control my system.

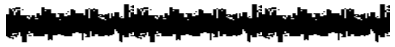
Response 3: Reversing the asymmetry



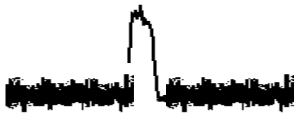
Data Encryption:
Fragile, Incomplete,
easy to detect, crack

Data Obscuration:
("Concealment")
Robust,
computationally hard

The Myth:

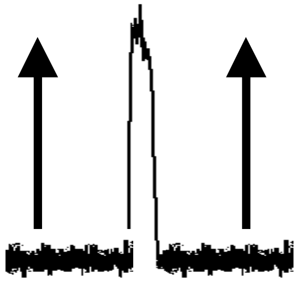


The Reality:



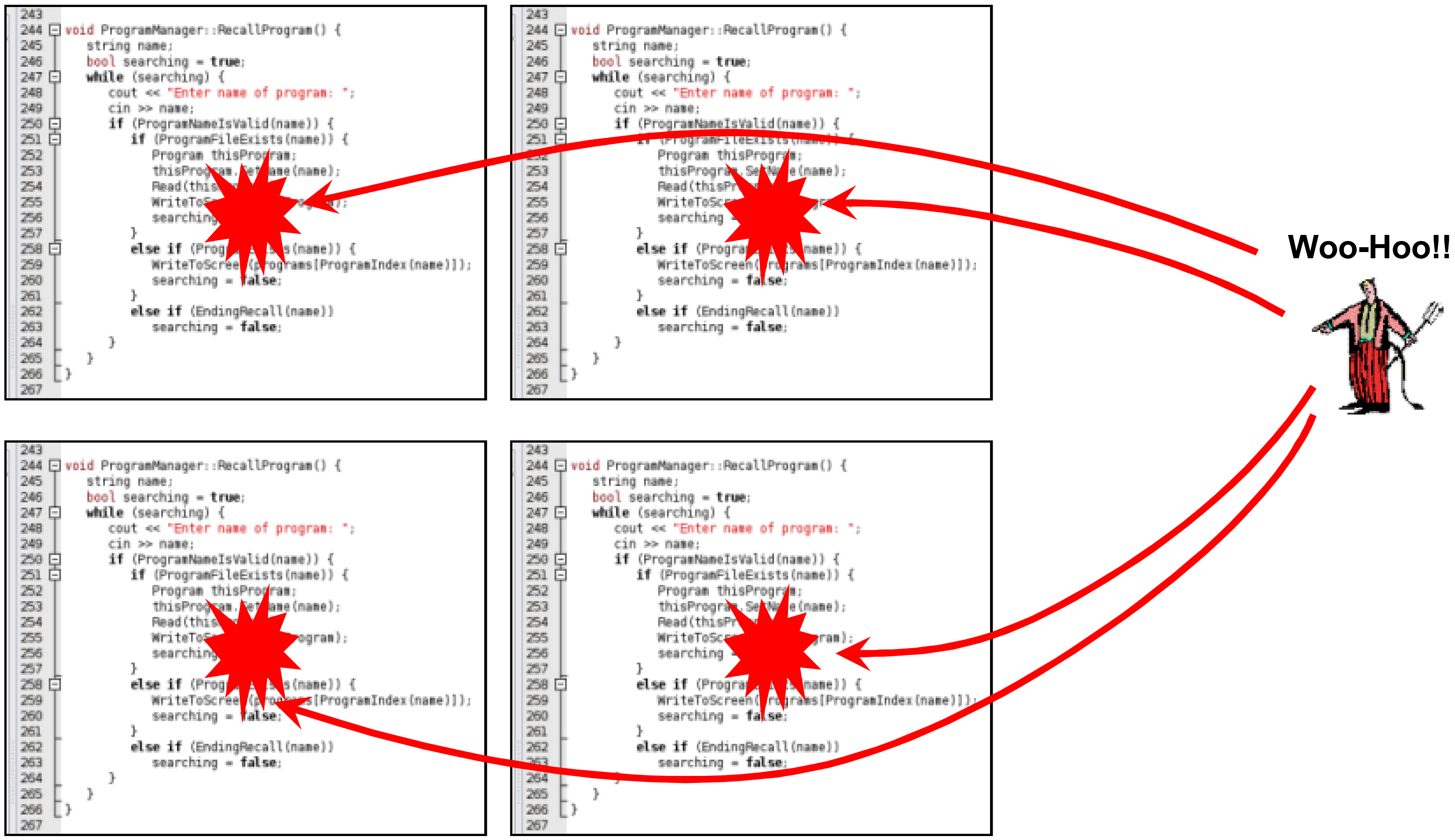
"First, there are three general types of secrecy system:
(1) concealment systems,…
(2) privacy systems,…
(3) cipher, code…"

- From *Communication Theory of Secrecy Systems*, 1949, C. Shannon



Myth 3: Running my executables on my data on my system is secure because I control my system.

Monoclonal implementations share security holes.

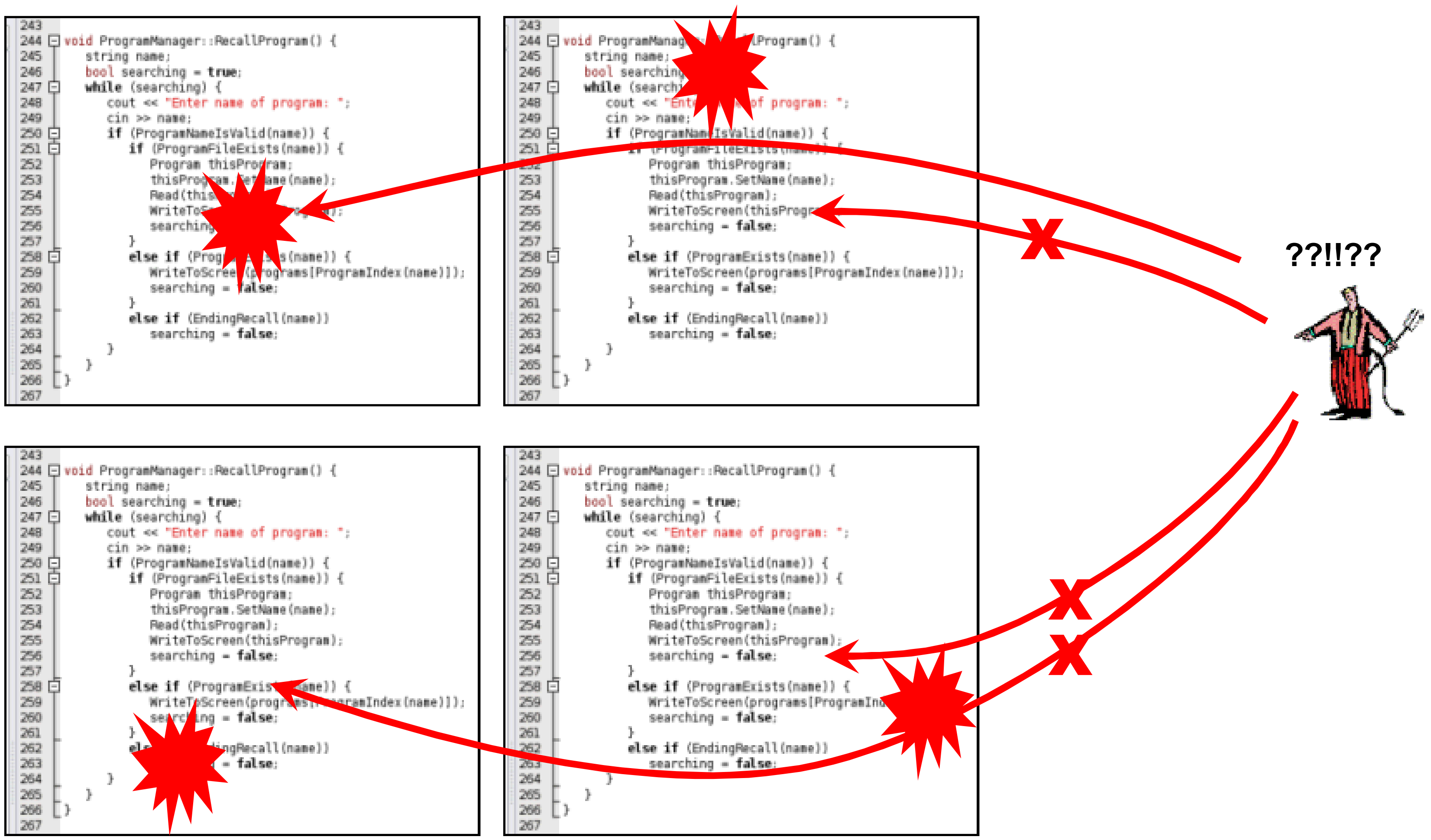


```
void ProgramManager::RecallProgram() {
    string name;
    bool searching = true;
    while (searching) {
        cout << "Enter name of program: ";
        cin >> name;
        if (ProgramNameIsValid(name)) {
            if (ProgramFileExists(name)) {
                Program thisProgram;
                thisProgram.SetName(name);
                Read(this[illegible]
                WriteToS[illegible]gram);
                searching[illegible]
            }
            else if (Progra[illegible]s(name)) {
                WriteToScreen(programs[ProgramIndex(name)]);
                searching = false;
            }
            else if (EndingRecall(name))
                searching = false;
        }
    }
}
```

```
void ProgramManager::RecallProgram() {
    string name;
    bool searching = true;
    while (searching) {
        cout << "Enter name of program: ";
        cin >> name;
        if (ProgramNameIsValid(name)) {
            if (ProgramFileExists(name)) {
                Program thisProgram;
                thisProgram.SetName(name);
                Read(this[illegible]
                WriteToS[illegible]gram);
                searching[illegible]
            }
            else if (Progra[illegible]s(name)) {
                WriteToScreen(programs[ProgramIndex(name)]);
                searching = false;
            }
            else if (EndingRecall(name))
                searching = false;
        }
    }
}
```

Myth 3: Running my executables on my data on my system is secure because I control my system.

Multiple implementations randomize security holes.

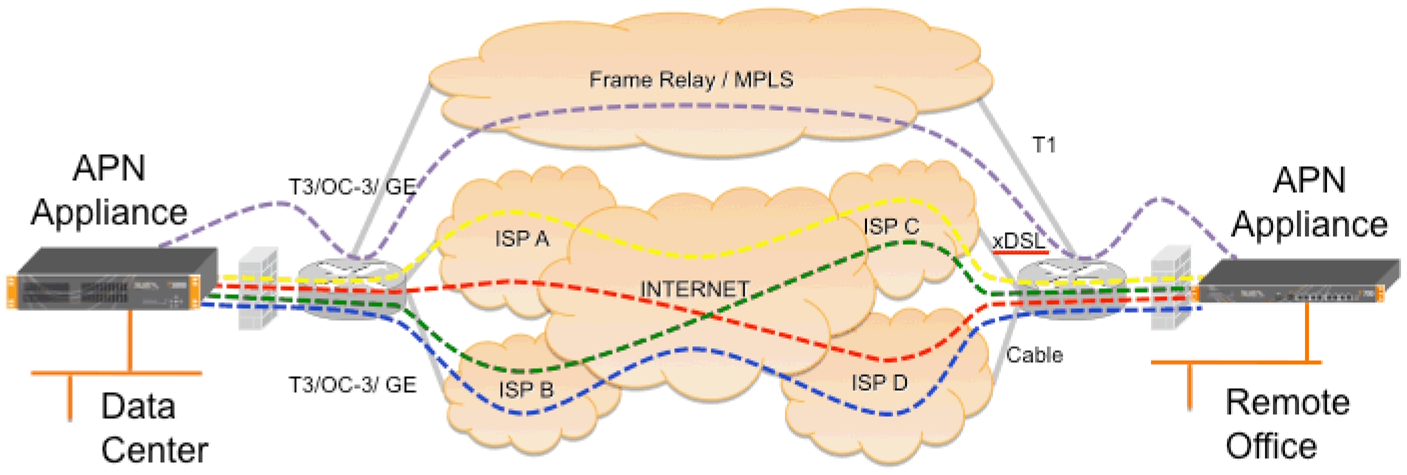


```
void ProgramManager::RecallProgram() {
    string name;
    bool searching = true;
    while (searching) {
        cout << "Enter name of program: ";
        cin >> name;
        if (ProgramNameIsValid(name)) {
            if (ProgramFileExists(name)) {
                Program thisProgram;
                thisProgram.SetName(name);
                Read(thisProgram);
                WriteToScreen(thisProgram);
                searching = false;
            }
            else if (ProgramExists(name)) {
                WriteToScreen(programs[ProgramIndex(name)]);
                searching = false;
            }
            else if (EndingRecall(name))
                searching = false;
        }
    }
}
```

Multiple-version codes enable security improvement statistics.

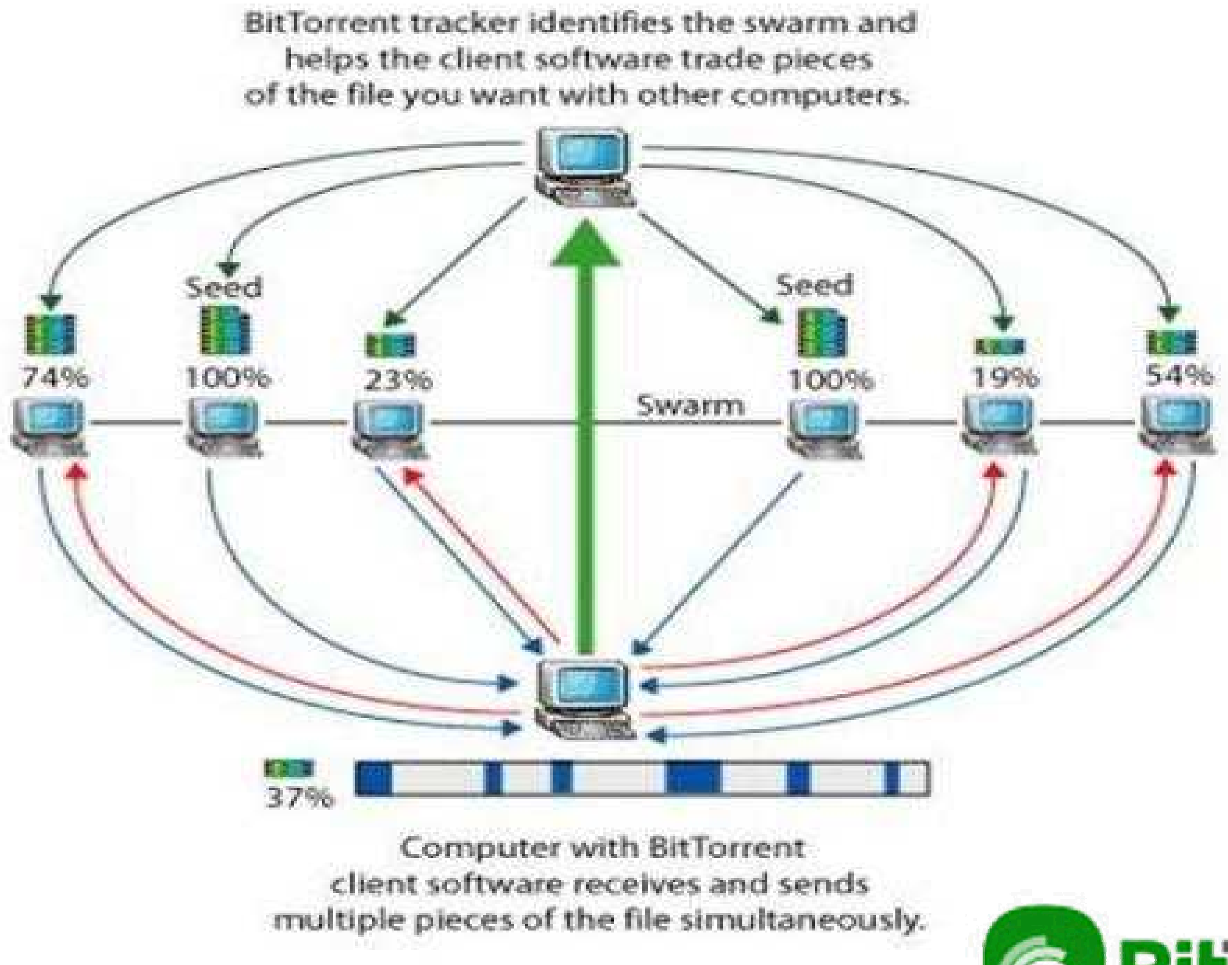
Multiple computing implementations can randomize security vulnerabilities.

Multiple communication paths can randomize security vulnerabilities.



TALARI NETWORKS

Multiple storage locations can randomize security vulnerabilities.


BitTorrent tracker identifies the swarm and helps the client software trade pieces of the file you want with other computers.
Seed
Seed
74%
100%
23%
100%
19%
54%
Swarm
37%
Computer with BitTorrent client software receives and sends multiple pieces of the file simultaneously.

BitTorrent™

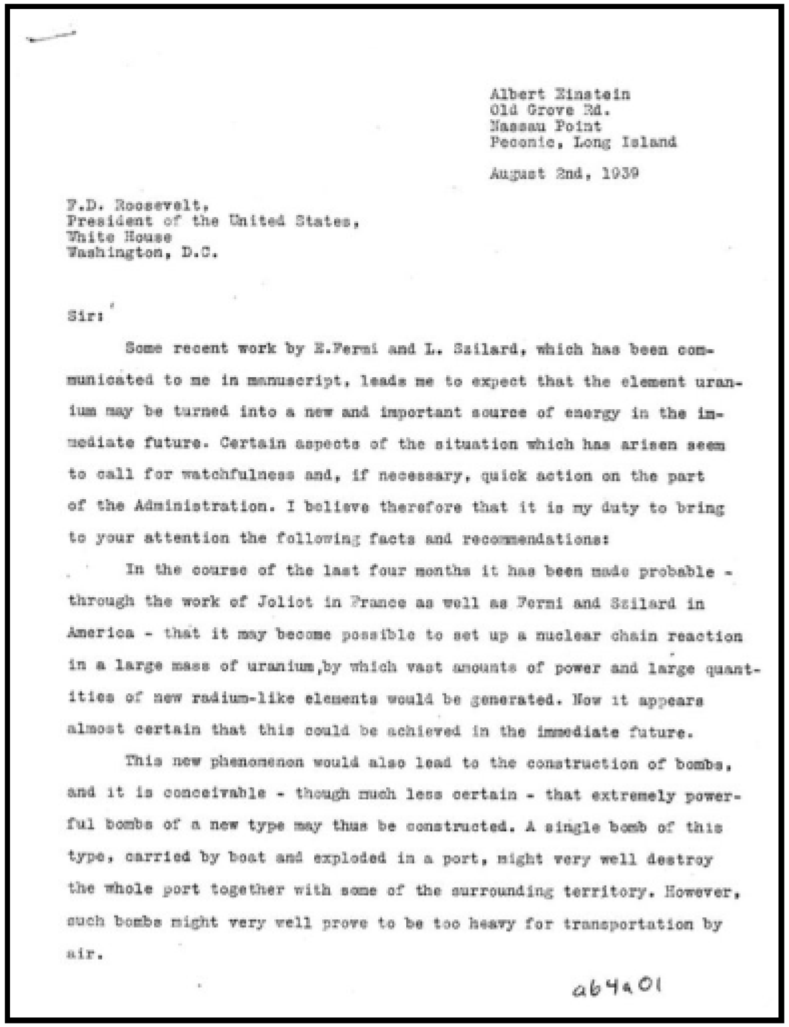
Myth 3: Running my executables on my data on my system is secure because I control my system.

Response 3: Reverse the asymmetry

A Challenge

From the "Einstein-Roosevelt" letter:

"Some recent work by E. Fermi and L. Szilard, which has been communicated to me in manuscript, leads me to expect that the element uranium may be turned into a new and important source of energy in the immediate future. Certain aspects of the situation which has arisen seem to call for watchfulness and if necessary, quick action on the part of the Administration. I believe therefore that it is my duty to bring to your attention the following facts and recommendations…"



Albert Einstein
Old Grove Rd.
Nassau Point
Peconic, Long Island

August 2nd, 1939

F.D. Roosevelt,
President of the United States,
White House
Washington, D.C.

Sir:

Some recent work by E.Fermi and L. Szilard, which has been communicated to me in manuscript, leads me to expect that the element uranium may be turned into a new and important source of energy in the immediate future. Certain aspects of the situation which has arisen seem to call for watchfulness and, if necessary, quick action on the part of the Administration. I believe therefore that it is my duty to bring to your attention the following facts and recommendations:

In the course of the last four months it has been made probable - through the work of Joliot in France as well as Fermi and Szilard in America - that it may become possible to set up a nuclear chain reaction in a large mass of uranium,by which vast amounts of power and large quantities of new radium-like elements would be generated. Now it appears almost certain that this could be achieved in the immediate future.

This new phenomenon would also lead to the construction of bombs, and it is conceivable - though much less certain - that extremely powerful bombs of a new type may thus be constructed. A single bomb of this type, carried by boat and exploded in a port, might very well destroy the whole port together with some of the surrounding territory. However, such bombs might very well prove to be too heavy for transportation by air.

ab4a01

Demythifying Cybersecurity

Myths	Responses
Myth 1: More layers of defense are better.	**Response 1: Provable, science-based cyber security** Move cyber security from a trade craft to scientific discipline. Limit complexity to enable provability
Myth 2: Burdensome security is good security.	**Response 2: Unambiguous identity**. Continuous, Adaptive Authentication
Myth 3: Running my executables on my data on my system is secure because I control my system.	**Response 3: Reverse the asymmetry** Turn complexity against the attacker Attacker faces a combinatorially hard problem

For further information:

- http://doi.ieeecomputersociety.org/10.1109/MSP.2010.95

Sandia National Laboratories

Livermore, CA
Albuquerque, NM

Edward B. Talbot
ebtalbo@sandia.gov
Manager, Information Assurance Department
Sandia National Laboratories
Livermore, CA

Tom M. Kroeger
tmkroeg@sandia.gov
Information Assurance Security Department
Sandia National Laboratories
Livermore, CA

"Exceptional service in the national interest"