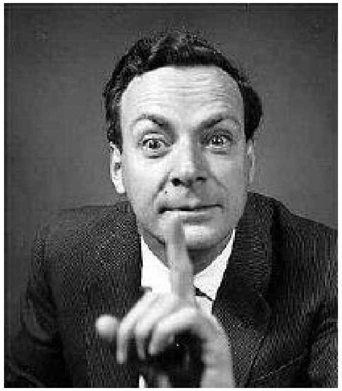
DIMENSIONS

Process of Science

We never are definitely right;
we can only be sure when we are wrong.

Richard Feynman
Lectures on the Character of Physical Law



Secure or Insecure

Insecure!

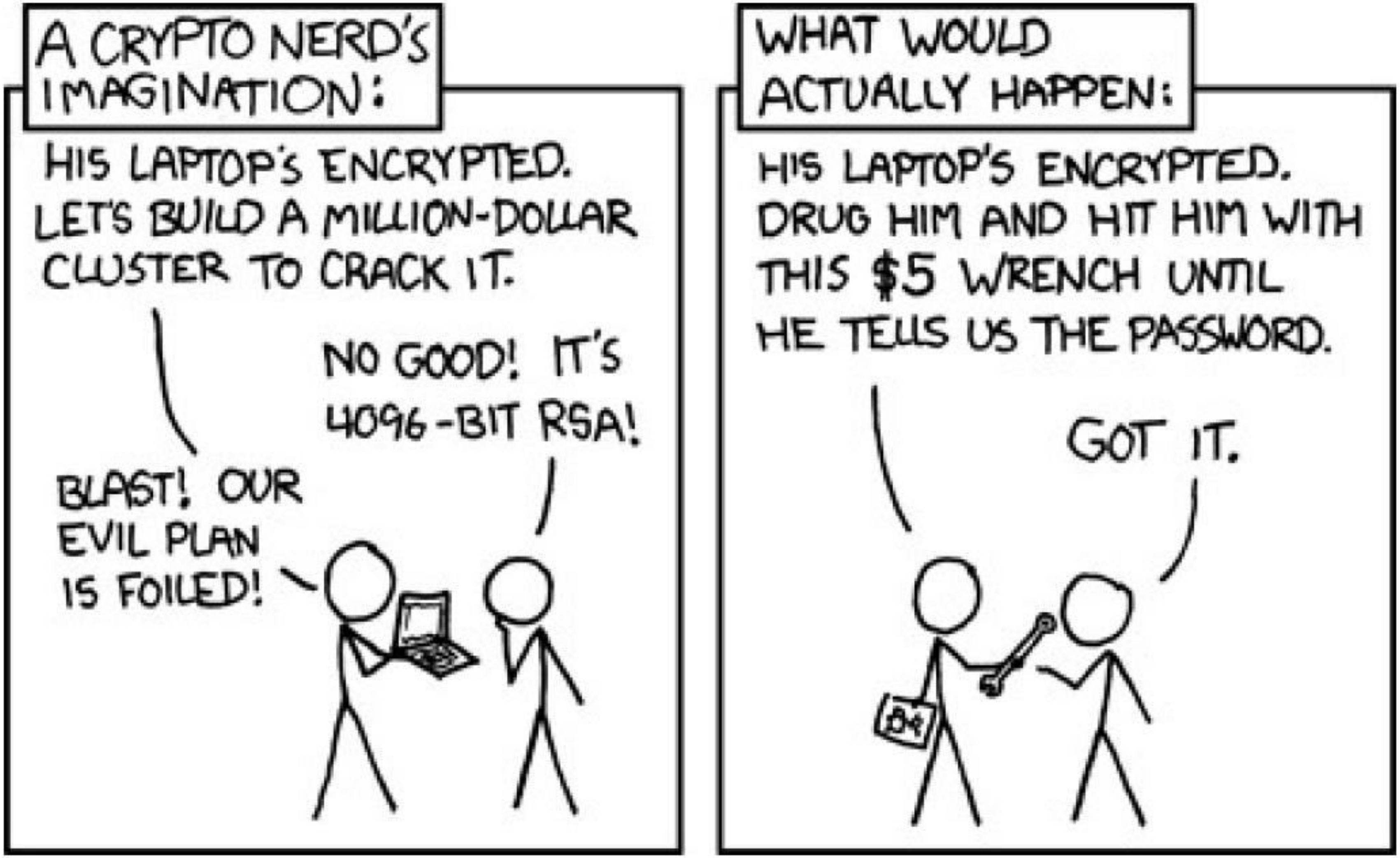
- *Suppose we have a precisely defined security claim about a system,*

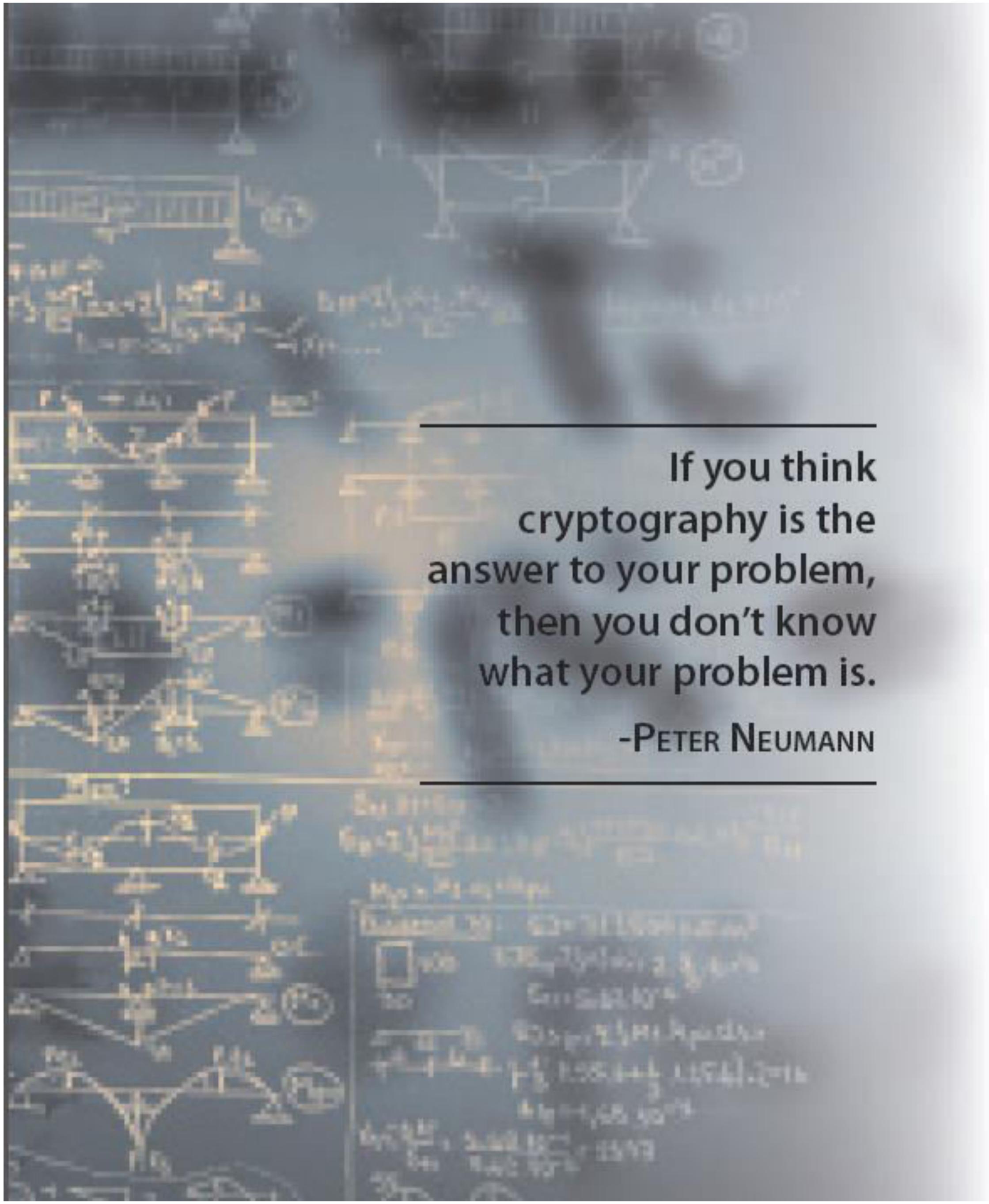
from which we can derive the consequences which can be tested,

- *Then* ***in principle*** *we can prove that the system is* ***insecure****.*

Secure?

- *Suppose you design a system, derive some security claims, and discover every time that the system remains secure under all tests.*
- *Is the system then secure?*
- *No, it is simply not proved insecure.*
- *In the future you could refine the security model, there could be a wider range of tests and attacks, and* ***you might then discover that the thing is insecure.***


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.



> If you think cryptography is the answer to your problem, then you don't know what your problem is.
>
> -Peter Neumann

Side channel Attacks

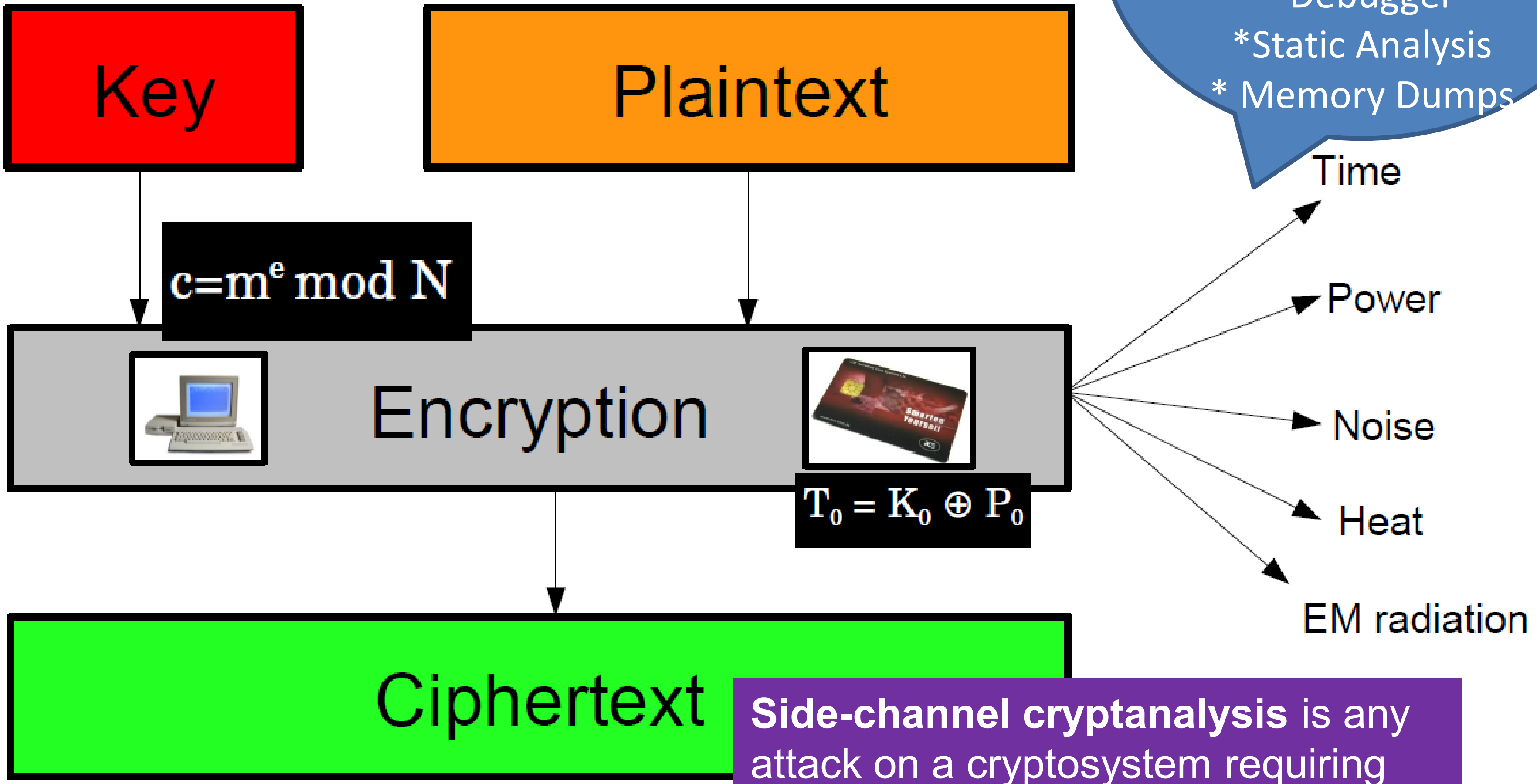
White Box Crypt analysis

Nothing is hidden (white box)

*Debugger

*Static Analysis

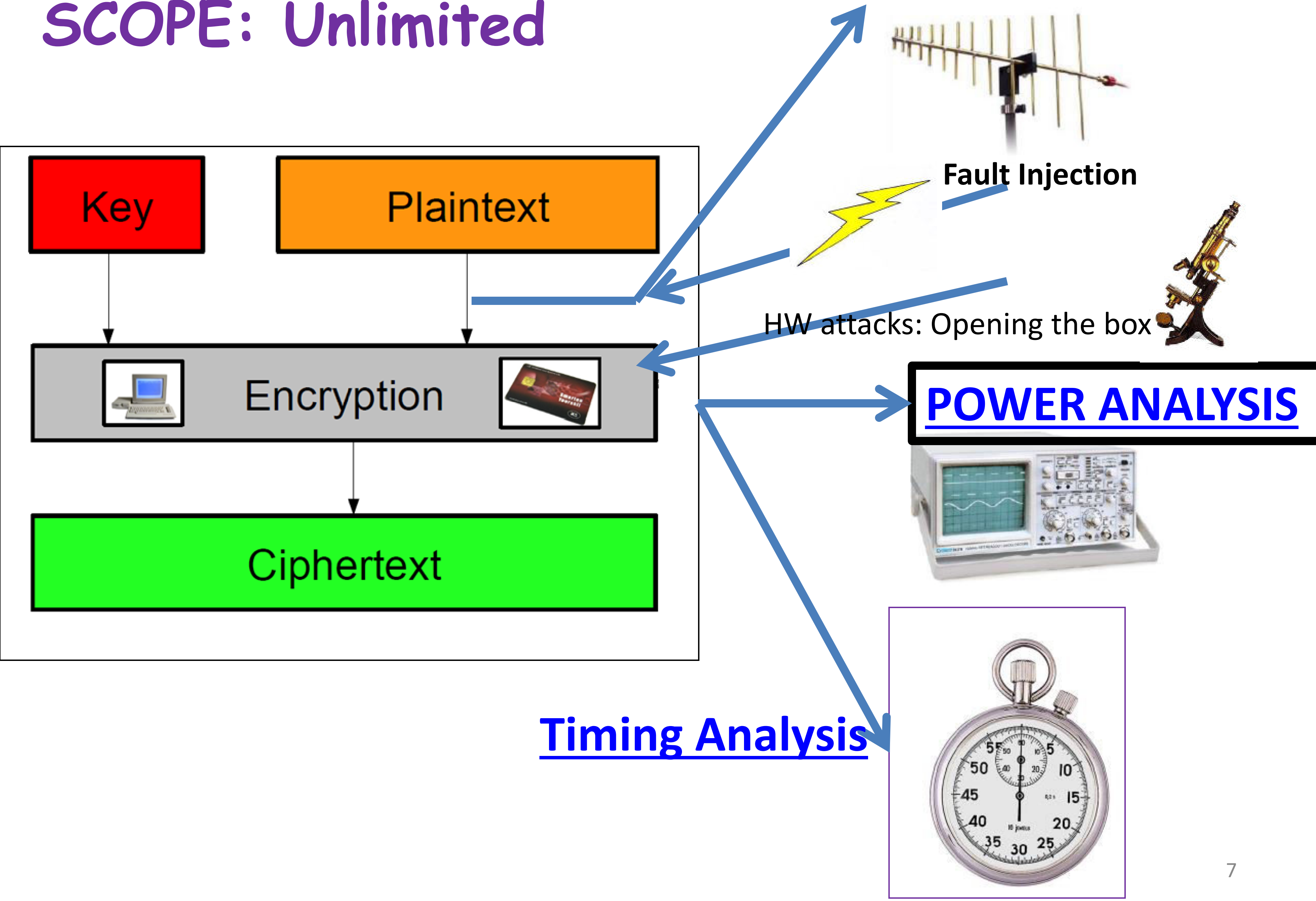
* Memory Dumps



Side-channel cryptanalysis is any attack on a cryptosystem requiring information emitted as a byproduct of the physical implementation.

Paul Kocher

SCOPE: Unlimited



EM Signals containing full secrets

Fault Injection

HW attacks: Opening the box

POWER ANALYSIS

Timing Analysis

Science of Guessing Passwords

- Joseph Bonneau

Ph.D. Thesis,

Univ. of Cambridge, 2012

Advisor:

Ross Anderson, FRS

NSA AWARD FOR THE BEST SCIENTIFIC CYBERSECURITY PAPER

- Banking PINs

Tracking, say, SKYPE Locations

Real Time Communication:

Peer-to-Peer (P2P)

- Datagram flows between the two conversing partners
- Exposes the IP addresses of all the participants to one another

- If A knows B's VoIP ID, she can establish a call with Bob & obtain his current address by simply sniffing datagrams arriving at her computer.

Steven Le Blond et al (2012)

- Using Geo-localization services, one can map B's IP address to a location and ISP.
- If B is Mobile, she can call him over a week/month and observe
- Once A knows B's IP, she can crawl P2P file-sharing systems to see if that IP is **uploading/downloading files**
- VoIP can potentially collect targeted user's location
- A SERIOUS INFRINGEMENT ON PRIVACY

STUXNET

Attacks on Supervisory Control And Data Acquisition (SCADA)

SCADA

- Control Systems
  - Now at a higher risks to computer attacks because their vulnerabilities are increasingly becoming exposed and available to an ever-growing set of motivated and highly-skilled attacker
- Miscreants tailor their attacks with the aim of damaging the physical systems under control
- Essentially a **Cyberwar**

STUXNET Attacks

- Stuxnet is a Windows computer worm discovered in July 2010 that targets industrial software and equipment
- it is the first discovered malware that spies on and subverts industrial systems
- Kaspersky Labs concluded that the sophisticated attack could only have been conducted "with nation-state support”
- Stuxnet attacked Windows systems using an unprecedented four zero-day attacks (plus the CPLINK vulnerability and a vulnerability used by the Conficker worm)

Stuxnet

- Astonished by the complexity of the program and the quantity of zero day exploits used in this worm.
  - Zero day exploits are those that have no work around or patch.
- Another unique aspect of Stuxnet is that it contained components that were digitally signed with stolen certificates.
- a root kit was found for the programmable logic controller (PLC) which allows the manipulation of sensitive equipment.

- Expected to have been created by a team of as many as 30 individuals. – STATE SUPPORT
- indicates a level of organization and funding that probably has not been seen before
- What was Stuxnet designed to do?
  - While there is no direct evidence, the code suggests that Stuxnet looks for a setup that is used in processing facilities that handle uranium used in nuclear devices
  - Thus the ultimate goal is to sabotage that facility by reprogramming to controllers to operate

What should be the strategy to deal with these kinds of attacks?

- Should it go along the lines of IT security?
- How about Defense-in-depth mechanisms analogous to anomaly detection?
- What about false-alarms in anomaly detection?
- Should the focus be on Physical systems rather than software/network models?

Control System: Characteristics

- Control systems not suitable for patching and frequent updates
- While current tools from Information security can give necessary mechanisms for securing control systems, these alone are not sufficient for defense-in-depth of control systems
- **When attackers bypass even basic defenses they may succeed in damaging the physical world**

SCADA Attacks: Summary

Consequences

Risk Assessment

- While studies exist on cyber security of SCADA there are very few studies to identify attack strategy of an adversary once it gains access (existing studies pertain to data injection for power grids, electricity markets etc.)
- Need to understand threat model to design appropriate defenses and take measures to secure the most critical sensors and actuators

SCADA Security Summary

- New Attack detection Patterns
  - Dynamic system models for specifying Intrusion detection Systems
- Attack Resilient Algorithms and Architectures
  - Design to withstand cyber assault
  - Reconfigure and adapt control systems when under attack

Multi Disciplinary: Control Engineers + CS + Domain of Application …

BigData: Algorithmic Approach

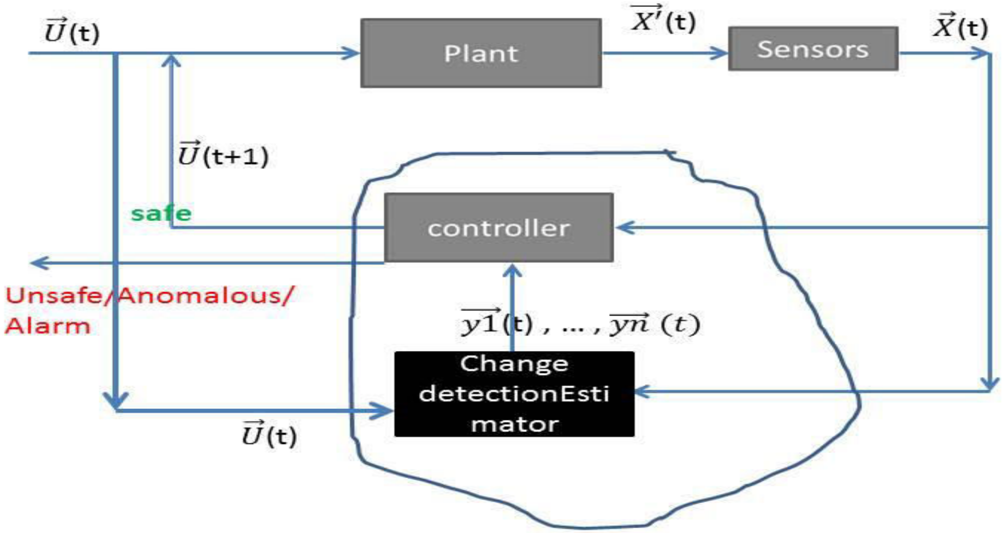


Figure 1. Anomaly Detecting Controller

- Compositionality + Scalablability (Reducing the problem to convex-hull detection over distributed streaming data) – Shyamasundar 2013

Tor Anonymity Network

Tor?

- Tor is free software and an open network that helps you defend **against traffic analysis**, a **form of network surveillance** that threatens personal freedom and privacy, confidential business activities and relationships, and state security.

Why Anonymity?

- Tor protects you by bouncing your communications around a distributed network of relays run by volunteers all around the world: **it prevents somebody watching your Internet connection from learning what sites you visit, and it prevents the sites you visit from learning your physical location.**

Threats: A Landscape

Threats

Trojan Botnet in 2010 -upward

- Significant as despite increasing coordinated efforts to shut down botnet activity (Mariposa, Bredolab and Waledec botnets)
- Shutting Waledac botnet resulted in an instantaneous drop off in observed command and control traffic.
- Zeus (also known as Zbot and Kneber), continues to evolve through intrinsic and plugin advances. The Zeus botnet malware is commonly used by attackers to steal banking information from infected computers.

SQL Injection, Obfuscation, PDF

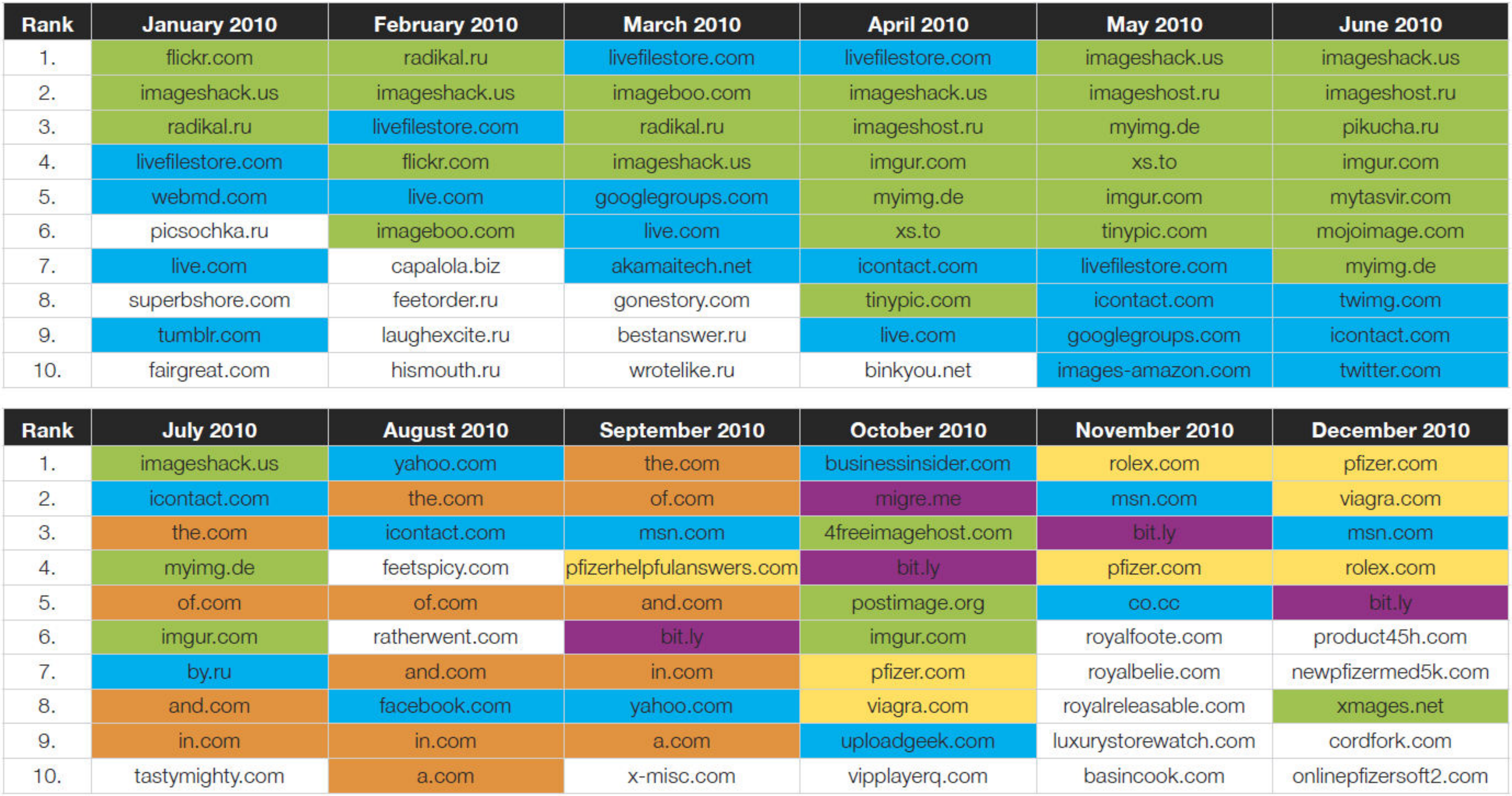
- **SQL**: Popular due to its simplicity to execute and its scalability to compromise large amounts of web servers across the Internet.
  - appears seasonal pattern: during each of the past 3 years, there has been a globally scaled SQL injection attack some time during May through August.
  - SQL Slammer worm first surfaced in Jan 2003
  - one of the most devastating Internet threats of the past decade.
  - continues to generate a great deal of traffic on the Internet in 2010
- **Obfuscation**: attackers attempt to hide their activities and disguise their programming,
  - Upward trend 2010 with no signs of waning.
- **PDF exploitation:**
  - favorite among attackers. In late April, a particular spam campaign contained an Adobe Acrobat PDF that used the Launch command to deliver malware.
  - At the peak of the attacks, IBM received more than 85,000 alerts in a single day.

IBM X-Force

Spam and Phishing

- Anonymous proxies – steady increase (5 times)
  - critical type of websites to track, because they allow people to hide potentially malicious intent.
- Spam: USA, India, Brazil, Vietnam, and Russia -- top five countries for spam origination in 2010.
  - spammers focused on content over volume.
  - spammers began sending spam threats with ZIP attachments with a single EXE file that was malicious.
  - In a short time spammers began shifting to HTML once again tricking the end-user
- Phishing : India 15.5%, Russia 10.4%; target finanicial institutions

- Vulnerability:
  - largest number of vulnerability disclosures in history—8,562. This is a 27 percent increase over 2009,
  - increase has had a significant operational impact for anyone managing large IT infrastructures.
  - More vulnerability disclosures can mean more time patching and remediating vulnerable systems.
  - 49 percent of the vulnerabilities disclosed in 2010 were web application vulnerabilities.
    - Cross site scripting and SQL injection issues.
  - 44 percent of all vulnerabilities in 2010 still had no corresponding patch by the end of the yearA recent IBM research study discovered that about
- IBM Study:
  - 14 percent of the Fortune 500 sites suffer from severe client-side JavaScript issues, which could allow malicious attackers to perform attacks:
  - Infecting users of these sites with malware and viruses.
  - Hijacking users' web sessions and performing actions on their behalf.
  - Performing phishing attacks on users of these sites.
  - Spoofing web contents.
- Based on the dataset analyzed,
  - likelihood that a random page on the Internet contains a client-side JavaScript vulnerability is approximately one in 55.



Rank	January 2010	February 2010	March 2010	April 2010	May 2010	June 2010
1.	flickr.com	radikal.ru	livefilestore.com	livefilestore.com	imageshack.us	imageshack.us
2.	imageshack.us	imageshack.us	imageboo.com	imageshack.us	imageshost.ru	imageshost.ru
3.	radikal.ru	livefilestore.com	radikal.ru	imageshost.ru	myimg.de	pikucha.ru
4.	livefilestore.com	flickr.com	imageshack.us	imgur.com	xs.to	imgur.com
5.	webmd.com	live.com	googlegroups.com	myimg.de	imgur.com	mytasvir.com
6.	picsochka.ru	imageboo.com	live.com	xs.to	tinypic.com	mojoimage.com
7.	live.com	capalola.biz	akamaitech.net	icontact.com	livefilestore.com	myimg.de
8.	superbshore.com	feetorder.ru	gonestory.com	tinypic.com	icontact.com	twimg.com
9.	tumblr.com	laughexcite.ru	bestanswer.ru	live.com	googlegroups.com	icontact.com
10.	fairgreat.com	hismouth.ru	wrotelike.ru	binkyou.net	images-amazon.com	twitter.com

Rank	July 2010	August 2010	September 2010	October 2010	November 2010	December 2010
1.	imageshack.us	yahoo.com	the.com	businessinsider.com	rolex.com	pfizer.com
2.	icontact.com	the.com	of.com	migre.me	msn.com	viagra.com
3.	the.com	icontact.com	msn.com	4freeimagehost.com	bit.ly	msn.com
4.	myimg.de	feetspicy.com	pfizerhelpfulanswers.com	bit.ly	pfizer.com	rolex.com
5.	of.com	of.com	and.com	postimage.org	co.cc	bit.ly
6.	imgur.com	ratherwent.com	bit.ly	imgur.com	royalfoote.com	product45h.com
7.	by.ru	and.com	in.com	pfizer.com	royalbelie.com	newpfizermed5k.com
8.	and.com	facebook.com	yahoo.com	viagra.com	royalreleasable.com	xmages.net
9.	in.com	in.com	a.com	uploadgeek.com	luxurystorewatch.com	cordfork.com
10.	tastymighty.com	a.com	x-misc.com	vipplayerq.com	basincook.com	onlinepfizersoft2.com

Table 4: Most common domains in URL spam, 2010

Geographical Distribution of Spam Senders

2010

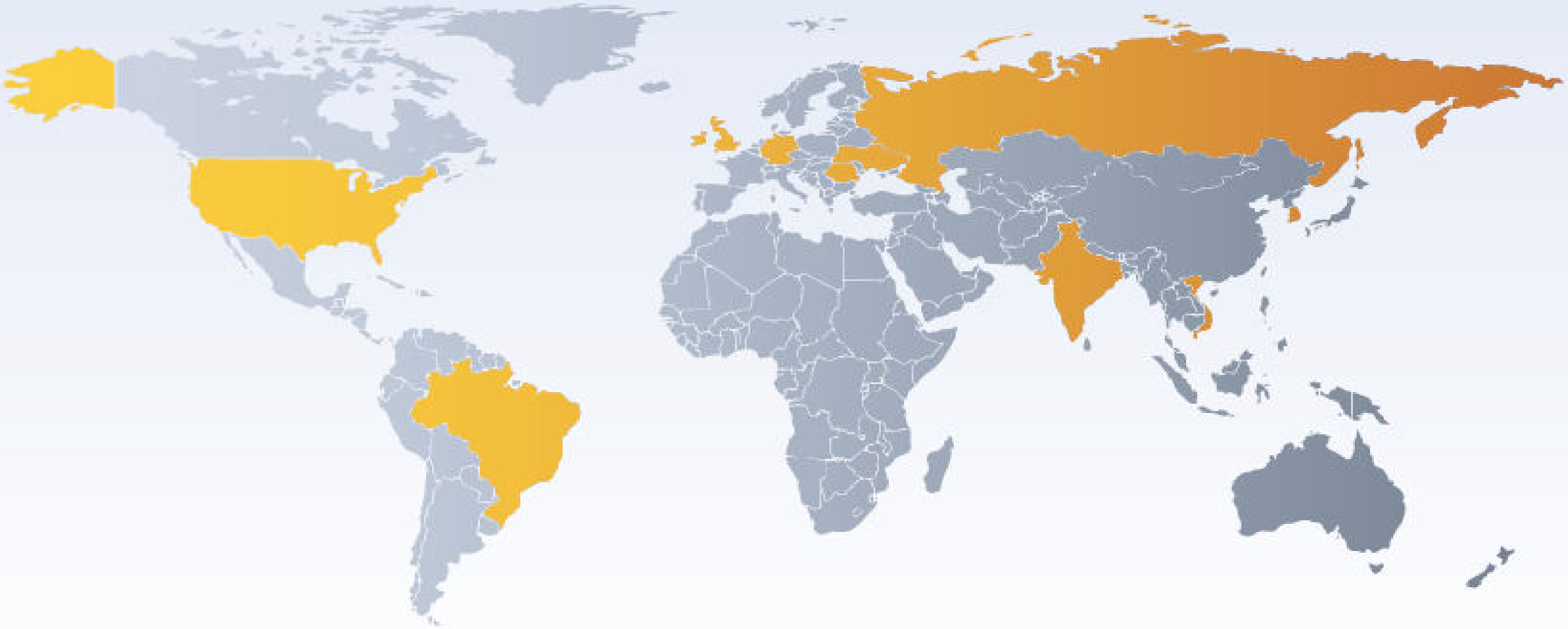
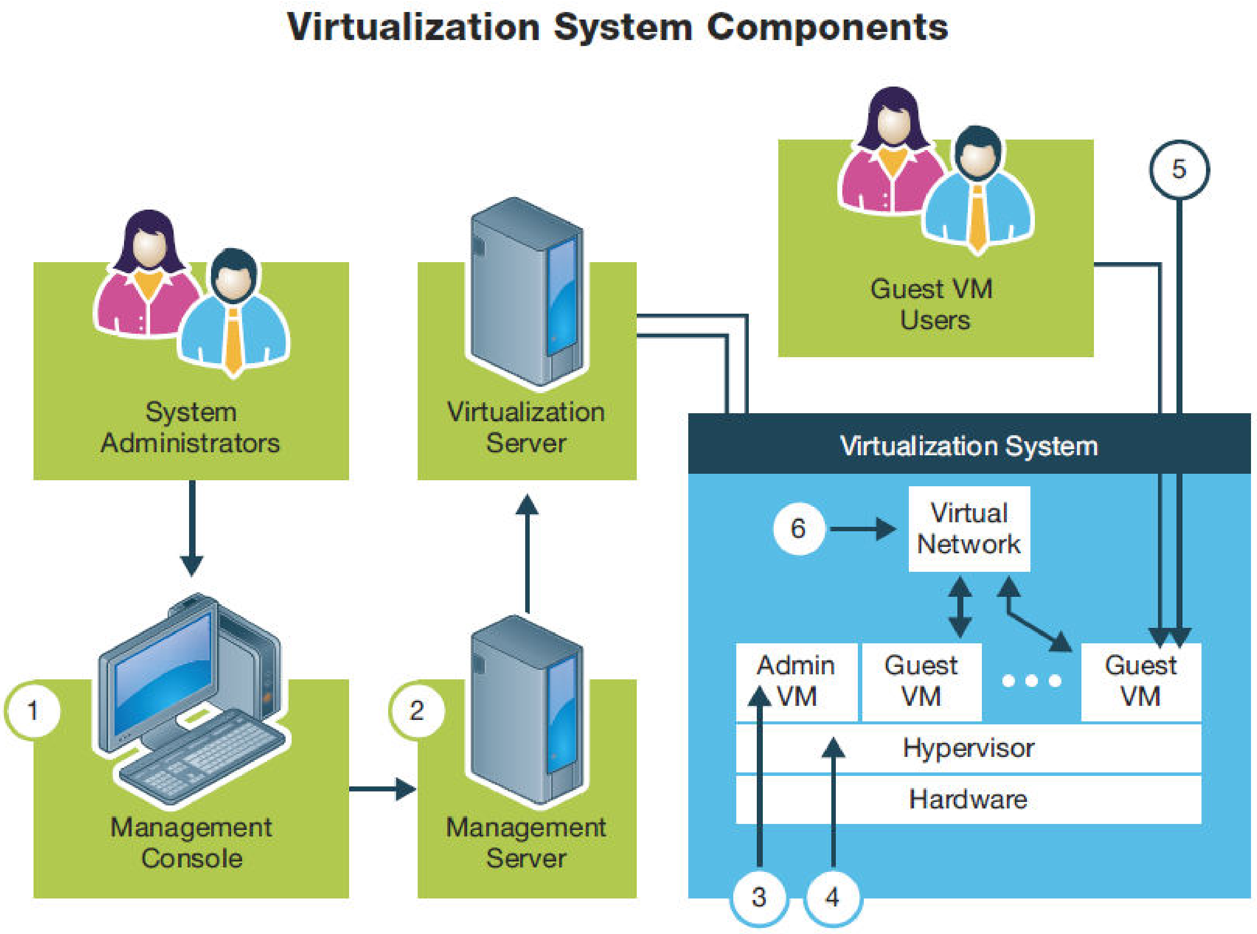


Figure 32: Geographical Distribution of Spam Senders – 2010

Country	% of Spam
USA	10.9%
India	8.2%
Brazil	8.1%
Vietnam	5.4%
Russia	5.2%
United Kingdom	4.4%
Germany	3.7%
South Korea	3.3%
Ukraine	3.0%
Romania	2.9%

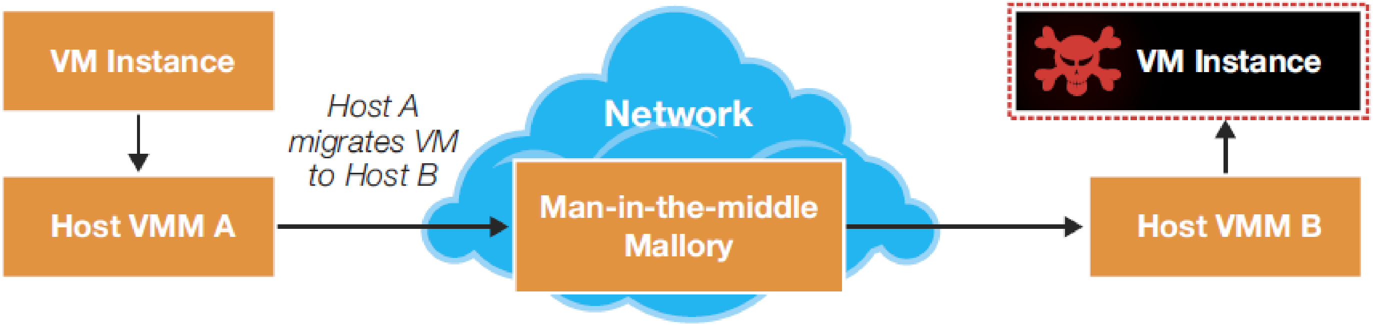
Table 6: Geographical Distribution of Spam Senders – 2010

Virtualization—risks



Virtualization Attacks

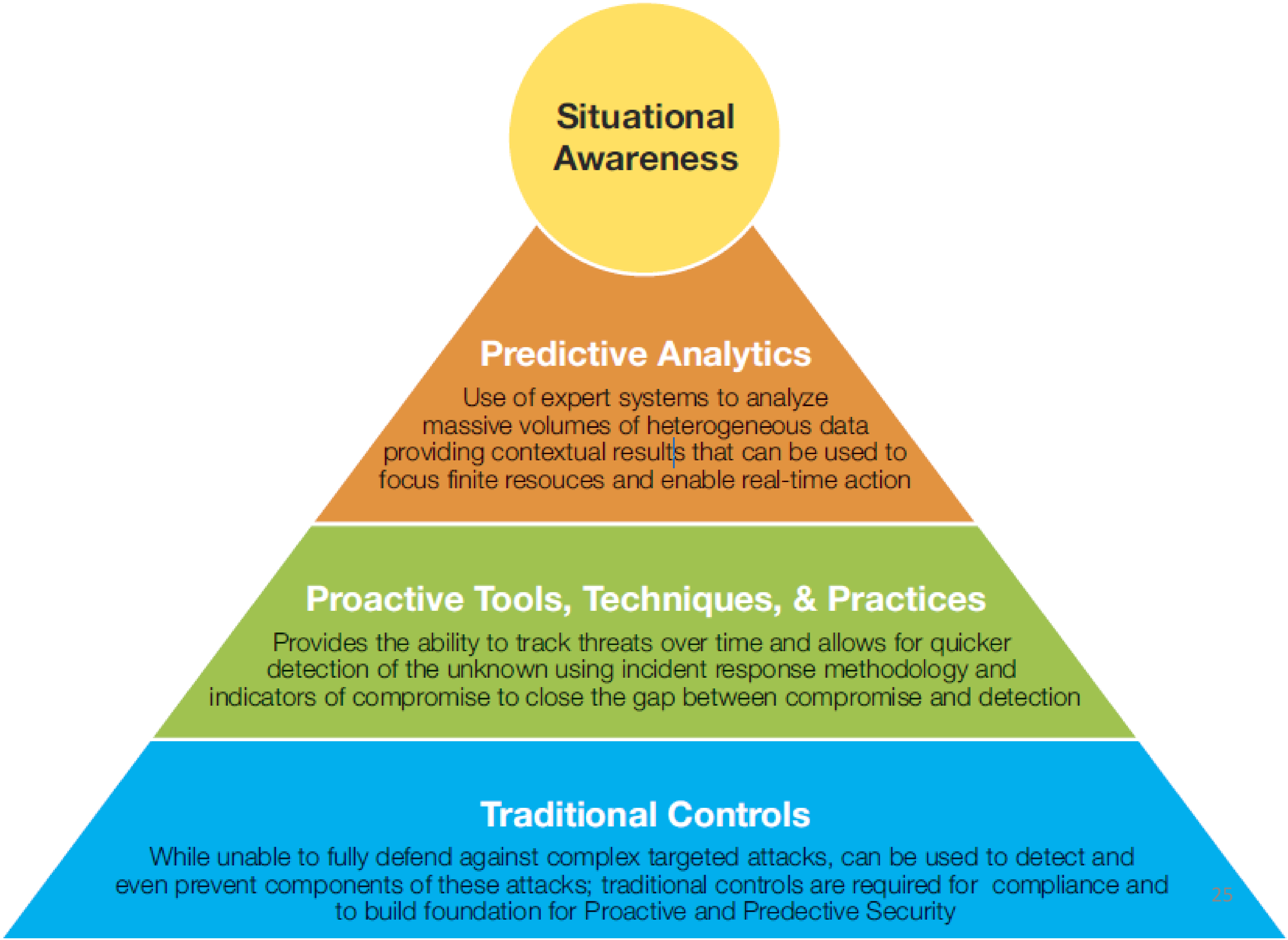
VM migration man-in-the-middle attack



If communication is not encrypted

Can modify arbitrary VM OS/application state

From "Exploiting Live Virtual Machine Migration", Black Hat DC 2008 briefings, John Oberheide.



Situational Awareness

Predictive Analytics

Use of expert systems to analyze massive volumes of heterogeneous data providing contextual results that can be used to focus finite resouces and enable real-time action

Proactive Tools, Techniques, & Practices

Provides the ability to track threats over time and allows for quicker detection of the unknown using incident response methodology and indicators of compromise to close the gap between compromise and detection

Traditional Controls

While unable to fully defend against complex targeted attacks, can be used to detect and even prevent components of these attacks; traditional controls are required for compliance and to build foundation for Proactive and Predective Security

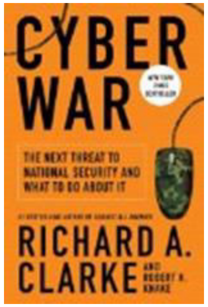
AV, Industry and Society

- Government controlled
  “Deep Packet Inspection”
- Malware inspection at fibres of Tier 1 ISPs
- Conflict between government and industry
- Which AV product?
- Who determines what an AV product is?
  (CC Protection Profile??)
- How is “Product Testing“ defined and controlled?
- Who's signatures
- Who controls signatures DB
- Who protects Signature DB
- Who declares what a threat (Malware) is?

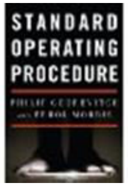
Malware: Issues

- Malware
  - Detection
  - Definition
  - Collection
  - Distribution
  - Protection
- Technical aspects
  - AV product
  - Definition
  - Categorisation
  - Testing

Cyber War: What does one understand?


CYBER
WAR
THE NEXT THREAT TO NATIONAL SECURITY AND WHAT TO DO ABOUT IT
RICHARD A. CLARKE
AND ROBERT K. KNAKE

- **Variations:** e-, i-, cyber-, info-, techno-, and net-, war
- **War:**
  - Declared outbreak of hostilities between countries carried out by legitimate combatants
- Legitimate combatant:
  - Someone who takes a direct part in the hostilities of an armed conflict
  - Follows the law of war
    - Wears uniform
    - Carries weapon openly
    - On capture qualifies as “Prisoner of War” under Geneva Convention



- **Geneva convention**
- **Wars of defense**: when one nation is attacked by an aggressor, it is considered legitimate for a nation along with its allies to defend itself against the aggressor. (NATO article 5)
- **Wars sanctioned by the UN Security Council:** when the United Nations as a whole acts as a body against a certain nation.

Current Understanding

- No clear definition for “Cyber”
- War and its participants defined for conventional war
- “Asymmetric War” not covered by legal framework or international treaties

Cyber War questions?

- Is Cyber War symmetric or asymmetric?
- Is “Cyber War” going to be declared?
- Who is a legitimate combatant – or participant?
- What is a cyber weapon?
- When is an attack against some systems in one country a hostile activity and as such cyber war?
- What is the next step after cyber war?

What is Cyber War?

- Cyber warfare has been defined by government security expert Richard A. Clarke, in his book Cyber War (May 2010), as "actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption
- All “big” nations are currently preparing for Cyber War
  - Cyber Defense Centers established in all these nations within their military structure & NATO
  - Cyber Defense Centre of Excellence in Estonia
  - Cyber Defense part of new NATO Strategy (Article 5 excluded)
  - Military and government networks are currently being hardened against attacks
  - All nations and, to and unbelievable large scale, China are training offensive cyber war personnel and are preparing for offensive an defensive cyber war
- **Information Superiority:** the capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same (US Army Vision 2010)

Some Cyber Wars

- **Titan Rain** was the U.S. government's designation given to a series of coordinated attacks on American computer systems since 2003
- **Estonia 2007** Cyberattacks on Estonia refers to a series of cyber attacks that began April 27, 2007 and swamped websites of Estonian organizations, including Estonian parliament, banks, ministries, newspapers and broadcasters
- **Israel attack on Syria** During the night, an Israeli transport helicopter entered Syrian airspace and dropped a team of Shaldag Unit commandos into the area. The commandos took up positions close to the nuclear site. Israeli Air Force F-15I Ra'am fighter jets armed with laser-guided bombs, escorted by F-16I Sufa fighter jets and an ELINT aircraft, took off from Hatzerim Airbase. The ELINT aircraft successfully obscured the attacking aircraft from detection by Syrian radars.

Cyber Crime/ Cyber Terrorism

- Cyber Crime : Crime is the breach of rules or laws for which some governing authority (via mechanisms such as legal systems) can ultimately prescribe a conviction
- Cyber Terrorism is a phrase used to describe the use of Internet based attacks in terrorist activities, including acts of deliberate, large-scale disruption of computer networks, especially of personal computers attached to the Internet, by the means of tools such as computer viruses.

Difference:

- Crime = violation of law and punishment
- Terrorism = Internet based attacks in terrorist activities

Cyber Crime vs Cyber War vs Cyber Terrorism

Cyber Crime

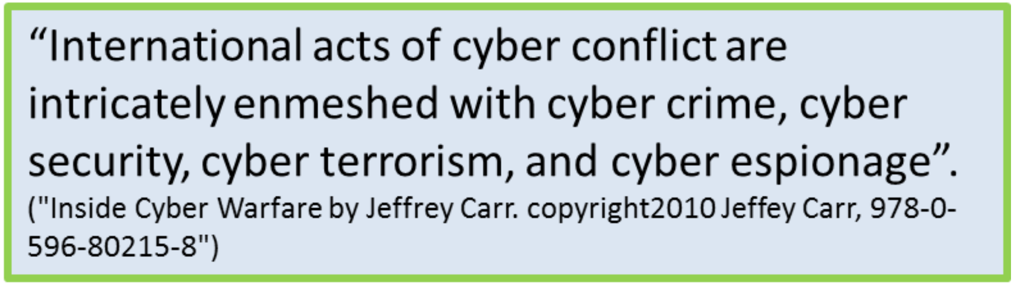
- Computer crime encompasses a broad range of potentially illegal activities. Generally, however, it may be divided into one of two types of categories:
  - crimes that target computer networks or devices directly;
  - crimes facilitated by computer networks or devices, the primary target of which is independent of the computer network or device
- EU Cyber Crime Convention

Cyber Terrorism

- There is no universally agreed, legally binding, criminal law definition of terrorism
- Since 1963, the international community has elaborated 13 universal legal instruments and three amendments to prevent terrorist acts

Cyber War

- actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption
- Battlefield is the network
- Offensive / defensive
- Reconnaissance
- Declaration of war
- Attack and attribution



"International acts of cyber conflict are intricately enmeshed with cyber crime, cyber security, cyber terrorism, and cyber espionage".
("Inside Cyber Warfare by Jeffrey Carr. copyright2010 Jeffey Carr, 978-0-596-80215-8")

Cyber Crime vs Cyber War

Cyber Crime

- Violates law
- Randomly or specifically targeted
- Isolated or element of attack

Cyber (Information) War

- Not necessarily violates law
- Never randomly
- Never isolated

Cyber war -- Weapons and Defence

"It comes hard to most of the U.S. military to think of technology as something that another nation could use effectively against us, especially when that technology is some geek's computer code and not a stealthy fighter-bomber. So, we cannot deter other nations with our cyber weapons. In fact, other nations are so undeterred that they are regularly hacking into our networks."
(Richard Clark)

Cyber Weapons

- cannot deter other nations with our cyber weapons

Cyber Weapons Include:

- electronic countermeasure, defence shields against electronic attack, infrared decoys, angle reflectors,
- false-target generators, root kits, malicious code, transient electromagnetic devices, Trojans, spyware, back-doors in commonly used
- software, autonomous mobile cyber weapons, key loggers, bot-nets, viruses, worms, and many other exploitation techniques.
- It should be noted that there are at least two other cyber weapons that are under development and classified.

Convergence on Cyber Weapons & its Consequences

Wassenarr Arrangement 1996/2001

It has been established in order to contribute to regional and international security and stability, by promoting transparency and greater responsibility in transfers of conventional arms and dual-use goods and technologies, thus preventing destabilising accumulations. Participating States seek, through their national policies, to ensure that transfers of these items do not contribute to the development or enhancement of military capabilities which undermine these goals, and are not diverted to support such capabilities.

Until 1995 cryptographic algorithm where listed in the arms list

Include Cyber weapons in WA

- Will there be export limitations?
- Who will control the DB of Samples (“Wildlist”)
- Will there be a “Misuse of Cyber Weapons Act”?
- Who will find, collect, list and control new vulnerabilities (0-day bug)?
- Will the possession be sanctioned?
- How do we distinguish between legitimate- and misuse? (and by who's standard?
- Will there be “engagement” rules for the use of cyber weapons?
- Is “hacking” into a target computer done by a state cyber warrior covered under immunity?

AV and Cyberwar

- How much trust can we have in AV?
- Magic Lantern
  keystroke logging software developed by the United States' Federal Bureau of Investigation.
- Third party access
- Is “mod n” a strong cryptographic algorithm?
- “Bundestrojaner”
  - Trojan installed clandestinely by law enforcement
  - Not to be recognised by AV

AV and the Cyber War

- Government controlled
  “Deep Packet Inspection”
- Malware inspection at fibres of Tier 1 ISPs
- Conflict between government and industry
- Which AV product
- Who determines what an AV product is?
  (CC Protection Profile??)
- How is “Product Testing“ defined and controlled?
- Who's signatures
- Who controls signatures DB
- Who protects Signature DB
- Who declares what a threat (Malware) is?

Summary

Designing Systems

- Correctness and Efficiency
- Security!!: Defenders react to known attacks:
    - New attack succeeds; we deploy a defense.
- Shift from **reactive** to **proactive** mode
- How do we measure effectiveness of defenses -- impt for investments
- Technology base is a moving target.
  - Computers replaced every 3-5 years
    - New deployment environments
    - SCADA, electronic health, …
    - New insights needed to transcend technology and applications
- NEED: Science of Security: Science & Engg

- … Need insights that transcend technology and applications

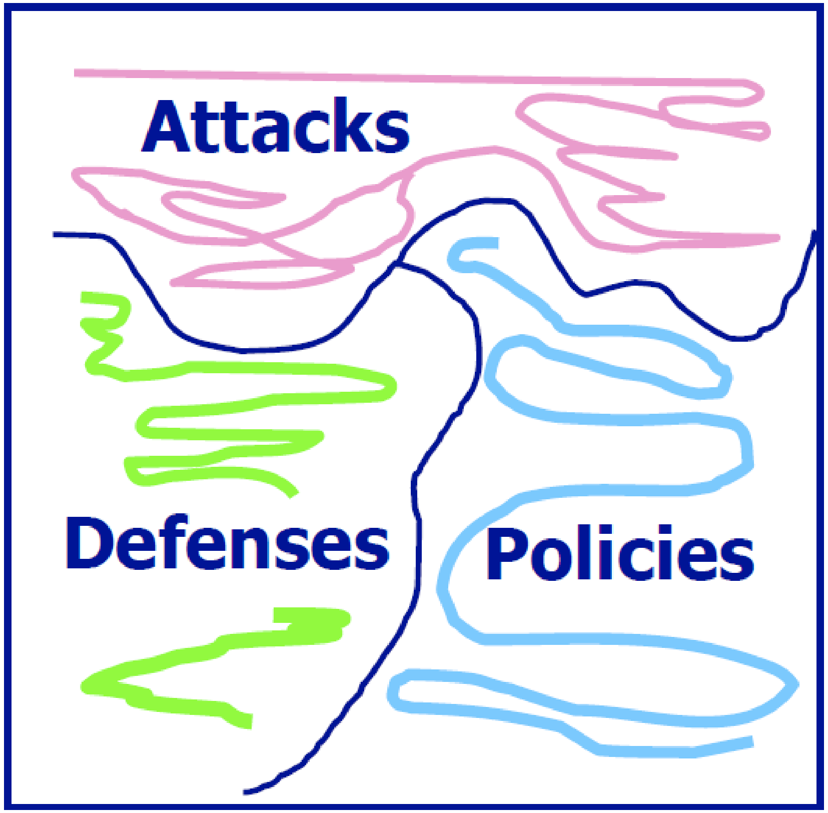
Science of Security (Schneider)

- **Science**:
  - An organized body of knowledge gained through research **-versus-**
  - System of acquiring knowledge based on the scientific method **-versus-**
  - Laws or theories that are predictive.
- **Engineering**: Craft informed by Science.

Body of Laws

- That are predictive
  - Transcend specific systems,attacks/ defenses
  - Applicable in real settings.
  - Provide explanatory value
    - Abstractions and models
    - Connections and relationships
  - Not necessarily quantitative
    - Channel leaks b bits/sec
    - Cannot enforce policy P with mechanism M

Theories About



Features:

- Classes of policies
- Classes of attacks
- Classes of defenses

Relationships:

"Defense class D enforces policy class P despite attacks from class A."

"Defense D + Defense D' = …"

THANK YOU QUESTIONS??