

Classes of Defense for Computer Systems

Josephine Wolff

April 21, 2015

Berkman Center for Internet & Society

Why Information Security is Hard— An Economic Perspective (Anderson, 2001)

“Attack is simply easier than defense. Defending a modern information system could also be likened to defending a large, thinly-populated territory like the nineteenth century Wild West: the men in black hats can strike anywhere, while the men in white hats have to defend everywhere.”

Cyber Attack Kill Chain Model (Hutchins et al., 2011)



“the adversary must progress successfully through each stage of the chain before it can achieve its desired objective; just one mitigation disrupts the chain and the adversary ... the defender can achieve an advantage over the aggressor”

Attack Stage

1 Wardriving
(Miami, FL)



2 Blabla sniffer
(New York, NY)



3 TJX servers
(Framingham, MA)



4 Exfiltrate data
(Ukraine & Latvia)



5 Imprint blank credit cards
(China)









6 Decrypt PIN numbers
(Eastern Europe)



Attack Stage

Possible Defenses

- 1** Wardriving (Miami, FL)  Possible Defenses: Wi-Fi Protected Access (WPA); no wireless network
- 2** Blabla sniffer (New York, NY)  Possible Defenses: Restricting connectivity to known/registered devices
- 3** TJX servers (Framingham, MA)  Possible Defenses: Storage of less customer information; stronger encryption
- 4** Exfiltrate data (Ukraine & Latvia)  Possible Defenses: Monitoring outbound traffic on store servers
- 5** Imprint blank credit cards (China)  Possible Defenses: Regulate black market card sellers
- 6** Decrypt PIN numbers (Eastern Europe)  Possible Defenses: Better key management

Attack Stage

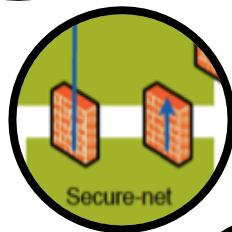
Possible Defenses

1 Connection to DMZ-ext-net



Patching web content management system, better configured IPS

2 Connection to secure-net



Less convoluted firewall rules

3 Remote desktop connection



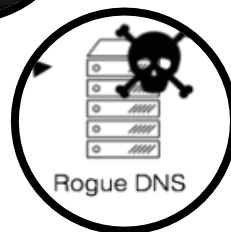
Blocking remote access tools

4 Activate physical private key card



Manual insertion of keycards for CRL generation

5 DNS cache poisoning



DNSSEC, disregarding records received w/out query

6 MITM attacks on Google sites



Certificate pinning in browsers

Two Ways of Looking at Defense

- Defense to limit access/computer system capabilities
 - Access to computer systems is not a binary “in” or “out” but rather a range of capabilities
 - Each time a bad actor acquires a new, useful capability is a potential opportunity for defense
- Defense to limit harm/damage
 - The closer malicious actors comes to actually harming their victims the easier it becomes to identify their behavior as decisively illegitimate
 - Much of this indisputably harmful behavior occurs outside the context of the protected computer system, offering additional opportunities for defense

Why access defense is hard

- Difficult to distinguish between malicious and legitimate activity early on in many types of attacks
- Access stages of attacks are more likely to be highly replaceable for adversaries
 - Resonates with the “weakest link” theory of defense

Attack Stage

Possible Defenses

Aug. 13

Phishing
e-mails



E-mail filtering;
phishing alerts

Aug. 14

Employee
response



Employee education about phishing;
two-factor authentication

Aug. 27

Remote log-in
to network



Restrictions on
remote log-in access

Sept. 1

Windows OS
malware installed



Software patching;
antivirus programs

Sept. 12

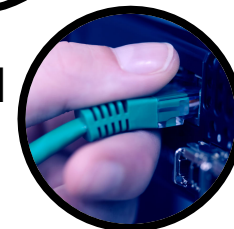
Database files
(~75GB) copied



Audit logs; flags for
unusual network activity

Sept. 13

Copied files exported
over the Internet



Monitoring
outbound traffic

How should we think about classes of attacks?

- Early access modes, prior to the infliction of harm, are the stages of an attack or intrusion that are likely to be most replaceable for the adversary
 - Defending against the acquisition of initial capabilities may help narrow that adversary's options, but is unlikely to provide protection against the class of harm that adversary intends to inflict
- Classes of harm are more static than the classes of exploitable technical capabilities—the former set is relatively contained and unchanging, the latter much larger and in constant flux

Classes of harm

- Financial theft/fraud
- Physical service disruption
 - Incidents that require going beyond a computer system to inflict damage offer additional opportunities for defensive intervention
- Digital service disruption
- Political/military espionage
 - Incidents whose scope is solely digital rely heavily on access defense and are constrained in some ways as to how devastating their impact can actually be on people
- Economic espionage

What can application designers do?

- Make it easier to distinguish legitimate and malicious behavior through the design of applications
 - Establishing enduring reputation markers for identity indicators based on previous behavior
 - Using behavioral indicators to enforce the accuracy of identity indicators
 - Checking the consistency of behavioral and identity indicators

What can organizations and managers do?

- Understand the threats they face and the ultimate harms that can result to both themselves and others
 - Define what constitutes legitimate and malicious behavior in particular environments
- Implement independent lines of defense
 - Focus resources on harms and essential (rather than replaceable) threat capabilities (e.g., data exfiltration)





about

visiting | maps | offices | history

admissions

undergrad | graduate | financial aid

education

schools+courses
OpenCourseWare | MITx | edX

research

labs+centers | lincoln lab | libraries

community

students | faculty | staff | alumni

life@MIT

arts | athletics | connect

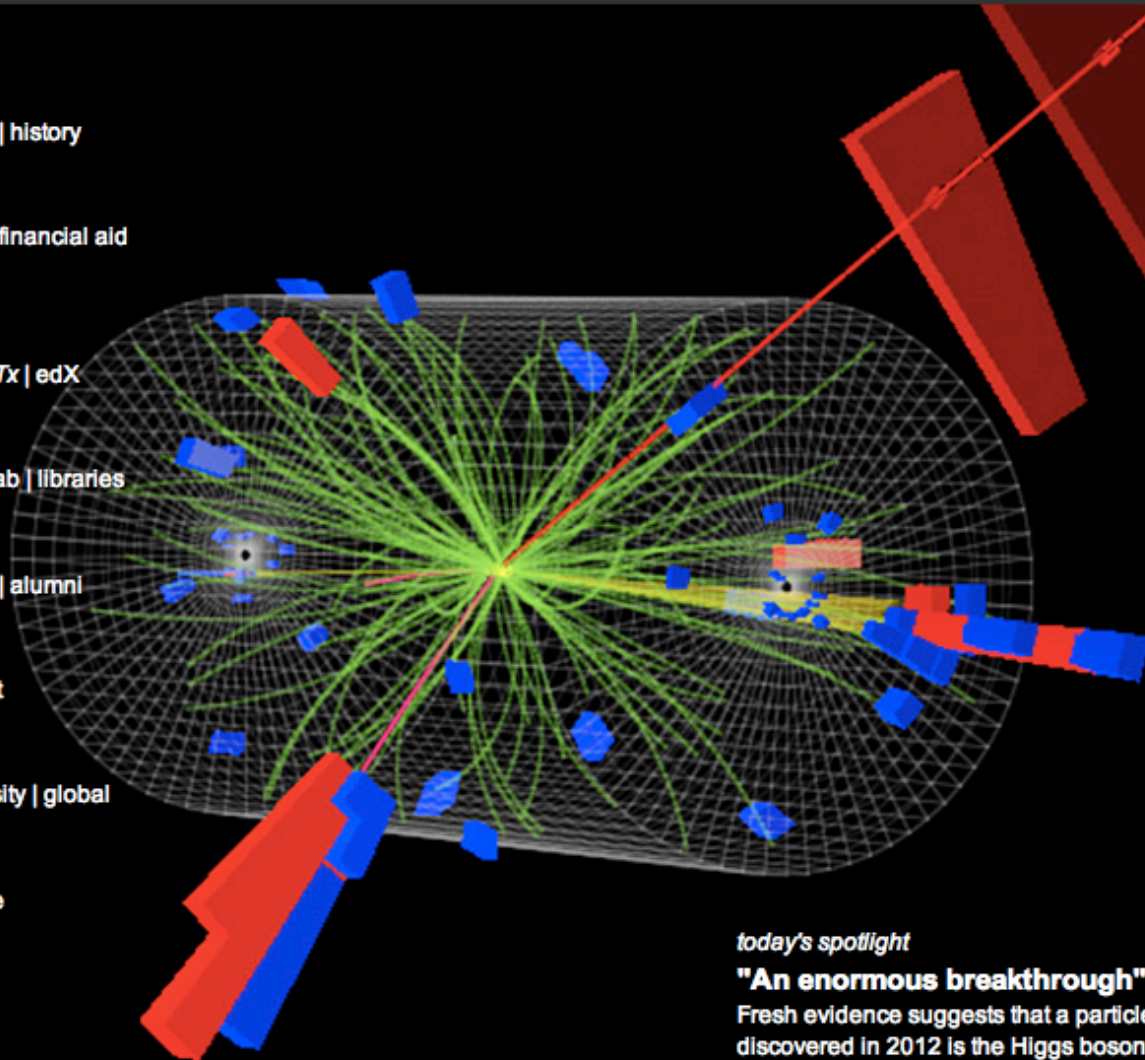
Initiatives

energy | cancer | diversity | global

Impact

industry | public service

commencement



news

Rett syndrome drug shows promise in clinical trial

Experimental 36-core chip employs innovative communication scheme

Graduate student Kaitlin Goldstein dies in India

Robert Langer receives Kyoto Prize

research | campus | press

events

Campus Tours and Info Sessions

9 Artists: MIT List Visual Arts Center

The Good Jobs Strategy: Why Good Jobs Are Good for Businesses (June 26)

today's spotlight

"An enormous breakthrough"

Fresh evidence suggests that a particle discovered in 2012 is the Higgs boson

Today's image



In Memoriam, Aaron Swartz, November 8, 1986 – January 11, 2013, Requiescat in pace.

A brief message from Anonymous.

Whether or not the government contributed to his suicide, the government's prosecution of Swartz was a grotesque miscarriage of justice, a distorted and perverse shadow of the justice that Aaron died fighting for — freeing the publicly-funded scientific literature from a publishing system that makes it inaccessible to most of those who paid for it — enabling the collective betterment of the world through the facilitation of sharing — an ideal that we should all support.

Moreover, the situation Aaron found himself in highlights the injustice of U.S. computer crime laws, particularly their punishment regimes, and the highly-questionable justice of pre-trial bargaining. Aaron's act was undoubtedly political activism; it had tragic consequences.

[#JusticeForAaronSwartz](#)
[#freemanning](#)
[#OpFreeAssange](#)
[#Antisec](#)

Our wishes

- We call for this tragedy to be a basis for reform of computer crime laws, and the overzealous prosecutors who use them.
- We call for this tragedy to be a basis for reform of copyright and intellectual property law, returning it to the proper principles of common good to the many, rather than private gain to the few.
- We call for this tragedy to be a basis for greater recognition of the oppression and injustices heaped daily by certain persons and institutions of authority upon anyone who dares to stand up and be counted for their beliefs, and for greater solidarity and mutual aid in response.
- We call for this tragedy to be a basis for a renewed and unwavering commitment to a free and unfettered internet, spared from censorship with equality of access and franchise for all.

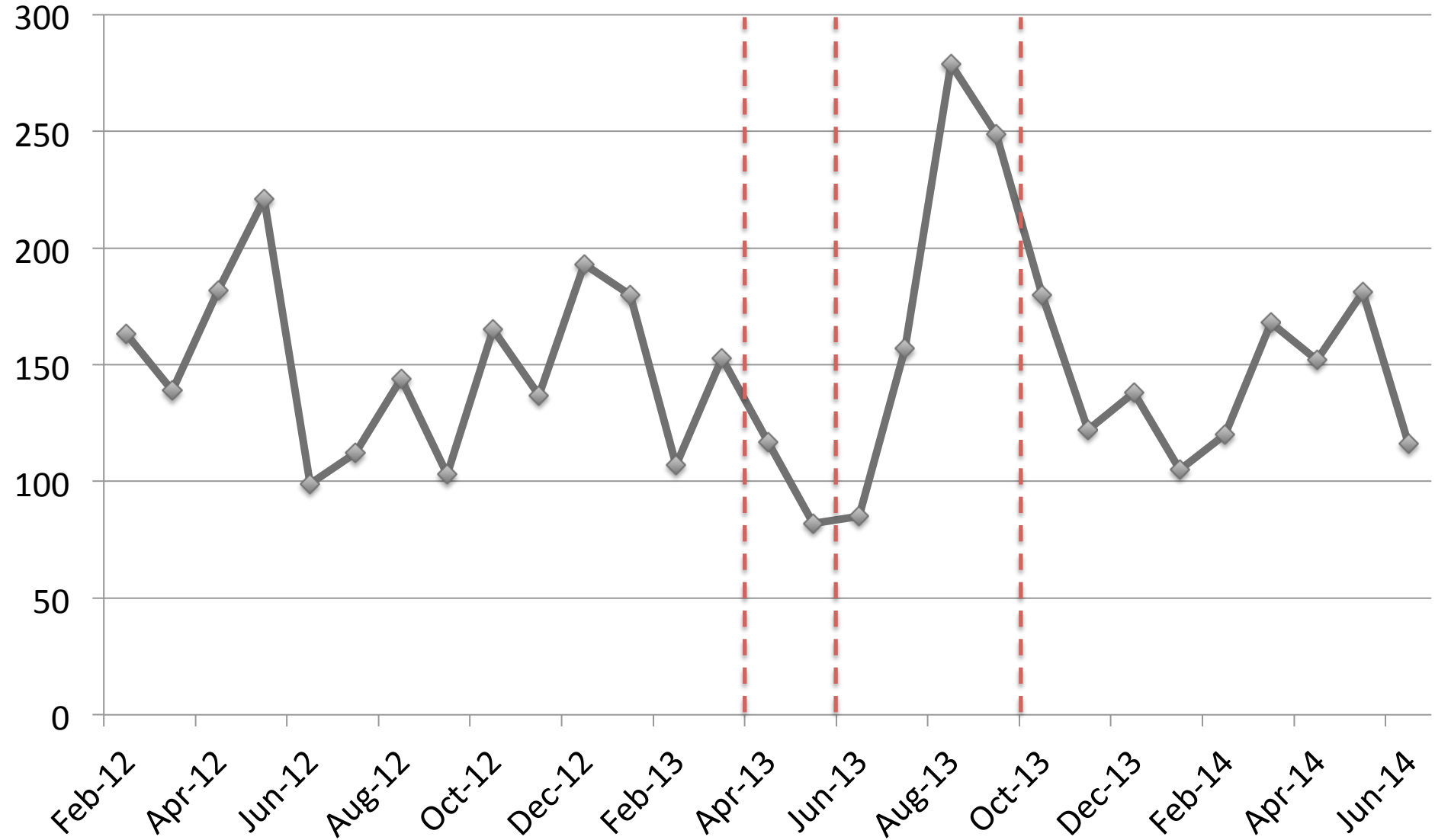
For in the end, we will not be judged according to what we give, but according to what we keep to ourselves.

Aaron, we will sorely miss your friendship, and your help in building a better world. May you read in peace.

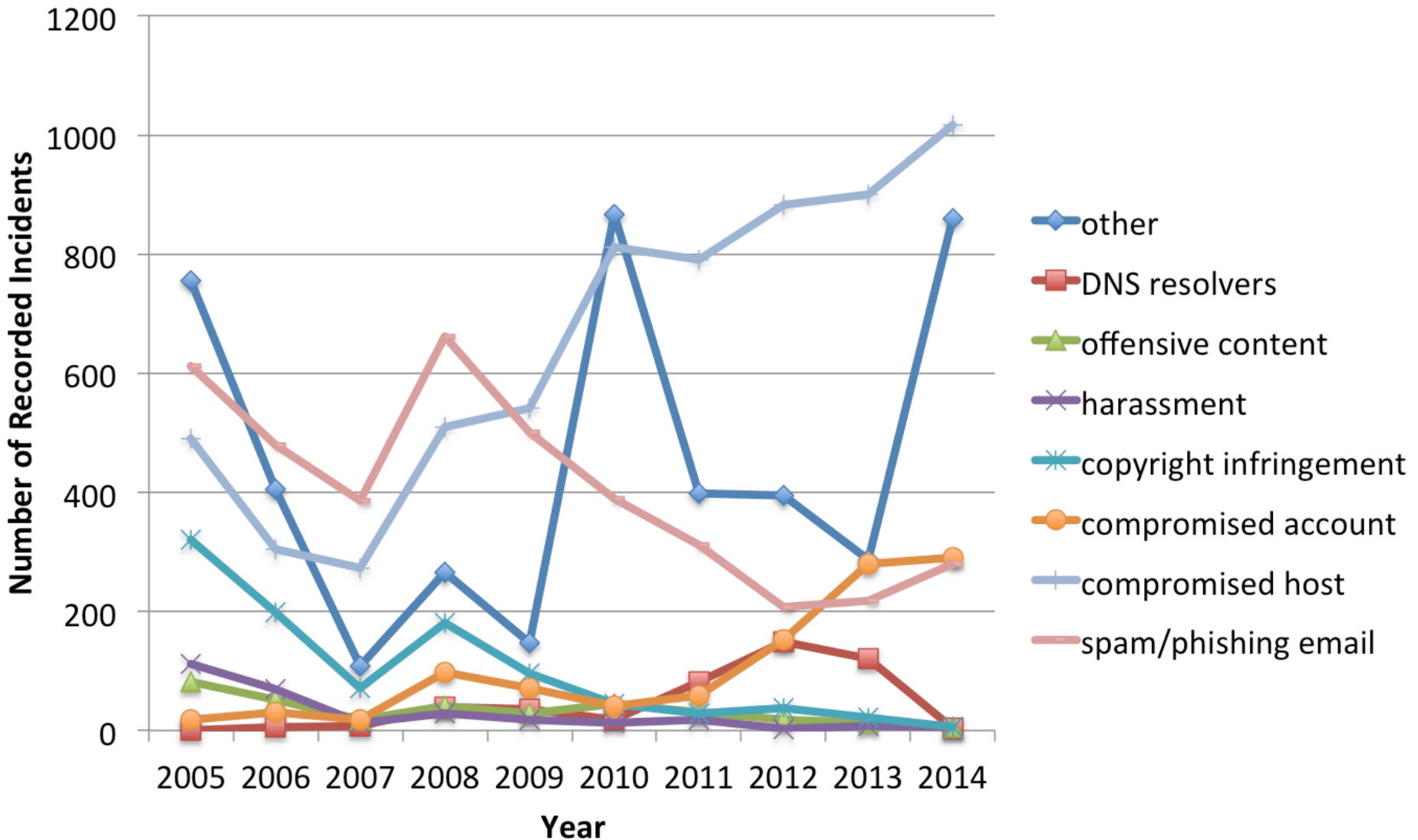
New Security Policies (April 2013)

- Firewall
- Password complexity requirements
- Password expiration limit
- Restrictions on off-campus access to MIT administrative applications and servers
- Additional resiliency measures for MIT's primary website

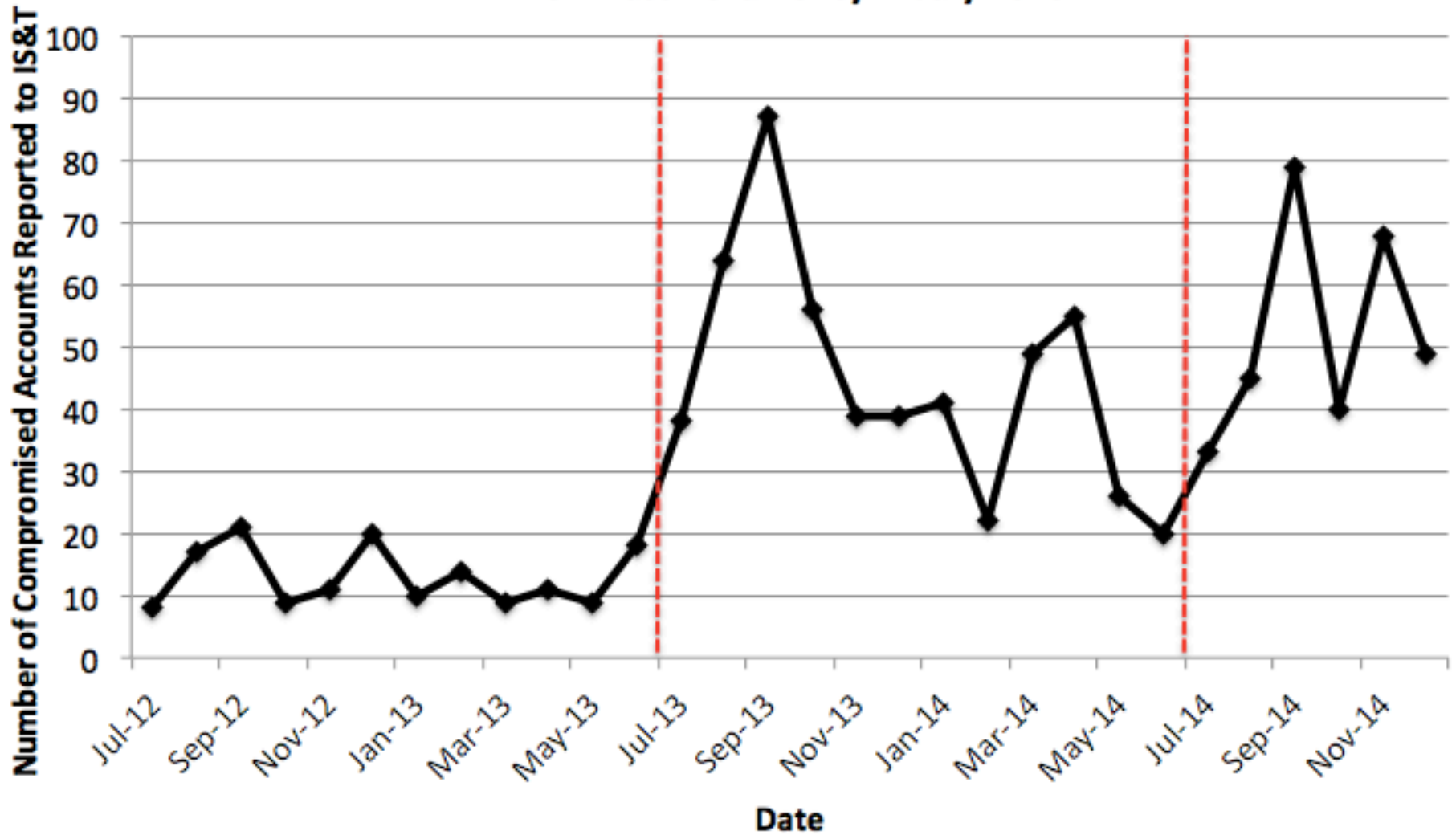
Security Incidents Per Month



Threat Landscape



Number of Compromised Accounts Before & After Implementation of New Password Policy in July 2013



From: **MIT Administrator** <info@mit.edu>

Date: 2014-06-14 15:45 GMT-04:00

Subject: MIT Update Email Account

To:

This Email is from MIT Technical team to inform you that all Staff in possession of the MIT University Email account is currently been affected by a deadly virus which automatically activates your message compose setting and automatically send virus messages to other email users hereby causing harm to the hard drive of your computer and in few days will crash your inbox.

Login into your account to automatically enroll your email into the ongoing Anti-virus cleanser update, just by login into your account your email account shall be updated with our newest Antivirus software, which will protect your email account against any further spam or virus contained email sent to you.

Update E-mail Antivirus - Email Maintenance

<http://unionlineaccessonlinemitlivenow.yolasite.com/>



120,000
Devices on
MITnet/year

80 Security
Contacts/
week

35,000
Probes/
host/day

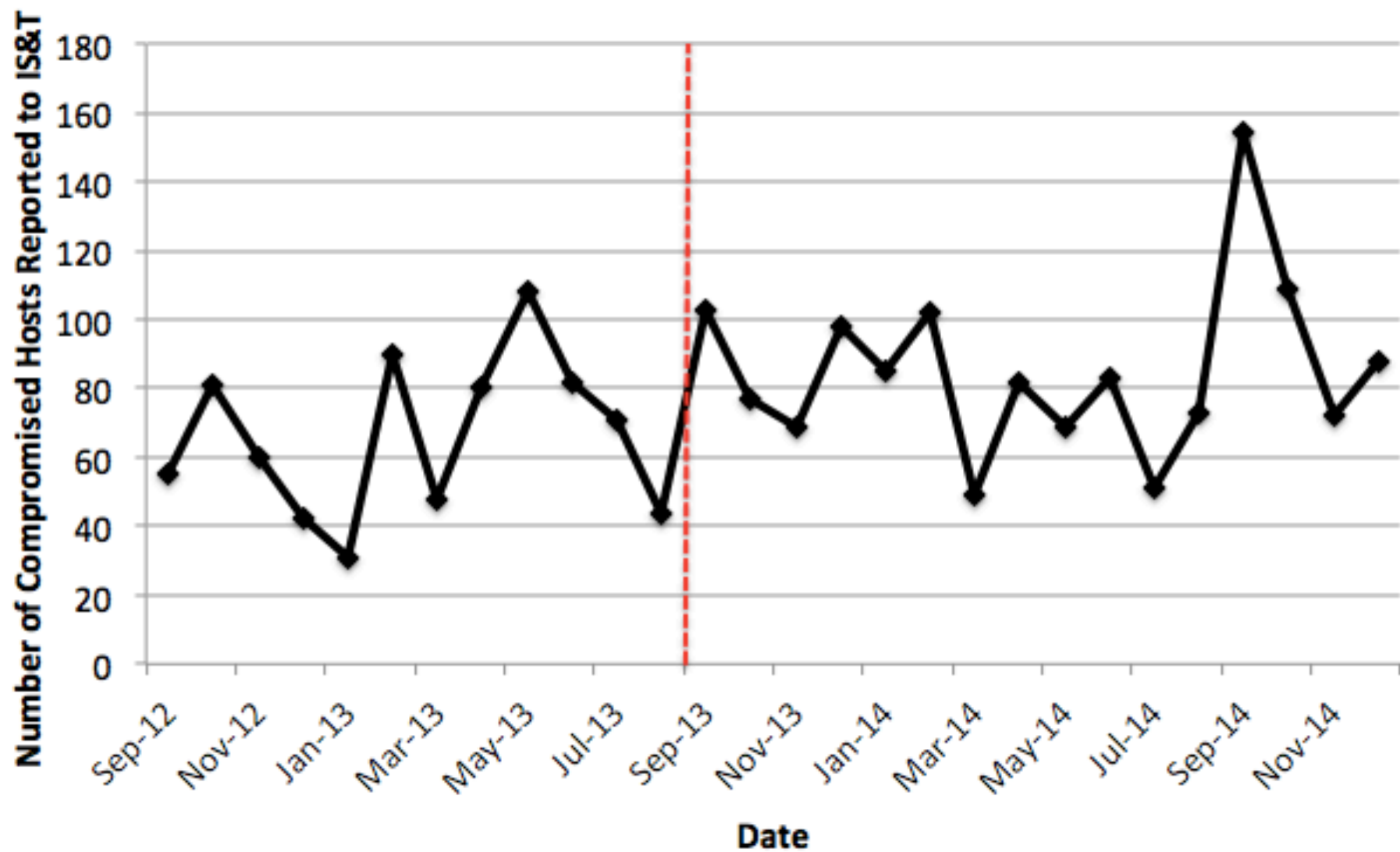
2 Million
Password Crack
Attempts/day

600 © DMCA
Takedown
Notices/month

~400 Malware
Infections/
week

US Dept of State Geographer
© 2013 Google
Image/IBCAO
Data SIO, NOAA, U.S. Navy, NGA, GEBCO

Number of Compromised Hosts Reported to IS&T, September 2012-December 2014



What can policy-makers do?

- Harm defense, cut off criminal money flows
 - Law enforcement focus on fraud activity
 - Deter Cyber Theft Act
- Incentive/externality problem
 - Hold intermediaries responsible for attacks on third parties or mandate security requirements
- Visibility & measurement problem
 - Collect data on security incidents and associated defensive postures to determine which mitigation measures are effective

Some final thoughts

- Do we over-emphasize access defense and role of individual organizations as defenders?
- To what extent are the externality and incentive issues in security compounded by limited visibility and information?
- To what extent can we reframe problems of computer security—and defense—to be less about computers?

Funding Acknowledgments

This material is based upon work supported by the National Science Foundation Graduate Research Fellowship under Grant No. 1000135412. Additional support is provided by the Office of Naval Research under award number N00014-09-1-0597 as well as a grant from the Northrop Grumman Cybersecurity Research Consortium.



Questions & Discussion

Reporting

Purpose	Examples	What is reported?	When is it reported?	To whom?
Consumer protection	Data breach notification laws (e.g., California SB 1386)	Who was affected, what information was revealed	Shortly after a breach is detected	Affected parties (i.e., consumers)

Reporting

Purpose	Examples	What is reported?	When is it reported?	To whom?
Consumer protection	Data breach notification laws (e.g., California SB 1386)	Who was affected, what information was revealed	Shortly after a breach is detected	Affected parties (i.e., consumers)
Real-time threat mitigation	Information sharing policies (e.g., CISA, CISPA)	Signature/detection information, countermeasures	Immediately	Other parties poised to mitigate the threat

Reporting

Purpose	Examples	What is reported?	When is it reported?	To whom?
Consumer protection	Data breach notification laws (e.g., California SB 1386)	Who was affected, what information was revealed	Shortly after a breach is detected	Affected parties (i.e., consumers)
Real-time threat mitigation	Information sharing policies (e.g., CISA, CISPA)	Signature/detection information, countermeasures	Immediately	Other parties poised to mitigate the threat
Threat trends, root causes, & defense impact	Data collection efforts (e.g., Verizon DBIR)	Why threat succeeded, defenses in place, what might have helped	Following a (potentially lengthy) internal investigation	A party able to aggregate incidents reported by others

Narrowing of options

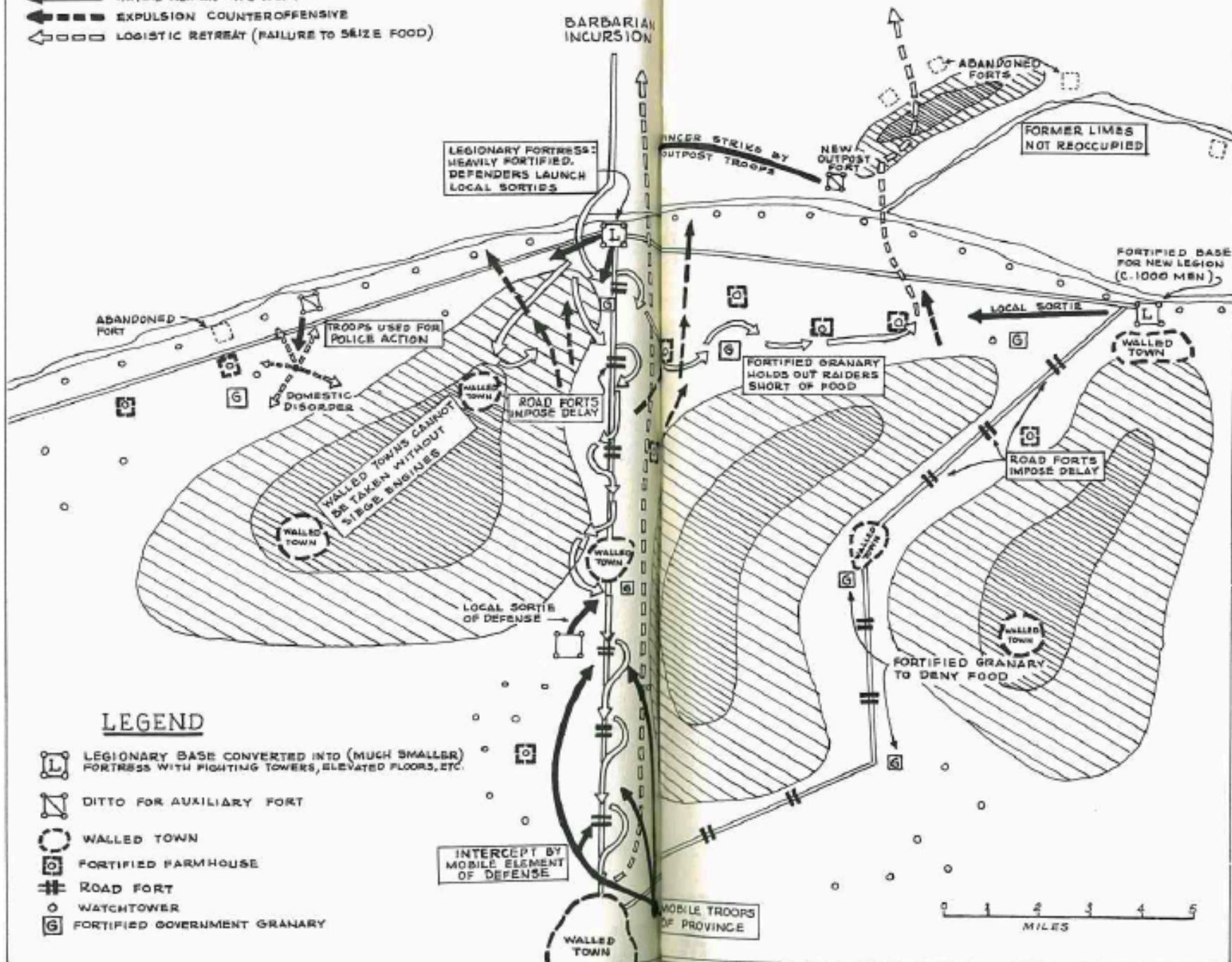
- As bad actors get closer to achieving their end goals, their behavior is likely to become more unambiguously malicious and the available options for how to achieve those malicious ends are likely to narrow
 - Access itself is rarely an attacker's end goal, so it is unlikely to matter to them whether that initial access occurs at the operating system and application level, or the network level, or even physically
 - These different access pathways are interchangeable, making it necessary to defend against a much wider array of different actions than is needed later on, when the intruders close in on their specific, ultimate goals, leaving them fewer alternative paths

Identifying malicious activity

- Defense gets easier as attackers get closer to their end goals because, generally, we identify malicious activity by associating it with a particular type of inflicted (or intended) harm
 - So the closer someone comes to actually inflicting harm, the easier it is to identify his behavior as malicious and try to put a stop to it
 - Similarly, the further away they are from having the necessary capabilities and tools to inflict harm, the harder it is to make that distinction

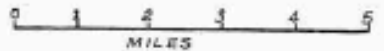
- ← INITIAL BARBARIAN INCURSION
- INITIAL ROMAN INTERCEPT AND SORTIES
- EXPULSION COUNTEROFFENSIVE
- LOGISTIC RETREAT (FAILURE TO SEIZE FOOD)

BARBARIAN INCURSION

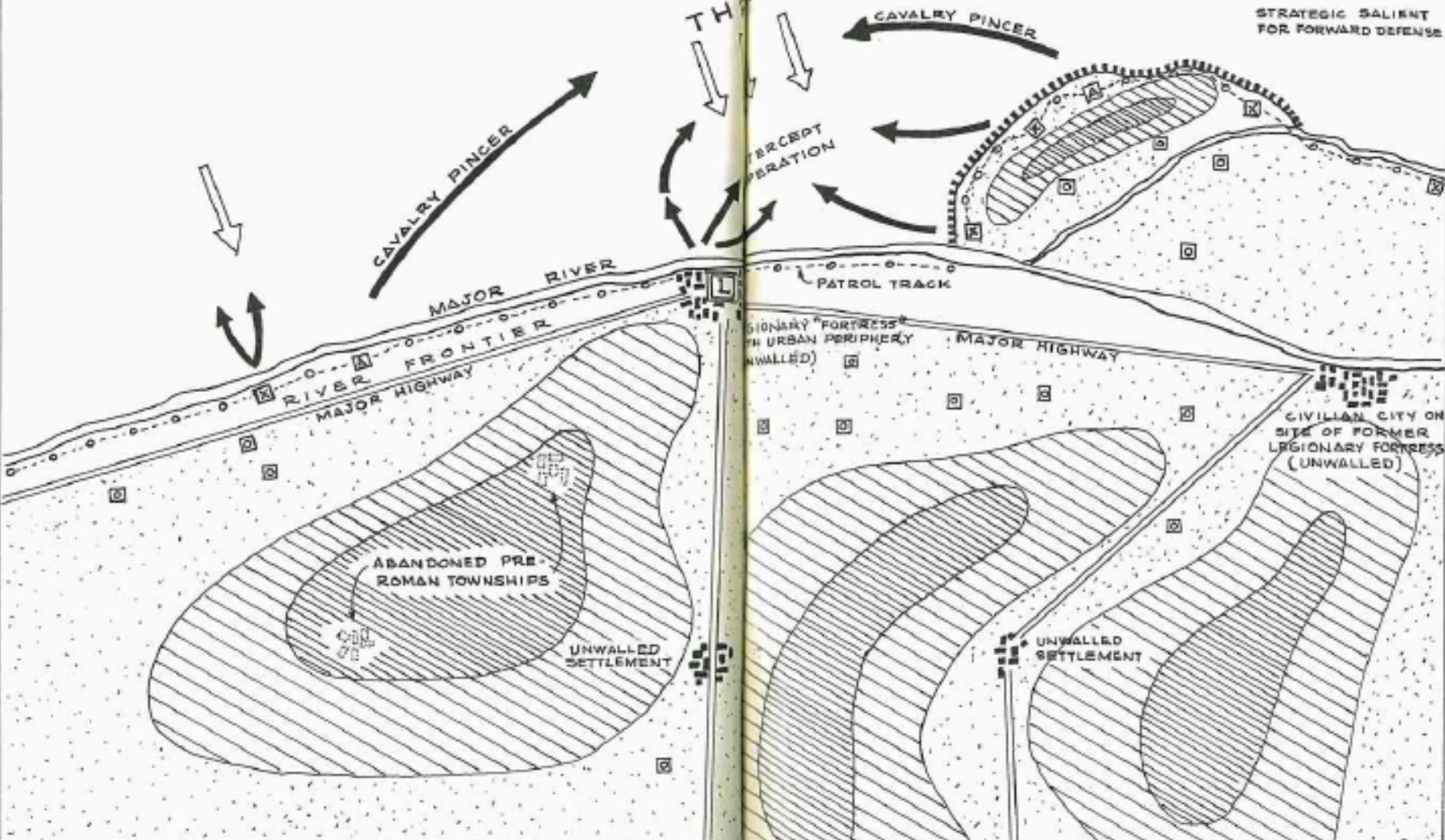


LEGEND

- LEGIONARY BASE CONVERTED INTO (MUCH SMALLER) FORTRESS WITH FIGHTING TOWERS, ELEVATED FLOORS, ETC.
- DITTO FOR AUXILIARY FORT
- WALLED TOWN
- FORTIFIED FARMHOUSE
- ROAD FORT
- WATCHTOWER
- FORTIFIED GOVERNMENT GRANARY



STRATEGIC SALIENT FOR FORWARD DEFENSE



LEGEND

- LEGIONARY "FORTRESS" (BASE)
- ALA FORT
- COHORT FORT
- GUARD POST
- FARM HOUSE
- AGRICULTURAL LAND (ARABLE)
- HIGH GROUND
- HIGHER GROUND



INSAG-10

Defence in Depth in Nuclear Safety

INSAG-10

A REPORT BY THE
INTERNATIONAL NUCLEAR SAFETY ADVISORY GROUP

INSAG

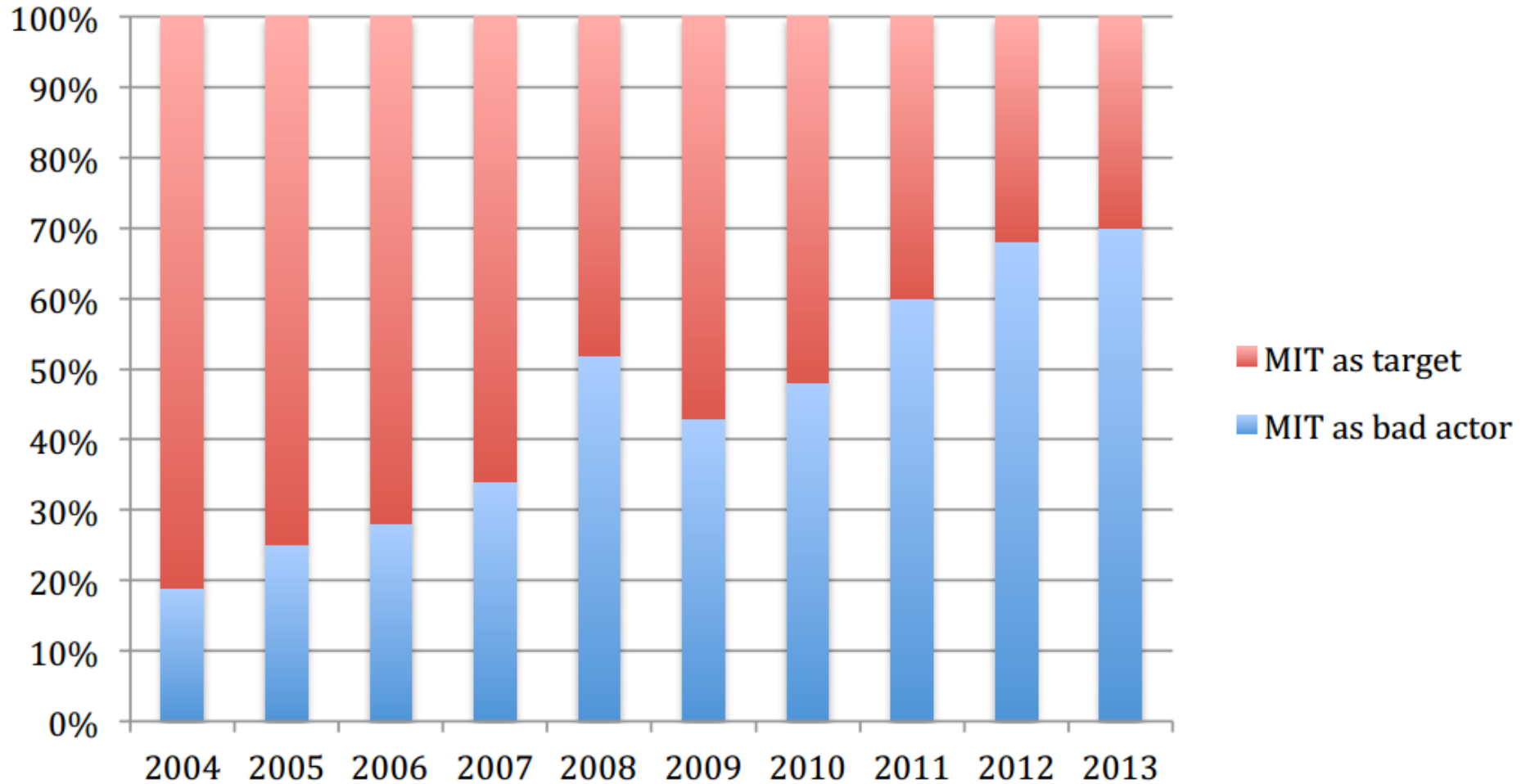


IAEA

TABLE I. LEVELS OF DEFENCE IN DEPTH

Levels of defence in depth	Objective	Essential means
Level 1	Prevention of abnormal operation and failures	Conservative design and high quality in construction and operation
Level 2	Control of abnormal operation and detection of failures	Control, limiting and protection systems and other surveillance features
Level 3	Control of accidents within the design basis	Engineered safety features and accident procedures
Level 4	Control of severe plant conditions, including prevention of accident progression and mitigation of the consequences of severe accidents	Complementary measures and accident management
Level 5	Mitigation of radiological consequences of significant releases of radioactive materials	Off-site emergency response

MIT as Target vs. Bad Actor



Actions

Outcomes

Reporting

Actions

Outcomes

Reporting

Software industry

Hardware industry

Service providers

Content providers

Payment processors

DNS operators

Web hosts

End users

Software industry

Hardware industry

Service providers

Content providers

Payment processors

DNS operators

Web hosts

End users

Actions

Code review/testing process

Testing or audit requirements

Inspect and drop malicious traffic

Review or notice and takedown process

Flag fraud to look for patterns

DNSSEC deployment

Notice and takedown process

Patch systems

Outcomes

Fewer errors/exploits, rapid patching

Reduce counterfeit hardware

Reduce bots, clean infected machines

Rapid removal of abusive content

Reduce fraudulent payments

Fewer corrupt records, rapid removal

Rapid removal of abusive content

Avoid being part of DDoS attacks

Reporting

Bugs, exploits, exploit signatures

Flaws, exploits

Bots, DoS attacks, malicious traffic signatures

Abusive content incidents, signatures

Financial fraud cases

DoS, corruption incidents

Abusive sites, modes of payment

Infection vector

Actions

Outcomes

Reporting

Future Work

- Empirical analysis of the impact of new security measures (particularly combinations of security measures)
- Effect of cybersecurity policies and regulations on incidence and cost of cybercrime
- Characterizing defense independence scale for issuers of cyberinsurance

Identity indicators

Identity indicator	Barrier created for intruders	Vulnerabilities of the indicator	Work required to exploit vulnerabilities
Code signature	Cannot reuse known malware to infect new computers	Unable to detect new malware until it has been exploited/used	Programming new malware that does not use older code signatures
Domain	Cannot reuse known domains for phishing/malicious communications	Unable to detect new domains before they are set up and used in a malicious manner	Purchasing and setting up new domains
Certificate	Cannot reuse known fraudulent certificates	Unable to detect new fraudulent certificates	Purchasing/acquiring new certificate
Authentication credential (e.g. password, one-time code, biometric)	Cannot access capabilities without figuring out or stealing credentials	Credentials may be stolen, imitated, or guessed by bad actors to exploit protected capabilities	Stealing, imitating, or guessing the required credentials

Behavioral indicators

Behavioral indicator	Barrier created for intruders	Vulnerabilities of the indicator	Work required to exploit vulnerabilities
Sending executable files as attachments	More difficult to transmit malware via email	Other interfaces for transmitting malware, recognizing file type	Disguising executable files as other types, identifying alternative pathway
Repeated, regularly scheduled contact with unknown servers	More difficult to maintain regularly scheduled communication with compromised systems	Relies on communication with malicious servers happening at routine intervals and consistent addresses	Disguising or changing communicating servers and varying the timing of communication with compromised systems
Unusually large volume of standard activity (e.g., queries, login attempts, exfiltrated data)	Harder to execute capabilities in large volume (large-scale denial-of-service, dictionary attacks, or espionage)	Requires setting some limit under which malicious activity may not be detected, allowing attackers to operate just below that limit	Figuring out the volume limitations and then just meeting, but not exceeding, them
Standard activity originating from or going to unusual source/destination	Attackers must take time to establish some familiarity of their tools/resources with target	Source and destination identifiers may be forged or manipulated to appear familiar	Disguising or introducing source/ destination identifiers to targets gradually so they are considered trusted

Research questions

- How do we define defense-in-depth in the context of computer systems?
- What classes of defense can we identify and how can they be combined to build design patterns for computer systems?
- What are the implications of these classes for different actors in the security ecosystem and their defensive responsibilities and investments?

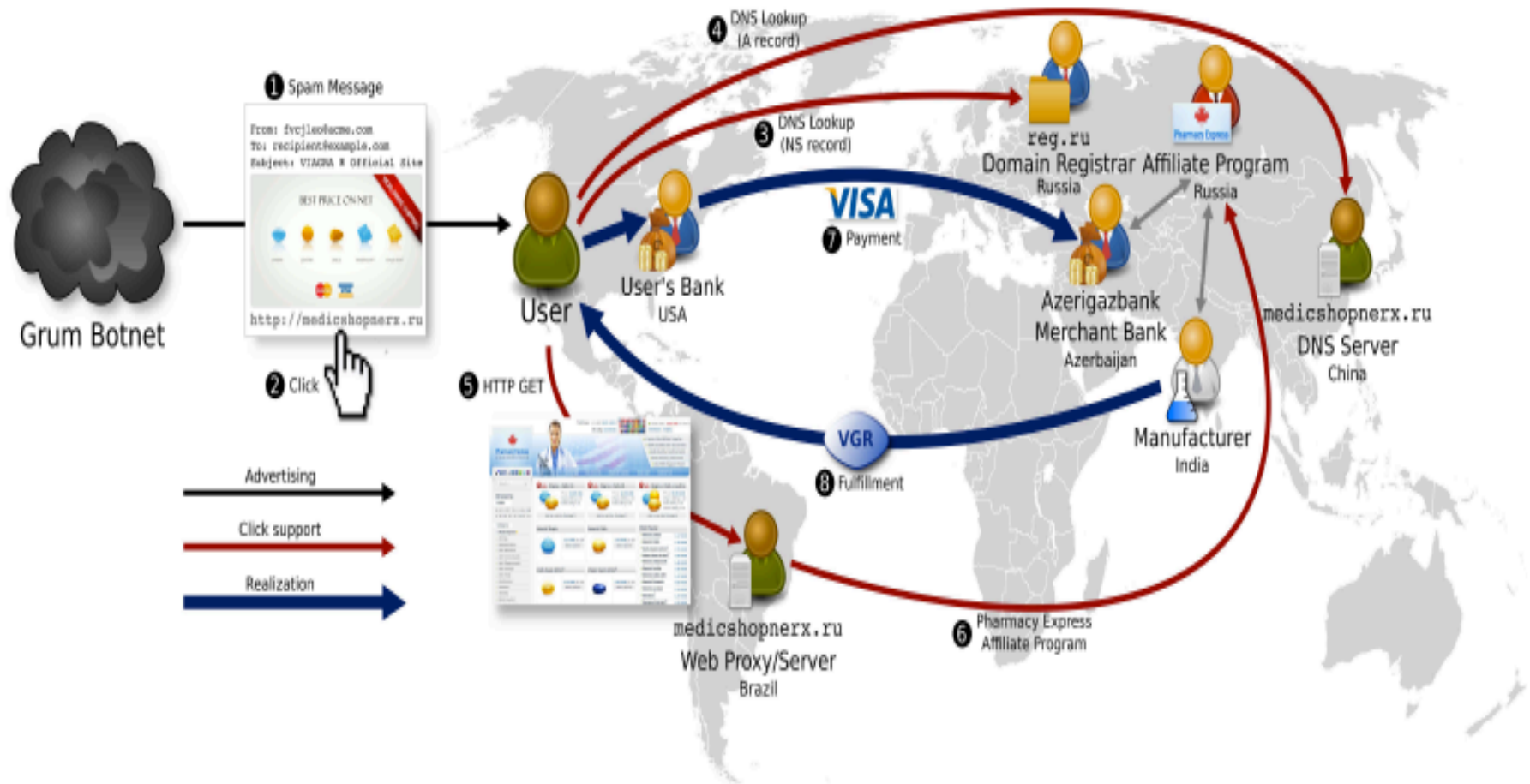
Defining defense-in-depth for computer systems

- Defense-in-depth is the combination of security mechanisms that are both *independent* and *overlapping*
 - a single attack would be unlikely to compromise all of the security mechanisms simultaneously
 - all of the security mechanisms must be compromised for an attack to be successfully carried out

Degrees of Independence

- No two mechanisms can ever be completely independent; their degree of independence is defined by their common sphere of dependence (e.g., an operating system, a person, a network, a company, etc.) and how difficult that sphere is to compromise
 - The larger the sphere (i.e., that more difficult it is to compromise), the more independent the defenses

Spam Click Value Chain Analysis (Levchenko et al., 2011)



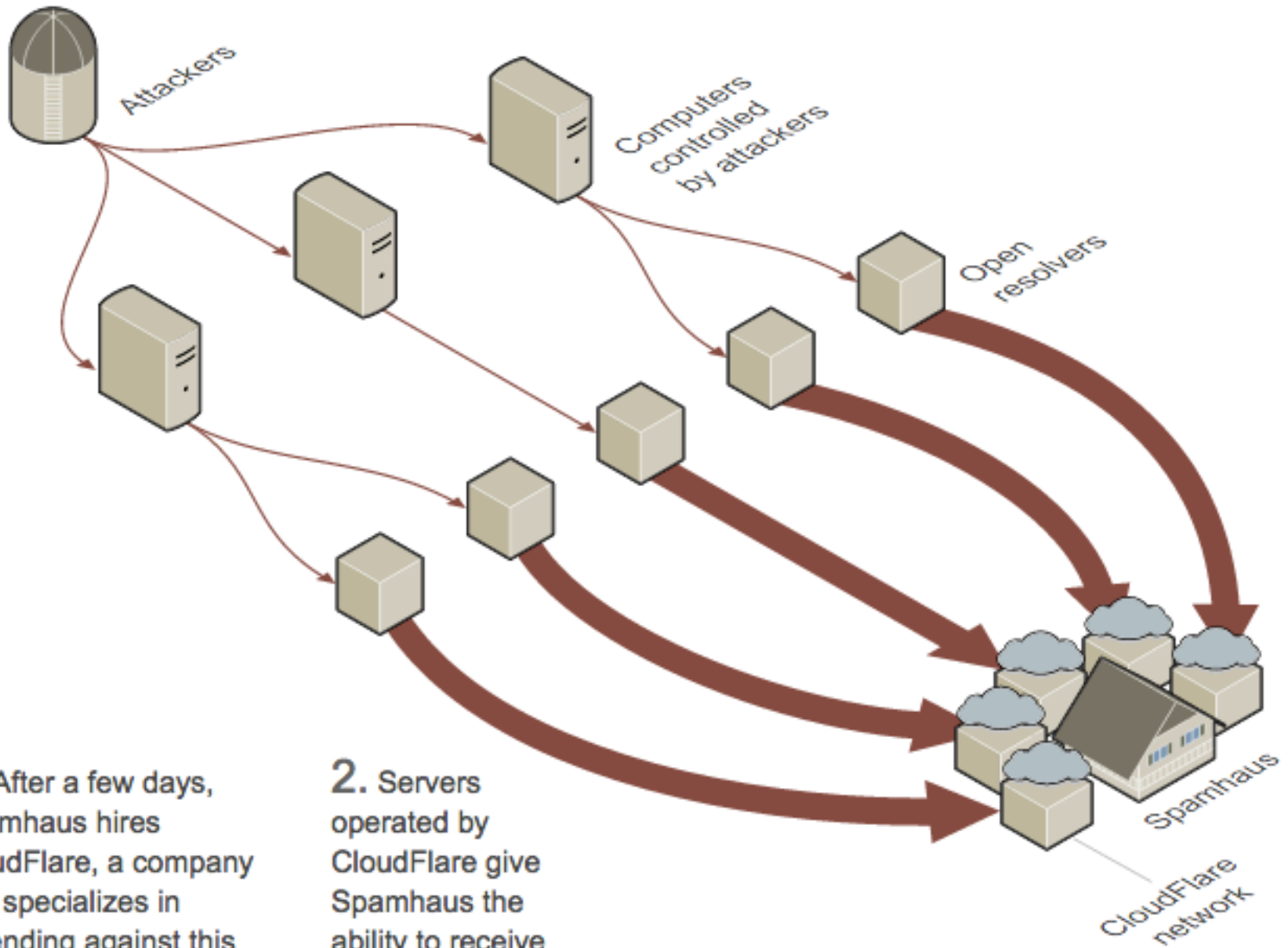
Identifier	Class
FAU	Security Audit
FCO	Communication
FCS	Cryptographic Support
FDP	User Data Protection
FIA	Identification and Authentication
FMT	Security Management
FPR	Privacy
FPT	Protection of Security Functionality
FRU	Resource Utilization
FTA	Access
FTP	Trusted Path/Channels

ISO/IEC 15408: Common Criteria for Information Technology Security Evaluation

Essential capabilities for digital harm

- Two classes of incidents that are largely dependent on access defenses—denial-of-service attacks and espionage—suggest two types of behavioral indicators that may be valuable for distinguishing between malicious and legitimate activity:
 - Volume
 - Data exfiltration
- Mitigation may involve inserting new intermediate steps and monitoring third parties

The Response



1. After a few days, Spamhaus hires CloudFlare, a company that specializes in defending against this kind of cyberattack.

2. Servers operated by CloudFlare give Spamhaus the ability to receive more traffic.

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	AM	Asset Management
		BE	Business Environment
		GV	Governance
		RA	Risk Assessment
		RM	Risk Management
PR	Protect	AC	Access Control
		AT	Awareness and Training
		DS	Data Security
		IP	Information Protection Processes and Procedures
		PT	Protective Technology
DE	Detect	AE	Anomalies and Events
		CM	Security Continuous Monitoring
		DP	Detection Processes
RS	Respond	CO	Communications
		AN	Analysis
		MI	Mitigation
		IM	Improvements
RC	Recover	RP	Recovery Planning
		IM	Improvements
		CO	Communications

Defense-in-depth

- We need to know how different defenses fit together because we know that we can't rely on just one
- This leads to the notion of “defense-in-depth” or assembling multiple defenses with orthogonal vulnerabilities



Classes of defense

- We use a variety of different tools and mechanisms to defend computer systems against abuse or attacks:
 - Encryption
 - Firewalls
 - Certificates
 - Anti-virus programs
 - Password complexity requirements
 - Multi-factor authentication

How do these defenses fit together?

- There is considerable work on each of these individual areas of defense, but very little that helps defenders understand:
 - How they relate to each other, or how each individual defense augments the others and fits into a broader strategy
 - What a group of security mechanisms does (and does not) defend against in aggregate

Information Assurance Through DEFENSE IN DEPTH



February 2000

20000523 141

InformationWeek

THE BUSINESS VALUE OF TECHNOLOGY

FEB. 22, 2010



Time For A New Strategy

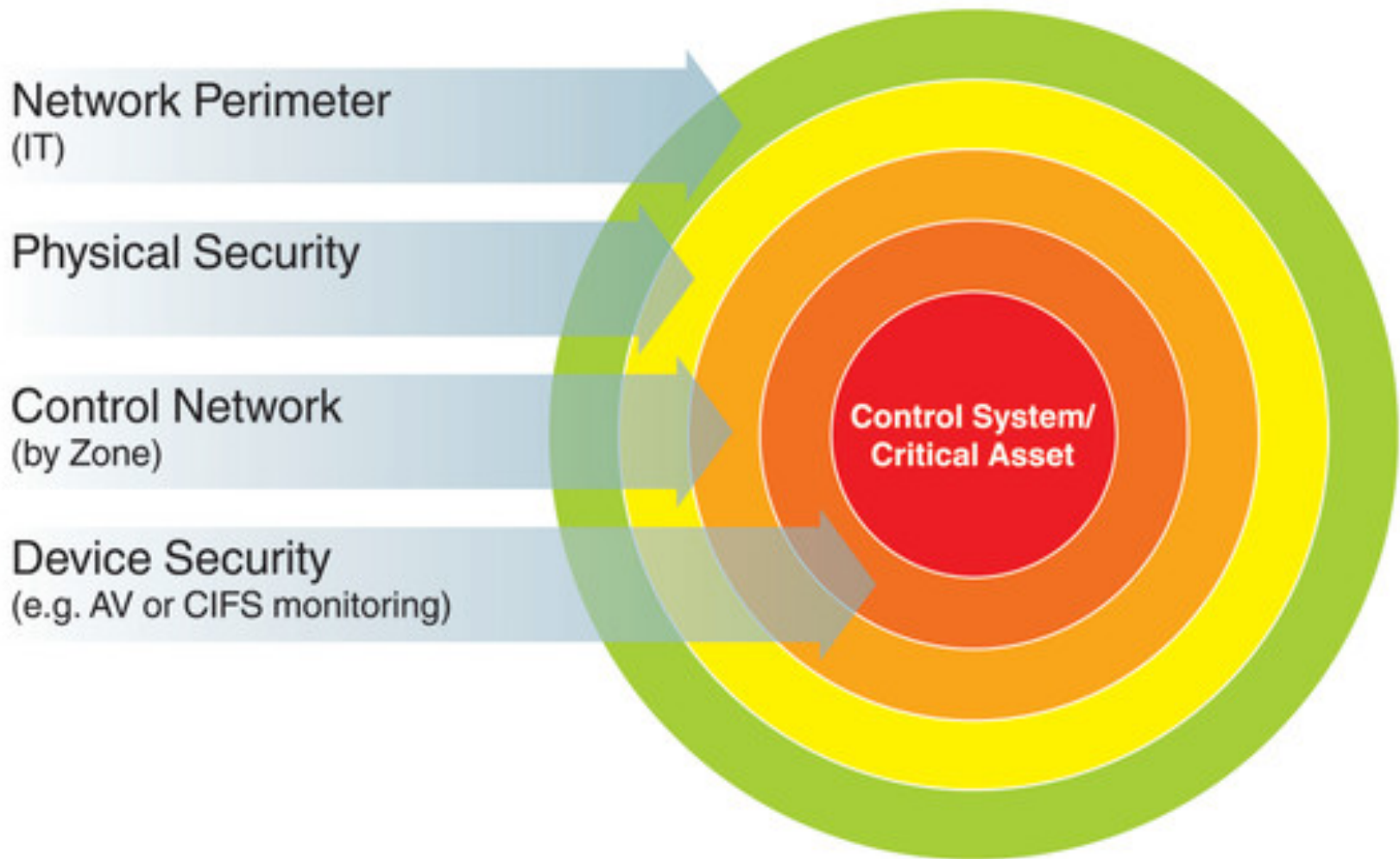
If you think walls will keep your treasured data secure, you're living in a fairy tale p.29

By Michael A. Davis

Information Assurance Through Defense-in-Depth (2000)

- Defense-in-depth is:
 - increasing and strengthening defensive barriers as well as providing targets with the means to fight back actively;
 - when multiple different types of defensive mechanisms are deployed in concert (people, operations, technology);
 - when multiple different elements of computer systems are protected (enclaves, enclave boundaries, networks linking enclaves, and supporting infrastructures);
 - when every means of attacking a computer system is protected against;
 - when several defenses are arranged to be encountered sequentially so that an attacker must overcome all of them in order to be successful;
 - when the vulnerabilities of each defense are reinforced by other defenses with different vulnerabilities that cannot be exploited in the same manner.

Defense in Depth





CONFIDENTIALITY

INTEGRITY

AVAILABILITY

10 essential practices— cyber security defense in depth



Phase	Detect	Deny	Disrupt	Degrade	Deceive	Contain
Reconnaissance	Web Analytics	Firewall ACL				Firewall ACL
Weaponization	NIDS	NIPS				NIPS
Delivery	Vigilant User	Proxy Filter	Inline AV	Queuing		App-Aware Firewall
Exploitation	HIDS	Patch	DEP			Inter-Zone NIPS
Installation	HIDS	'chroot' Jail	AV			EPP
Command & Control	NIDS	Firewall ACL	NIPS	Tarpit	DNS Redirect	Trust Zones
Actions on Targets	Audit Logs	Outbound ACL	DLP	Quality of Service	Honeypot	Trust Zones



Defense In Depth Strategy

People

Technology

Operations

Defense in Depth Focus Areas

**Defend the
Network &
Infrastructure**

**Defend the
Enclave
Boundary**

**Defend the
Computing
Environment**

**Supporting
Infrastructures**

KM/PKI

**Detect &
Respond**

What classes of defense do we use?

Identifier	Family	Class
AC	Access Control	Technical
AT	Awareness and Training	Operational
AU	Audit and Accountability	Technical
CA	Security Assessment and Authorization	Management
CM	Configuration Management	Operational
CP	Contingency Planning	Operational
IA	Identification and Authentication	Technical
IR	Incident Response	Operational
MA	Maintenance	Operational
MP	Media Protection	Operational
PE	Physical and Environmental Protection	Operational
PL	Planning	Management
PS	Personnel Security	Operational
RA	Risk Assessment	Management
SA	System and Services Acquisition	Management
SC	System and Communications Protection	Technical
SI	System and Information Integrity	Operational
PM	Program Management	Management

Inventory of Authorized and Unauthorized Devices
Inventory of Authorized and Unauthorized Software
Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
Continuous Vulnerability Assessment and Remediation
Malware Defenses
Application Software Security
Wireless Device Control
Data Recovery Capability
Security Skills Assessment and Appropriate Training to Fill Gaps
Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
Limitation and Control of Network Ports, Protocols, and Services
Controlled Use of Administrative Privileges
Boundary Defense
Maintenance, Monitoring, and Analysis of Security Audit Logs
Controlled Access Based on the Need to Know
Account Monitoring and Control
Data Loss Prevention
Incident Response Capability
Secure Network Engineering
Penetration Tests and Red Team Exercises

Twenty Critical Controls for Effective Cyber Defense

Critical Security Control	Corresponding NIST 800-53 Controls
Inventory of Authorized and Unauthorized Devices	CM-8 (a, c, d, 2, 3, 4), PM-5, PM-6
Inventory of Authorized and Unauthorized Software	CM-1, CM-2 (2, 4, 5), CM-3, CM-5 (2, 7), CM-7 (1, 2), CM-8 (1, 2, 3, 4, 6), CM-9, PM-6, SA-6, SA-7
Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers	CM-1, CM-2 (1, 2), CM-3 (b, c, d, e, 2, 3), CM-5 (2), CM-6 (1, 2, 4), CM-7 (1), SA-1 (a), SA-4 (5), SI-7 (3), PM-6
Continuous Vulnerability Assessment and Remediation	RA-3 (a, b, c, d), RA-5 (a, b, 1, 2, 5, 6)
Malware Defenses	SC-18, SC-26, SI-3 (a, b, 1, 2, 5, 6)
Application Software Security	CM-7, RA-5 (a, 1), SA-3, SA-4 (3), SA-8, SI-3, SI-10
Wireless Device Control	AC-17, AC-18 (1, 2, 3, 4), SC-9 (1), SC-24, SI-4 (14, 15)
Data Recovery Capability	CP-9 (a, b, d, 1, 3), CP-10 (6)
Security Skills Assessment and Appropriate Training to Fill Gaps	AT-1, AT-2 (1), AT-3 (1)
Secure Configurations for Network Devices such as Firewalls, Routers, and Switches	AC-4 (7, 10, 11, 16), CM-1, CM-2 (1), CM-3 (2), CM-5 (1, 2, 5), CM-6 (4), CM-7 (1, 3), IA-2 (1, 6), IA-5, IA-8, RA-5, SC-7 (2, 4, 5, 6, 8, 11, 13, 14, 18), SC-9
Limitation and Control of Network Ports, Protocols, and Services	CM-6 (a, b, d, 2, 3), CM-7 (1), SC-7 (4, 5, 11, 12)
Controlled Use of Administrative Privileges	AC-6 (2, 5), AC-17 (3), AC-19, AU-2 (4)
Boundary Defense	AC-17 (1), AC-20, CA-3, IA-2 (1, 2), IA-8, RA-5, SC-7 (1, 2, 3, 8, 10, 11, 14), SC-18, SI-4 (c, 1, 4, 5, 11), PM-7
Maintenance, Monitoring, and Analysis of Security Audit Logs	AC-17 (1), AC-19, AU-2 (4), AU-3 (1,2), AU-4, AU-5, AU-6 (a, 1, 5), AU-8, AU-9 (1, 2), AU-12 (2), SI-4 (8)
Controlled Access Based on the Need to Know	AC-1, AC-2 (b, c), AC-3 (4), AC-4, AC-6, MP-3, RA-2 (a)
Account Monitoring and Control	AC-2 (e, f, g, h, j, 2, 3, 4, 5), AC-3
Data Loss Prevention	AC-4, MP-2 (2), MP-4 (1), SC-7 (6, 10), SC-9, SC-13, SC-28 (1), SI-4 (4, 11), PM-7
Incident Response Capability	IR-1, IR-2 (1), IR-4, IR-5, IR-6 (a), IR-8
Secure Network Engineering	IR-4 (2), SA-8, SC-7 (1, 13), SC-20, SC-21, SC-22, PM-7,
Penetration Tests and Red Team Exercises	CA-2 (1, 2), CA-7 (1, 2), RA-3, RA-5 (4, 9), SA-12 (7)

Classification inconsistencies

- Categories like “boundary defense,” “data loss prevention,” “penetration tests,” “wireless device control,” and “secure configuration” are presented in parallel, switching between classifying defenses by:
 - what piece of the network they protect
 - what they aim to protect against
 - how they are tested
 - what type of devices they apply to
 - whether or not they are properly configured

Confidentiality, Integrity, Availability

- The existing catalogs and classifications of defense reflect a lack of organizing high-level principles
- While confidentiality, integrity and availability are certainly desirable properties of a secure computer system, we can't actually sort out defenses that address each of those components individually