Cybersecurity Challenges and Opportunities

Governance of Technology, Information, and Policies
December 6th, 2011

Edward B. Talbot

Distinguished Member of the Technical Staff

Sandia National Laboratories, Livermore CA

ebtalbo@sandia.gov

edward.talbot@gmail.com

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.
SAND Number: 2011-8889P

Outline

- A Thought Experiment
  - Are we doing cybersecurity wrong?
- The Exemplar Threat
  - The Insider
- Full-scope Cybersecurity
- Effective Cybersecurity

Outline

- A Thought Experiment
  - Are we doing cybersecurity wrong?
- The Exemplar Threat
  - The Insider
- Full-scope Cybersecurity
- Effective Cybersecurity

"…U.S. networks are "as porous as a colander," Richard Clarke, the former White House counterterrorism chief turned cybersecurity Cassandra, told a packed ballroom."

http://www.wired.com/dangerroom/2011/11/darpa-hackers-cybersecurity/

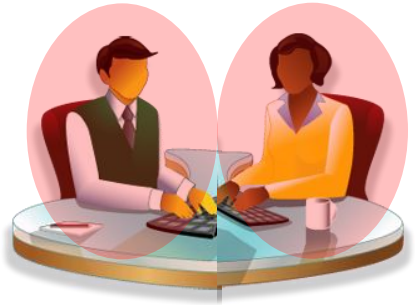
Analyst, Administrator or Adversary?

- "To do my job, I need the following for all web traffic entering or leaving your site:
  - I need access to every packet.
  - I need the time-history of the traffic.
  - I need tools so I can analyze the data."
- Analysts, administrators, and adversaries desire the same resources.
- Analysts, administrators, and adversaries pose similar threats to cybersecurity.

"In US Criminal law, **means**, **motive**, and **opportunity** is a popular cultural summation of the three aspects of a crime needed to convince a jury of guilt in a criminal proceeding."

Source: http://en.wikipedia.org/wiki/Means,_motive,_and_opportunity

Are we doing cybersecurity wrong?



"Critical Control 9: Controlled Access Based on the Need to Know"

- http://www.sans.org/critical-security-controls/control.php?id=9

Probability of compromise increases with each "monitor" (program, administrator, analyst,…) that is added to the communication path.

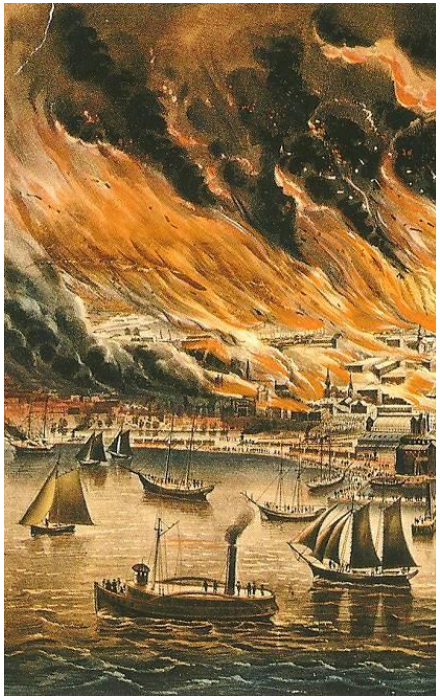
Are detection and protection mutually exclusive?

- Increased **detection**:
  - ***may*** increase the probability that a bad guy will be discovered and caught.
  - ***will*** increase the probability that data will be compromised.

- Improved user **protection**:
  - ***will*** decrease the probability that data will be compromised.
  - ***may*** enable compromise without detection.

Any system that is capable of ***detecting*** all that is going on inside of it is capable of ***revealing*** all that is going on inside of it.

The Thought Experiment in Perspective: Moving from Fire *Fighting* to Fire *Science*



Chicago, 1871

NFPA®

San Francisco, 1906

A Thought Experiment

A comprehensive approach to cybersecurity has multiple timeframes and objectives.

NEAR TERM: *Put the fire out ....*

Strong Kerberos Passwords
Upgrade and Patch
Better Education of Users

Improve HYGIENE

MID TERM: *Install fire suppression sprinklers ...*

Model Adversaries, Their Operations, and Develop Deterrence Strategies
Make Cyber Security Easier, Clearer and More Intuitive
Develop Robust Cultural Security Metaphors

Create a Cyber Security CULTURE

LONG TERM: ***Intrinsically fireproof buildings***

Complex Systems, Informatics, Information Theory
Systems Engineering, Risk Management
Human, Economic, Legal Systems

Develop and Apply Cyber Security SCIENCE

Outline

- A Thought Experiment
  - Are we doing cybersecurity wrong?
- The Exemplar Threat
  - The Insider
- Full-scope Cybersecurity
- Effective Cybersecurity

"The *self-fulfilling prophecy* is, in the beginning, a *false* definition of the situation evoking a new behavior which makes the original false conception come 'true'."

- *Social Theory and Social Structure*, Robert K. Merton

User actions can defeat the strongest security system.

The Ottomans laid siege to Constantinople in April 1453.

After two months of unsuccessful attempts to breach the city walls, the Ottomans discovered an **unlocked** gate.

The Ottomans rushed in and conquered the city.

Users are the critical element in any security strategy.

"Errant Keystrokes" can be caused by malevolent, manipulated, or confused users.

"…the turbine room of the Shushenskaya hydroelectric power plant before **errant keystrokes** by the operator of a remote cybernetwork turned on a disused turbine and created a disaster."

"The disused turbine created a "water hammer" that destroyed the facility, killed dozens of workers and tore the machinery out of it's mountings… Military officials fear that such effects can be created by hackers or cyberwarriors."

Quote Source: "Cyber Deluge," Aviation Week and Space Technology, May 23, 2011, p.42

Photo Source: http://www.bigpicture.in/the-sayano-shushenskaya-dam-accident/

Insider Threat Observations

- Intent is the only certain way to distinguish between benign and malicious insiders.
  - Intent is devilishly hard to determine.
  - Manipulated or confused insiders are equivalent to malicious insiders.
- In cyberspace, smart and/or well-resourced people will always be able to redirect attribution to the not-so-smart or well-resourced.
  - There is no physicality in cyberspace.
  - Any conclusion reached based solely on cyber data is subject to deception.

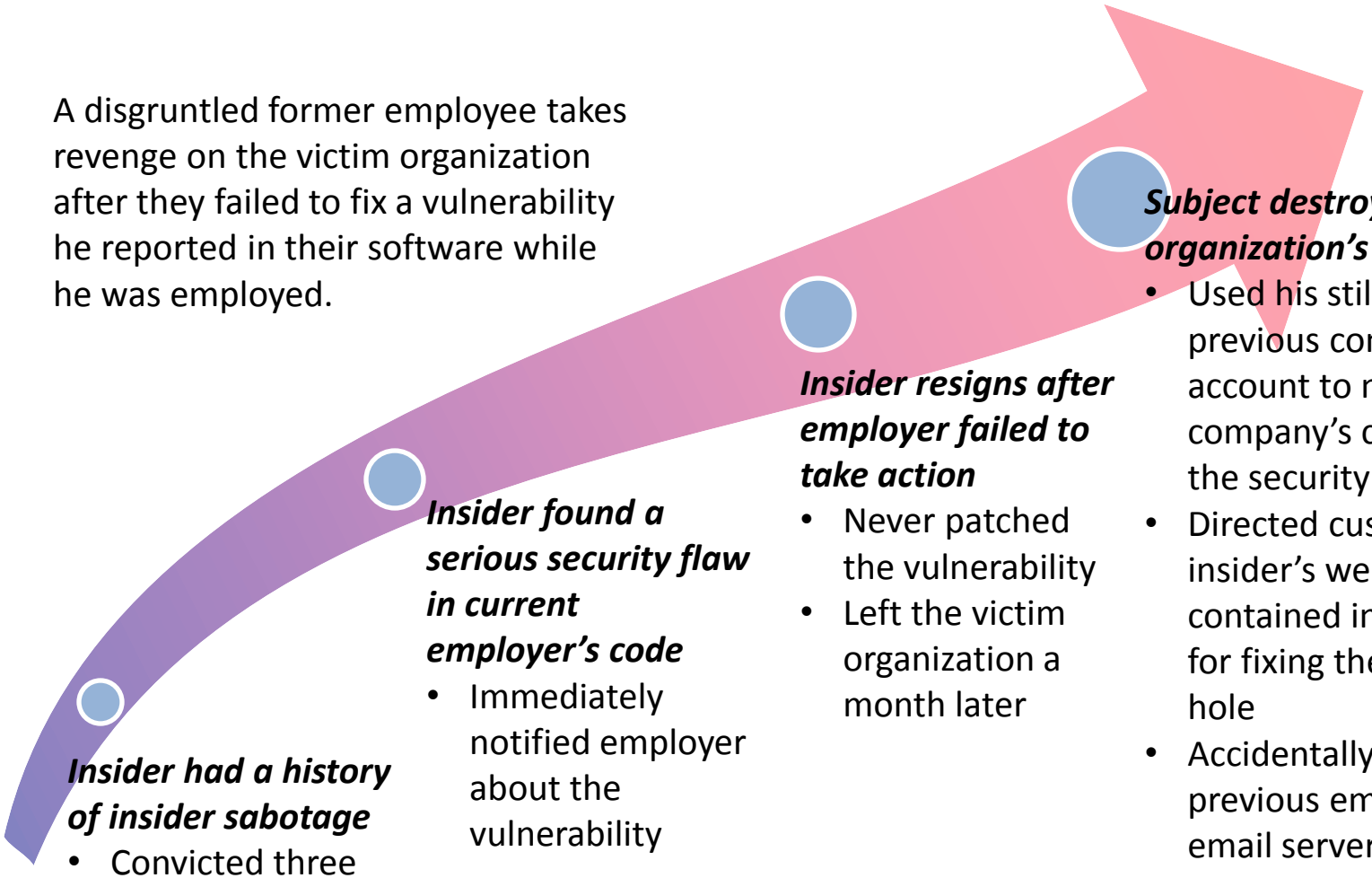
"Beyond a Reasonable Doubt:

The standard that must be met by the prosecution's evidence in a criminal prosecution: that no other logical explanation can be derived from the facts except that the defendant committed the crime, thereby overcoming the presumption that a person is innocent until proven guilty."

Source: http://legal-dictionary.thefreedictionary.com/Beyond+a+Reasonable+Doubt

"Generic" Insider Threat Model

A disgruntled former employee takes revenge on the victim organization after they failed to fix a vulnerability he reported in their software while he was employed.



Insider had a history of insider sabotage

- Convicted three years earlier at a previous employer

Insider found a serious security flaw in current employer's code

- Immediately notified employer about the vulnerability

Insider resigns after employer failed to take action

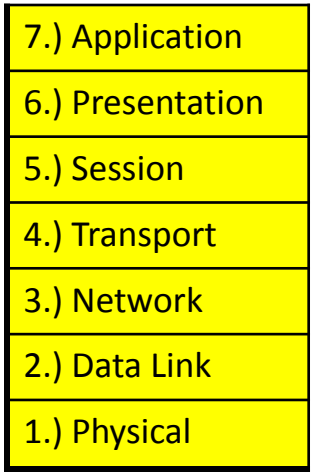
- Never patched the vulnerability
- Left the victim organization a month later

Subject destroyed organization's reputation

- Used his still-active previous company email account to notify the company's customers of the security flaw
- Directed customers to insider's website, which contained instructions for fixing the security hole
- Accidentally crashed previous employer's email servers
- Victim organization went out of business

The content of this slide was collected strictly from publicly available information.
(from http://www.cert.org/insider_threat/)

The insider threat is out-of-scope for current cybersecurity thinking.



- "Base Rate Fallacy":
  - The small proportion of insiders in a largely law-abiding population makes even a system with a very low false positive rate useless in practice.
- User frustration and confusion are unintended consequences of using limited scope rules to address an out-of-scope problem.
- The insider threat is a cybersecurity "Black Swan."

Outline

- A Thought Experiment
  - Are we doing cybersecurity wrong?
- The Exemplar Threat
  - The Insider
- Full-scope Cybersecurity
- Effective Cybersecurity

"That means, to use a hackneyed phrase, a “new paradigm,” according to Gen. Keith Alexander, who leads U.S. Cyber Command, the military organization devoted to active, day-to-day defense of military networks. “We diagnose the malware, clean up the systems, get set up again and wait for the next exploitation. We have to change the way we think about defending our systems.”

http://www.wired.com/dangerroom/2011/11/darpa-hackers-cybersecurity/

Full-scope cybersecurity addresses all systemic vulnerabilities *and* the insider threat.

HMI
Perception
Cognition
Experience

Authorities
Expectations
Incentives

15	Human
14	Cultural Norms
13	Social Norms
12	Organizational Roles
11	7.) Application
10	6.) Presentation
9	5.) Session
8	4.) Transport
7	3.) Network
6	2.) Data Link
5	1.) Physical
4	System Hardware (Motherboard, etc.)
3	Component (ICs…)
2	Semiconductor Physics
1	Atomic

Less predictable
Larger Error Bars
Less Deterministic

Example Layer 12-15 Vulnerabilities:
- Spear-phishing
- Social engineering

Traditional, *limited-scope* cybersecurity

More Certain
Smaller Error Bars
More Deterministic

Example Layer 1-4 Vulnerabilities:
- Supply Chain Attacks

Full-scope cybersecurity acknowledges that insiders can be *hired*, *ordered* or *created*.

Hired

Paycheck

Hiring and Recruiting

Benign

Poor Treatment and Incentives

Created

Poor Business Processes, Support, and Training

Ordered

Deliberate Malicious Insider (Intentional)

Manipulated Malicious Insider (Unknowing)

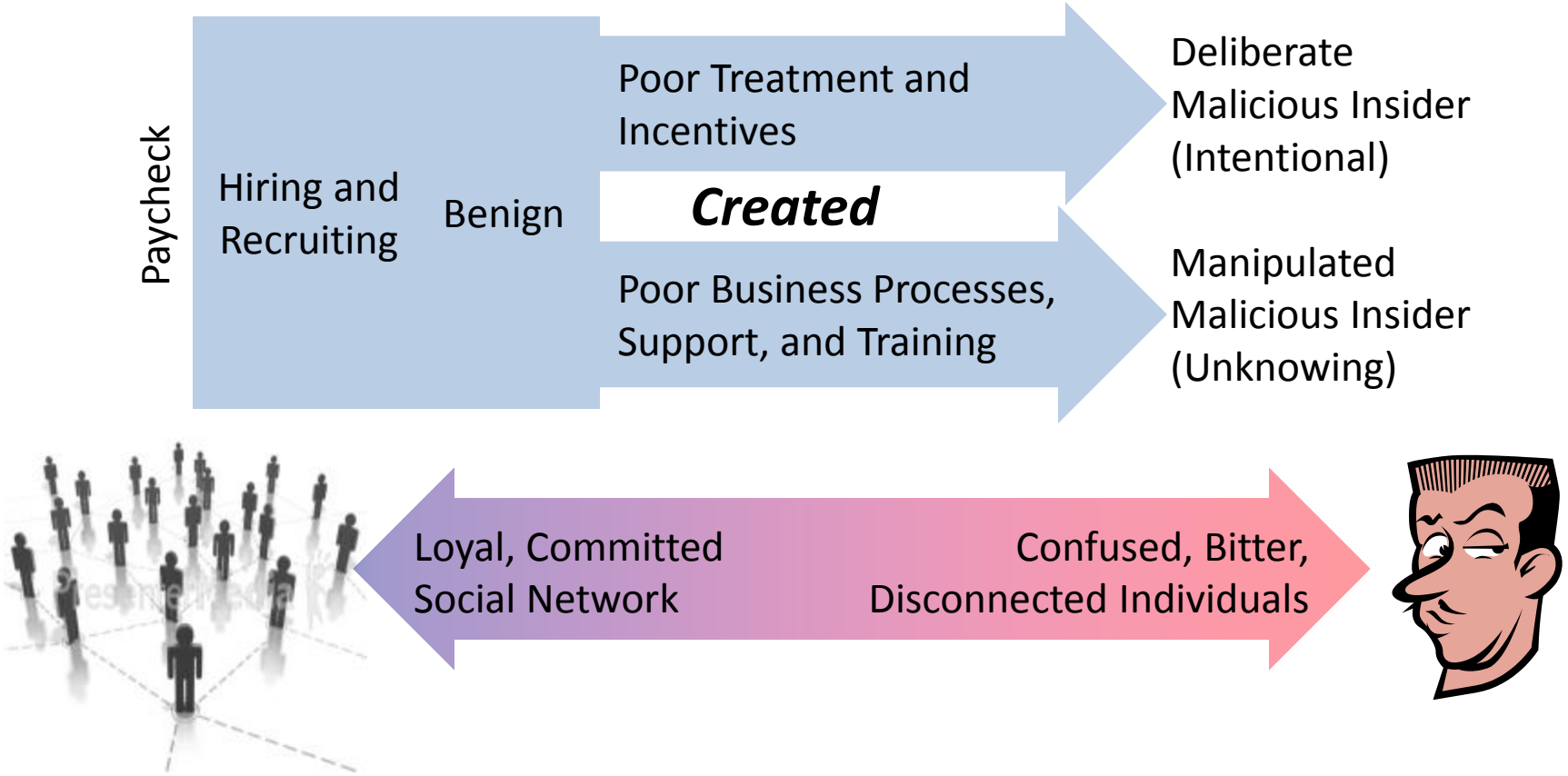
Purchase Order

Requisitions and Contracts

Service, Supplies, and Equipment

Solutions to the insider threat problem may lie predominantly **outside** the purview of traditional cybersecurity practice.

Limited scope strategies transform a loyal and committed workforce to a confused and/or bitter set of vulnerabilities.



"The *self-fulfilling prophecy* is, in the beginning, a *false* definition of the situation evoking a new behavior which makes the original false conception come 'true'."

- *Social Theory and Social Structure*, Robert K. Merton

What message does this banner convey?

A Generic Login Banner:

WARNING NOTICE TO USERS: Systems Are Monitored

---------- **Be aware you have no privacy on these systems.** ----------

All users of this system and all information on this system are subject to interception, monitoring, recording, copying, auditing, and inspection at our discretion, and disclosure to us and third parties, including, but not limited to, the United States Government, any authorized investigative and law enforcement personnel, and officials of other entities, both domestic and foreign. By using or accessing this system, you consent to and permit all of the above without limit as to when such action may be undertaken.

Unauthorized or improper use of this system may result in disciplinary, administrative, civil, and/or criminal penalties.

Outline

- A Thought Experiment
  - Are we doing cybersecurity wrong?
- The Exemplar Threat
  - The Insider
- Full-scope Cybersecurity
- Effective Cybersecurity

"We can have all the records in the world and if somebody wants to trade outside them or something, you know, they're not going to tell us they're trading in their cousin's name," [Warren Buffett's partner Charlie] Munger said. "I think your best compliance cultures are the ones which have this attitude of trust and some of the ones with the biggest compliance departments, like Wall Street, have the most scandals."

http://articles.economictimes.indiatimes.com/2011-05-03/news/29499643_1_charlie-munger-warren-buffett-berkshire-hathaway

Absolute Certainty is Unobtainable

Loyal, Committed Social Network

Confused, Bitter, Disconnected Individuals

No Certainty

Know Little — Know "Everything"

Know Trust — No Trust

Step 1: "We admitted we were powerless [over alcohol]—that our lives had become unmanageable." – from http://en.wikipedia.org/wiki/12-step_program

Effective Cybersecurity

Are the processes we are putting in place to *detect* this threat…

…inadvertently resulting in the *creation* of this threat?




- What doesn't work (by itself):
  - Enforcement/compliance/oversight/governance…
  - Physical controls (guards, gates, guns,…)
  - Cyber controls (access controls, IDS,…)
- What works – "attitude of trust":
  - Develop and cultivate trust, loyalty and accountability.

Are we doing cybersecurity wrong?

Opportunity: Balance ***detection*** with user ***protection.***

Changing the cybersecurity dialog.

- From: “How can we detect adversarial activity on our networks?”
- To: “How can we protect users (information, privacy, civil liberties…) from adversarial actions?”
  - Includes detection of adversaries.

“… structural reforms to ensure responsible sharing and safeguarding of classified information on computer networks that shall be consistent with appropriate protections for privacy and civil liberties.”

Executive Order 13587, “Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information” (aka the “Wikileaks Executive Order”), issued by the President on 7 October 2011

A Notional User Protection System

- Non-betrayal – data cannot be used against the users will.
- Privacy – user control over all data.
- Anonymity – adversary is provably unlikely to extract useful data.
- Non-attribution – forensics pushed to the physical endpoints.
- Non-persistence – no trace remains of data transferred.
- Strong authentication – at all endpoints, as certain as the real world (endpoint and real world equivalence).

Summary: Cybersecurity Challenges and Opportunities

- Cybersecurity as it is practiced today is limited in scope.
  - Ignores significant vulnerability space.
- Full-scope cybersecurity is based on what people (and systems) actually do.
  - Not what we wish they did.
  - A focus on user protection supports users.
- People respond favorably to interesting challenges, positive incentives and being treated well.
  - **Effective** cybersecurity develops a culture of trust, loyalty and accountability through positive incentives and fairness.

- What would a ***user-protection system*** look like?
  - What governance and policy changes are needed to encourage development of this system?

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

LASER 2013

Learning from Authoritative Security Experiment Results

SCHEDULE:

MAR 26 *Submissions Deadline*
MAY 07 *Decisions to Authors*
JUN 15 *Final Papers*
JUL 18 & 19 *Workshop*

LOCATION:

SRI International
1100 Wilson Boulevard, Suite 2800
Arlington, VA 22209

The goal of this workshop is to provide an outlet for publication of the results of all properly conducted experimental (cyber) security research. This will encourage people to share not only what works, but also what doesn't. Given the increased importance of computer security, the security community needs to quickly identify and learn from both success and failure. This is primary goal of this workshop. The specific technical results of the experiments are of secondary importance for this workshop.

Comments?

Edward B. Talbot
ebtalbo@sandia.gov
edward.talbot@gmail.com

Abstract

- Currently, cybersecurity practice is predominantly engaged in the detection of “bad” activity (from viruses to insiders). This focus on detection is often at odds with the protection of information since increasing detection can violate proven information protection doctrine such as limiting need-to-know. In addition to compromising information protection, detection limitations can disenfranchise users through false alarms. Effective information protection would develop systems that preserve anonymity, etc. just as effectively as in real-life (e.g. two colleagues chatting at a random café). Future cybersecurity investment should be re-balanced in favor of information protection.