Fine-Grained Cybersecurity for Continuous Assurance of Intellectual Property Integrity
Cybersecurity in the Headlines

Electricity Grid in U.S. Penetrated By Spies

Vast Spy System Loots Computers in 103 Countries

The Vast Reach of ‘GhostNet’

Researchers have detected an intelligence gathering operation involving at least 1,295 compromised computers. Below, the locations of 947 of the compromised machines, many of which were tracked to diplomatic and economic government offices of South and Southeast Asian countries.

Google Working With NSA to Investigate Cyber Attack

Google Working With NSA to Investigate Cyber Attack

By DIBOHN GORMAN

Officials at the National Security Agency have been working with Google Inc. to investigate the cyber attacks that Google announced publicly last month, according to people familiar with the investigation.

Broad New Hacking Attack Detected

Global Offensive Snagged Corporate, Personal Data at nearly 8,500 Companies; Is Still Running

By ALEX WILHET

We have found a way to reach for new heights

How the Stuxnet Digital Warheads Attacked Iran’s Nuclear Installations

Stuxnet is a computer worm that can do as much damage as a bomb could in destroying an industrial plant or military installation. The Stuxnet worm has been identified by experts as a sophisticated cyber attack that could cause significant damage to industrial control systems.

MAN

and China successfully broke into computers at nearly 2,500 companies and over the last 18 months in a coordinated global attack that exposed vast and corporate secrets to theft, according to a computer-security company breach.

The damage from the latest cyberattack is still being assessed, and affected companies are still being notified. But data compiled by NetWitness, the closely held firm that discovered the breaches, showed that hackers gained access to a wide array of data at 2,411 companies, from credit-card transactions to intellectual property.
Malicious cybersecurity incidents resulting from both insider and external vulnerabilities are on the rise

- Traditional **perimeter defense** has become less effective due to the rapid growth of information volume, fast adoption of new technologies and the need to flexibly collaborate across enterprise boundaries.

- Security policies and technologies will become more **fine-grained**. They will be complemented by a **multi-tier containment** security solution that spans across platform, cloud computing/data center, middleware and service oriented architecture, collaboration & community to protect individual business objects.

- **Security breaches & fraud are a continuum**. **Far field fraud detection** technologies which provide early warnings about major security breaches and fraudulent transactions before such incidents will emerge to complement existing near field techniques.

- Malicious attacks have surpassed human error for the first time in 2009 (ITRC)
- 48 percent of data breaches across all industries were caused by insiders. (Verizon 2010 Data Breach Investigations Report)
- Cybersecurity incidents in industrial control systems on the rise (HSNW 04/16/10)
Economic Impacts Landscape due to Cybersecurity vulnerabilities
Source: Robert Gibran

Different Types of Loss:
- Cash
- Data
- Intellectual Property
- Trust

Actual Loss:
- $105 billion a year (McAfee, 2007)
- $67 billion a year (FBI, 2006)
  - $50 billion a year in identity fraud
- $202 per compromised record, with an average $6.6 million per attack (Ponemon, 2009)
- $559 million in Intellectual Property loss, $4.6 million per firm (McAfee, 2008)

Potential Loss:
- Estimated at $700 billion for a major attack on critical infrastructures (U.S. Cyber Consequences Unit)

On May 29, 2009, the Federal government issued a report that stated that, between 2008 and 2009 American business losses due to cyber attacks had grown to more than $1 trillion worth of intellectual property

Changing Assumptions of Enterprise Security

- Mergers and Acquisitions
- Globalization
- Ubiquitous Workplace
- Globalization
- Smarter Planet
- Business Partners
- Suppliers
- Outsourcing
- Workforce Dynamics
- SaaS
- Cloud Computing
- Mobility
- Traditional Enterprise Security Model
- Degree of Interconnectivity

* Gifs from https://www.opengroup.org/jericho/Respondingtodp_implementation_080929.pdf

© 2011 IBM Corporation
Traditional Security Controls are ineffective against advanced persistence threat

<table>
<thead>
<tr>
<th>Traditional Malware</th>
<th>Advanced Persistent Threat</th>
</tr>
</thead>
<tbody>
<tr>
<td>▪ Opportunistic infection (non specific target), uncontrolled distribution</td>
<td>▪ Targeted at specific individuals and organizations, controlled distribution</td>
</tr>
<tr>
<td>▪ Motives: theft of personal info, disruption (DoS)</td>
<td>▪ Motives: theft of sensitive, high value information</td>
</tr>
<tr>
<td>▪ Static code, broadly deployed &amp; once deployed, does not change</td>
<td>▪ Dynamic code, customized for each target &amp; altered after infection</td>
</tr>
<tr>
<td>▪ One shot attack; once detected &amp; remediated, attack essentially over</td>
<td>▪ Persistent attack. If detected or defeated, alternate methods employed</td>
</tr>
<tr>
<td>▪ Operational objective: broad distribution scope</td>
<td>▪ Operational objective: remaining undetected</td>
</tr>
</tbody>
</table>

*From Eric J. Meyers, Du Pont*
Evolution of Threats, Escalation of Risks

**Business Level Risks**

- **Business level risks**
  - Fraud, loss of business-critical assets and theft of PII (e.g. payee fraud, theft of credit card numbers)

**IT Level Threats**

- **Existing threats**
  - Exploit vulnerabilities in servers, endpoints and networks directly or remotely (e.g. malware, DDOS, patch management, unauthenticated access)

- **Emerging threats**
  - Exploit vulnerabilities created in the infrastructure due to de-perimeterization of business and IT boundaries (e.g. insider threats, Trojan ICs, managed exploit providers)

**Nation-level risks (Cybersecurity)**

- Sabotage and subversion of the critical infrastructure, espionage and theft of top secret information, cyber warfare (e.g. APT, electricity grid, ghostnet, supply chain)

Evolution of threats (technological, organizational and workforce changes)
Our Proposition: Fine-grained, multi-tier containment approach to secure the critical infrastructure, IP resources and sensitive information.

End-to-end value@risk assessment and compliance

CLOSING THE LOOP: with continuous verification and assurance including investigation and remediation

Collaboration & Community
(Secure the Groups and Processes)

SOA, Information
(Secure the Services)

Middleware
(Secure the Middleware Servers and Applications)

Data Center/Network/Cloud
(Secure the Tenant)

Platform
(Secure the Platform)

Isolation Management

Federated Security Management Tier

Integrity Management

ISOLATION: Securing assets in insecure environments by deploying fine-grained perimeters (e.g. Enterprise, Cloud, Smarter Planet)

INTEGRITY: Create situational awareness capabilities by monitoring fine-grained perimeters

© 2011 IBM Corporation
1. Fine-grained security can complement perimeter-based protection in enterprises today

Systematic identification of IP assets (from loosely-coupled business units with potentially opposing business objectives operated by regular employee, contractors and business partners) and application of consistent and appropriate corporate-wide, fine-grained protection has been a major challenge for many enterprises.
1. Value@Risk Model: often required to rationalize the required investment in cybersecurity for protecting enterprise intellectual properties

source: the financial management of cyber risk, internet security alliance

**Example Value@Risk**

<table>
<thead>
<tr>
<th>Threat</th>
<th>Leakage: $10M/event</th>
<th>Obfuscation: $0.5M/event</th>
<th>Modification: $10M/event</th>
</tr>
</thead>
<tbody>
<tr>
<td>Net Financial Risk/year</td>
<td>$8M</td>
<td>$0.25M</td>
<td>$5M</td>
</tr>
</tbody>
</table>
2. Continuous assurance of IP integrity requires simultaneous integrity management across policy, process, and information

We are in the embryonic stages of a new epoch in IP integrity management as businesses evolve to develop a consistent and interdependent view of their policies, processes, and core entities.

Today information, processes and policies are typically inconsistent and incomplete.

Emerging solutions address consistencies and management of policies, processes and core entities independently.

Future solutions will emerge to ensure business integrity is maintained at all levels of the enterprise.

- Policy Integrity
  - Formal standards and policy management solutions

- Process Integrity
  - Formal standards and process management solutions

- Information Integrity
  - Master Information Management: a single semantic definition of core entities

© 2011 IBM Corporation
2. Continuous Assurance often relies on continuously capturing and cross validating provenance among policies, process, and information of IP

- Traditionally, provenance provides ownership history of a valued work of art or literature and is used to determine its authenticity
- Authenticity of provenance information is critical to ensure the integrity of the corresponding object
- For example, the provenance of the Mona Lisa is incomplete as it was stolen in 1911 and its whereabouts was unknown for two years
- Information provenance will capture the history of data objects and the processes that act on them

**Provenance:**
Acquired by François I, either directly from Leonardo da Vinci, during his stay in France, or upon his death from his heirs, the painting remained in the royal collections from the beginning of the sixteenth century to the creation of the Central Arts Museum at the Louvre in 1793. We know that it was kept at Versailles under the reign of Louis XIV and that it was in the Tuileries during the First Empire. Since the Restoration, the Mona Lisa has always remained in the Louvre Museum, a key piece of the national collections.

**Source:**

© 2011 IBM Corporation
3. Integrity Management: Interconnected platforms provide dynamic capture & assimilation of data, the orchestration of behavioral models, and control for closed-Loop prediction & response.
3. Capturing behavior models across the entire landscape will facilitate continuous integrity management.
3. Behavior Models from human, social networks, threats, system, and lifecycle of intellectual properties are often tightly coupled

- Leakage, obfuscation, or sabotage (modification)
- Insider or External

Diagram:
- Human Behavior Model
- Threat Behavior Model
- System/Network Behavior Models
- Lifecycles of Intellectual Properties
- Creator/Owner of IP

Perimeter of direct IP access
3. Mitigate the explosive growth of insider threats by using behavioral analytics and far-field detection techniques.

- Detecting and preventing abuse of authorized access is key to preventing insider attacks.

- **Far Field Detection**: Behavior monitoring of users to systems and networks as well as an analysis of user profiles, their business relationships and social networks can provide early warning indicators (in temporal, spatial and spatio-temporal dimensions) of insider attacks.

- Maintaining provenance of information and processes can improve auditability and accountability and facilitate information sharing without compromising security and privacy.
Summary: Moving to a more proactive and predictive stance is critical to tackling the challenge of Cybersecurity for Intellectual Properties

- **Situational awareness** is key and requires a wide range of sensors and systems that can operate both prospectively and in real-time.

- **Attack attribution** is important.

- Cyber defenders will have to deal with **rapidly evolving situations** as attackers use a wide range of techniques with widely ranging timescales, and can be expected to be able to rapidly switch among pre-loaded attacks as the situation evolves.

- Increasingly, systems will need to not only detect the problems but be able to implement a wide range of **adaptive defenses** either automatically or semi-automatically, examine the results of the defenses, and alter them accordingly.

- Defense requires **proactive preparation** of home-court.
Questions?

Please feel free to contact
Tilak Agerwala (tilak@us.ibm.com)
Chung-Sheng Li (csli@us.ibm.com)
J. R. Rao (jrrao@us.ibm.com)
Backup Charts
Intellectual Properties
wikipedia.org

- **Intellectual property (IP)** is a term referring to a number of distinct types of creations of the mind for which a set of exclusive rights are recognized—and the corresponding fields of law.
  - Under intellectual property law, owners are granted certain exclusive rights to a variety of intangible assets, such as musical, literary, and artistic works; discoveries and inventions; and words, phrases, symbols, and designs.
  - Common types of intellectual property include copyrights, trademarks, patents, industrial design rights and trade secrets in some jurisdictions.

- The existence of IP laws is credited with significant contributions toward economic growth.
  - Economists estimate that two-thirds of the value of large businesses in the U.S. can be traced to intangible assets.
  - "IP-intensive industries" are estimated to generate 72 percent more value added (price minus material cost) per employee than "non-IP-intensive industries".

- A joint research project of the WIPO and the United Nations University measuring the impact of IP systems on six Asian countries found "a positive correlation between the strengthening of the IP system and subsequent economic growth."
32% of the losses due to cyber attack result in theft of intellectual property; serious cost incurred on 92% of the loss cases for enterprises
Source: Symantec 2010 State of the Enterprise Security

- Most common losses are
  - Theft of customer personally identification information (32%)
  - Downtime of environment (32%)
  - Theft of intellectual property (32%)
  - Theft of customer credit card information

- Most common costs are
  - Lost productivity
  - Lost revenue
  - Loss of customer trust

- Average combined cost to enterprise: 2M/year (2.8M for large enterprise)
Companies lost on average $4.6M worth of intellectual property in 2008

- **Globalization**: More and more vital digital information, such as intellectual property and sensitive customer data, is being transferred between companies and continents—and lost. The average company has $12M worth of sensitive information residing abroad. Companies lost on average $4.6M worth of intellectual property in 2008.

- **Perfect information security risk storm**: as increased pressures on firms to reduce spending and cut staffing lead to more porous defenses and increased opportunities for cybercriminals. 42% respondents interviewed said laid-off employees are the biggest threat caused by the economic downturn.

- **Geopolitical Perception**: Elements in certain countries are emerging as clear sources of threats to sensitive data, in particular to intellectual property. Geopolitical perceptions are influencing data policy reality, as China, Pakistan, and Russia were identified as trouble zones for various legal, cultural and economic reasons.

- **Intellectual Property - the new currency**: Cyberthieves have moved beyond basic hacking and stealing of credit card data and personal credentials. An emerging target is intellectual property. Why sink all that time and money into research and development when you can just steal it?

Case Study: Unfair competitive Advantage

- An employee at Acme Tele Power Private Limited, an India-based company, allegedly leaked the software component of Acme’s patented product, Power Interface Unit (PIU), to Lambda Eastern Telecom, Acme’s competitor, in June 2006. Soon after the leak, the employee left Acme and joined Lambda, reportedly for a large pay increase. Acme claims that Lambda developed its product, BTS Shelter, based on the stolen research and development (R&D). Acme alleges that Lambda could not have made their product in such a short period of time without illegally using Acme’s intellectual property. The police were called to investigate and did eventually arrest the accused employee, although he was later released on bond. The role of Lambda in the incident remains unclear. Acme later moved its $10 million R&D operations to Australia, in hopes of finding a more business-friendly intellectual property protection environment.

- In 2008, a former Intel Corporation employee allegedly downloaded one billion dollars’ worth of confidential intellectual property documents before leaving the company to join AMD, a competitor. The U.S. Federal Bureau of Investigation (FBI) found more than 100 pages of sensitive documents and 19 computer-aided design (CAD) drawings of future processor chips at the home of the accused. The U.S. Department of Justice and the FBI was called after another Intel Corporation employee learned that the accused had started working for AMD before terminating employment with Intel, and that sensitive information had been accessed during that time frame. The former employee was charged in September 2008 with five counts of stealing trade secrets and wire fraud. He faces up to 90 years in prison if convicted on all counts. AMD did not use the information, but another company may not have been so ethical.

Case Study: Protecting Trade Secrets

- A former product engineer at Ford Motor Co. has been charged with stealing sensitive design documents from the automaker worth millions of dollars. Xiang Dong Yu, of Beijing – also known as Mike Yu – was arrested at Chicago’s O’Hare International Airport upon his entry into the U.S. from China, where he is working with a Ford rival.

- Yu, 47, was charged with theft of trade secrets, attempted theft of trade secrets, and unauthorized access to protected computers. Yu had access to trade secrets contained in Ford system design specification documents. The documents contained detailed information on performance requirements and associated testing processes for numerous major components in Ford vehicles.

- The documents, created and maintained by subject matter experts at Ford, are used by design engineers when building new vehicles and by suppliers providing parts to the company. According to the indictment papers, Ford has spent “millions of dollars and decades on research, developing, and testing” to create the requirements in the system design documents. Yu allegedly attempted to sell the stolen documents to a Ford competitor in China.

Source: The financial management of cyber risk, internet security alliance

© 2011 IBM Corporation