



## Le nuove tendenze degli attacchi cybercriminali secondo la ricerca di IBM X-Force



# Security has moved from an IT issue to an ongoing business concern



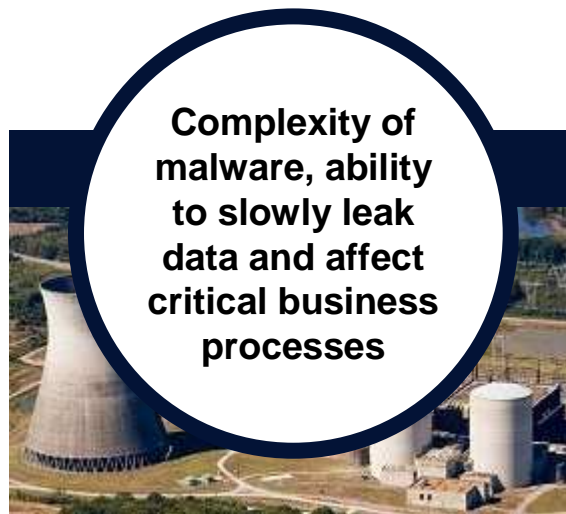
**Internal abuse of key sensitive information**

## **WIKILEAKS**

Unauthorized release of classified records

### **IMPACT**

Close to \$100M for the U.S. Army alone; damaged foreign relations worldwide



**Complexity of malware, ability to slowly leak data and affect critical business processes**

## **STUXNET**

Targeted changes to process controllers refining uranium

### **IMPACT**

Degraded ability to safely process and control highly volatile materials



**External data breach of third party data and theft of customer information**

## **EPSILON**

Theft of customer data affected > 100 companies

### **IMPACT**

Up to \$4 billion in costs for initial clean-up and longer term litigation risks

## Hacktivism and Hacktivists – An Overview

- **What is Hacktivism?**
- Essentially a new age of activism or “Cyber Activism”.
- Can be politically motivated but not always.
- Not new, Hacktivists groups can be tracked back to the late 80’s.
- Previously maintained closed groups for reasons of secrecy.
- Emerging “Opt-in” groups are posing a more volatile threat to today's networks.
- Attacks consist of Web Defacement, DoS, DDoS, Infobombing, unknown?



Lulz Security



# Security challenges are increasing in number and scope...



## EXTERNAL THREATS

Sharp rise in external attacks from non-traditional sources

- Cyber attack
- Organized crime
- Corporate espionage
- Government-sponsored attacks
- Social engineering

## INTERNAL THREATS

Ongoing risk of careless and malicious insider behavior

- Administrative mistakes
- Careless inside behavior
- Internal breaches
- Disgruntled employees actions
- Mix of private / corporate data

## COMPLIANCE

Growing need to address a steadily increasing number of mandates

- National regulations
- Industry standards
- Local mandates

# IBM X-Force® 2010 Trend and Risk Report

*Annual Review of 2010*



## What is X-Force?

X-Force is the pre-eminent security and threat protection brand for IBM customers.

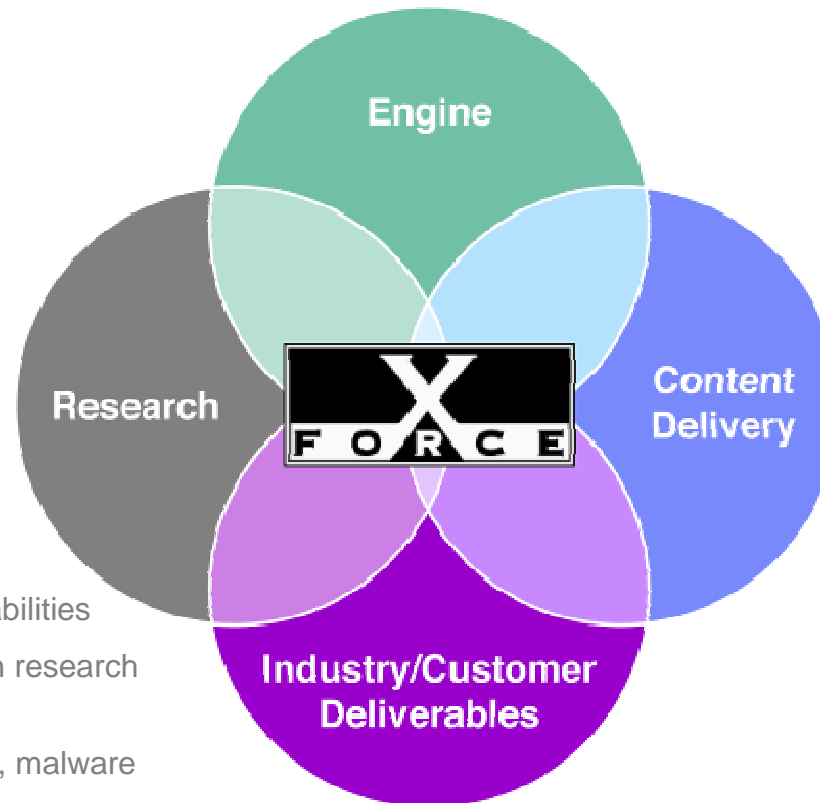
### IBM X-Force Research and Development

#### Engine

- Develop new security engines to solve evolving threats facing customers
- Add new capabilities to existing engines to combat new threats

#### Research

- Research **all** security vulnerabilities
- Expand current capabilities in research to stay Ahead of the Threat
- Continue unique vulnerability, malware and content filtering research



#### Content Delivery

- Continuous 3<sup>rd</sup> party testing
- Execute to deliver new content streams for new engines
- Continuously improve security effectiveness

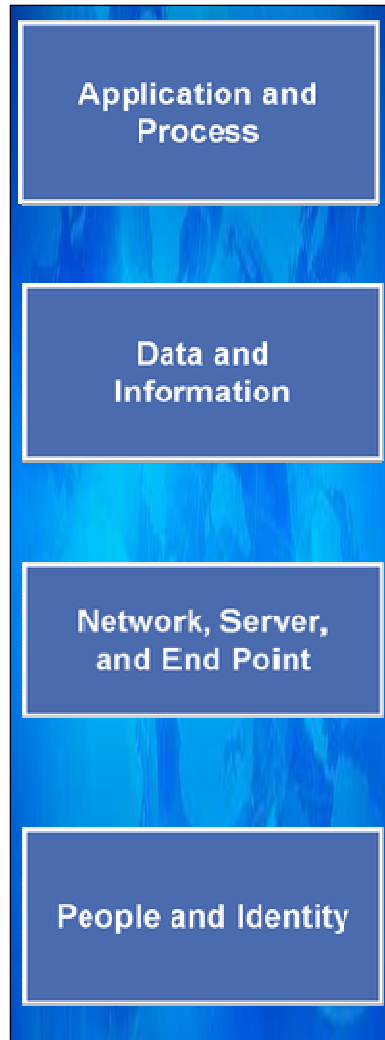
#### Industry/Customer Deliverables

- Blog, Marketing, and Industry Speaking Engagements
- X-Force Database Vulnerability Tracking
- Trend Analysis and Security Analytics

**The world's leading enterprise security R&D organization**



## Report Summary -- Attacks Continue Across all Security Domains

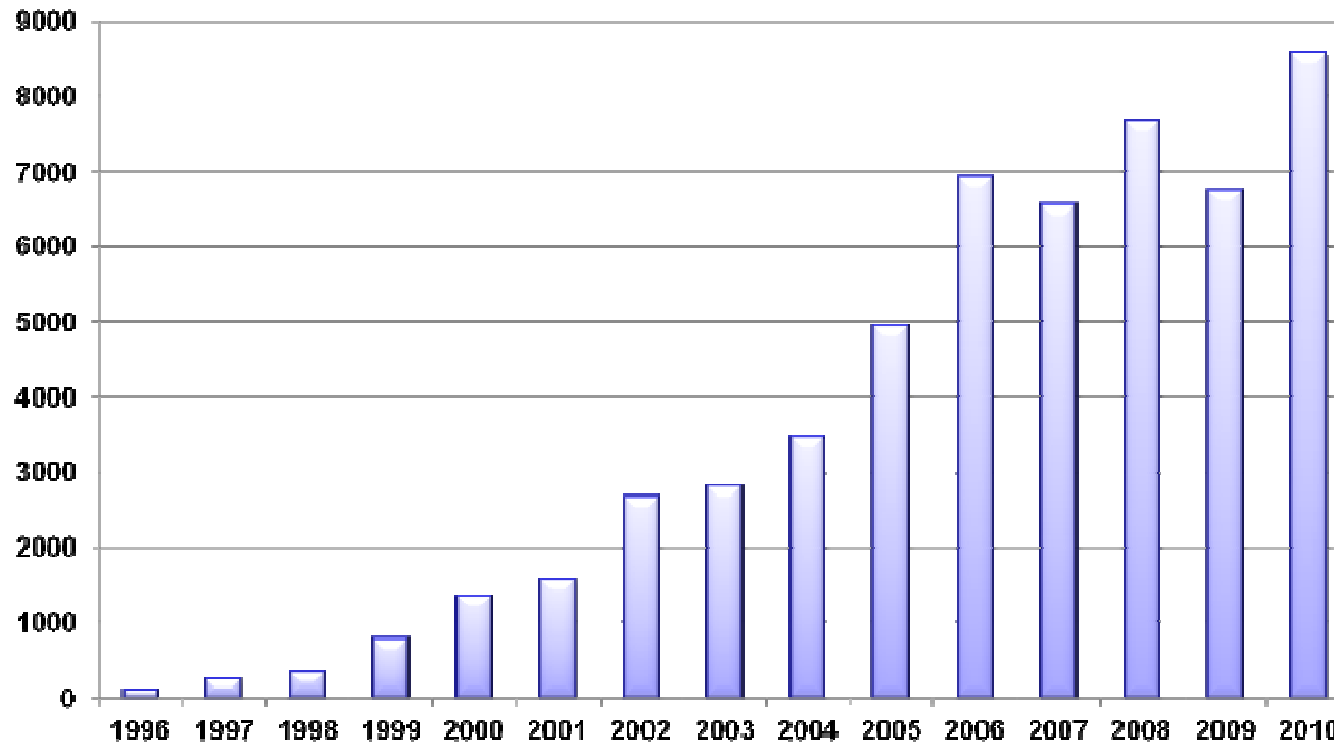


- 2010 saw the largest number of vulnerability disclosures in history, up **27%**. This increase has had a significant operational impact for anyone managing large IT infrastructures. More vulnerability disclosures can mean more time patching and remediating vulnerable systems.
  - **49%** of the vulnerabilities disclosed in 2010 were web application vulnerabilities.
  - **44%** of all vulnerabilities disclosed had no vendor-supplied patches available at the end of 2010.
- 
- Bot network activity continued to grow in 2010. Consolidation among Trojan botnets is expected to be an emerging trend.
  - The term “Advanced Persistent Threat” became an everyday part of the corporate security lexicon after high profile attacks on corporate enterprises by sophisticated, targeted attackers.
  - Anonymous proxy websites continue to increase in volume, quintupling since 2007.
- 
- The SQL Slammer worm continues to propagate on the Internet although it first surfaced back in January 2003. Today this worm continues to be the most common source of malicious Internet traffic.
  - Obfuscation, whereby attackers attempt to hide their activities and disguise their programming, continued to increase over 2010 and shows no signs of waning.
  - SQL injection is one of the leading attack vectors seen in 2010 because of its simplicity to execute and its scalability to compromise large amounts of Web servers across the Internet.
- 
- USA, India, Brazil, Vietnam, and Russia are the top five countries for spam origination in 2010.
  - The vast majority of spam, more than **90%**, is still classified as URL spam.
  - The amount of URL spam using well-known and trusted domain names declined slightly in the 2<sup>nd</sup> half of 2010, for the first time in more than two years.
  - The top spam domains have moved from China (.cn) to Russia (.ru).
  - In 2010, financial institutions continue to climb as the number one target for phishing attempts, representing **50%** of the targeted industries.

## Vendors Reporting the Largest Number of Vulnerability Disclosures in History

- Vulnerability disclosures up **27%**.
  - Web applications continue to be the largest category of disclosure.
- Significant increase across the board signifies efforts that are going on throughout the software industry to improve software quality and identify and patch vulnerabilities.

### Vulnerability Disclosures 1996 - 2010

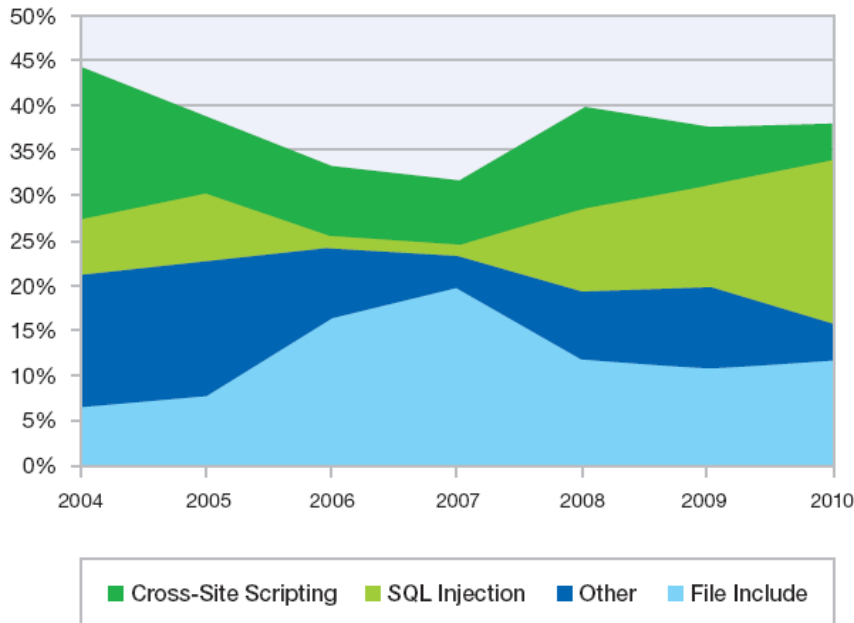




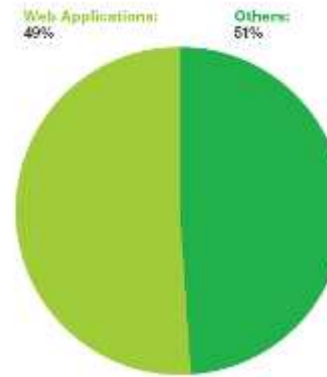
## Web App Vulnerabilities Continue to Dominate

- Nearly half (**49%**) of all vulnerabilities are Web application vulnerabilities.
- Cross-Site Scripting & SQL injection vulnerabilities continue to dominate.

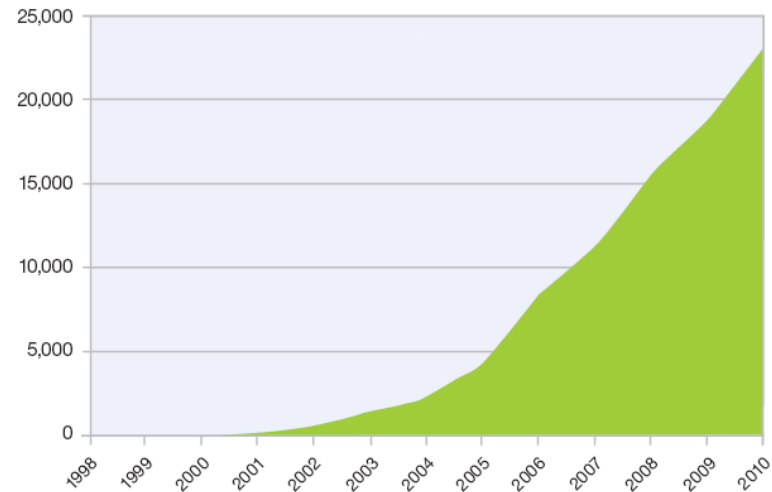
Web Application Vulnerabilities by Attack Technique  
2004-2010



Web Application Vulnerabilities  
as a Percentage of All Disclosures in 2010



Cumulative Count of Web Application Vulnerability Disclosures  
1998-2010



## Patches Still Unavailable for Many Vulnerabilities

- **44%** of all vulnerabilities disclosed in 2010 had no vendor-supplied patches to remedy the vulnerability.
  - Most patches become available for most vulnerabilities at the same time that they are publicly disclosed.
  - However some vulnerabilities are publicly disclosed for many weeks before patches are released.

Patch Timeline	All	Top Vendors
Same Day	3400	1814
Week 1	192	34
Week 2	55	11
Week 3	57	12
Week 4	33	7
Week 5	27	7
Week 6	22	4
Week 7	17	3
Week 8	16	8

# Public Exploit Exposures Up in 2010

- Public exploit disclosures up **21%** in 2010
  - Approximately **14.9%** of the vulnerabilities disclosed in 2010 had public exploits, which is down slightly from the **15.7%** last year
  - However more vulnerabilities were disclosed this year, so the total number of exploits increased.
  - The vast majority of public exploits are released the same day or in conjunction with public disclosure of the vulnerability.

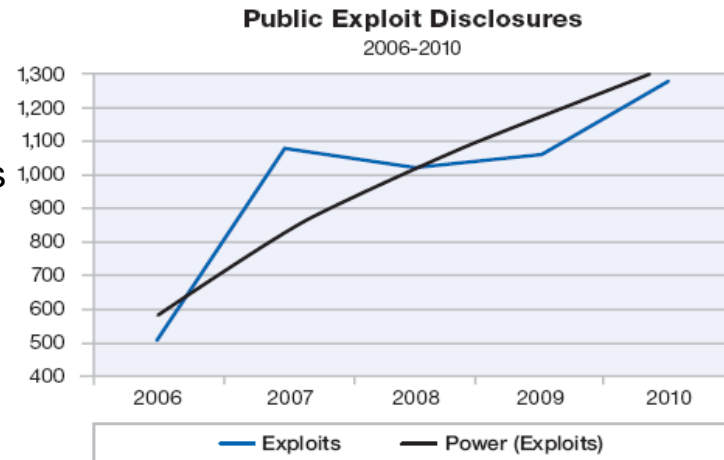


Figure 53: Public Exploit Disclosures – 2006-2010

	2006	2007	2008	2009	2010
True Exploits	504	1078	1025	1059	1280
Percentage of Total	7.3%	16.5%	13.4%	15.7%	14.9%

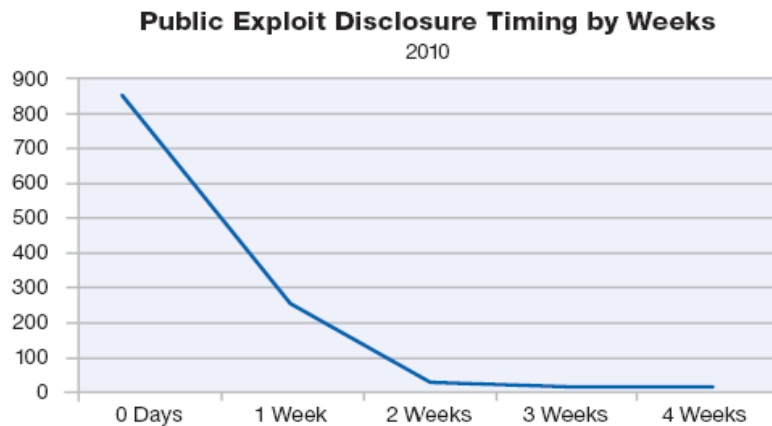
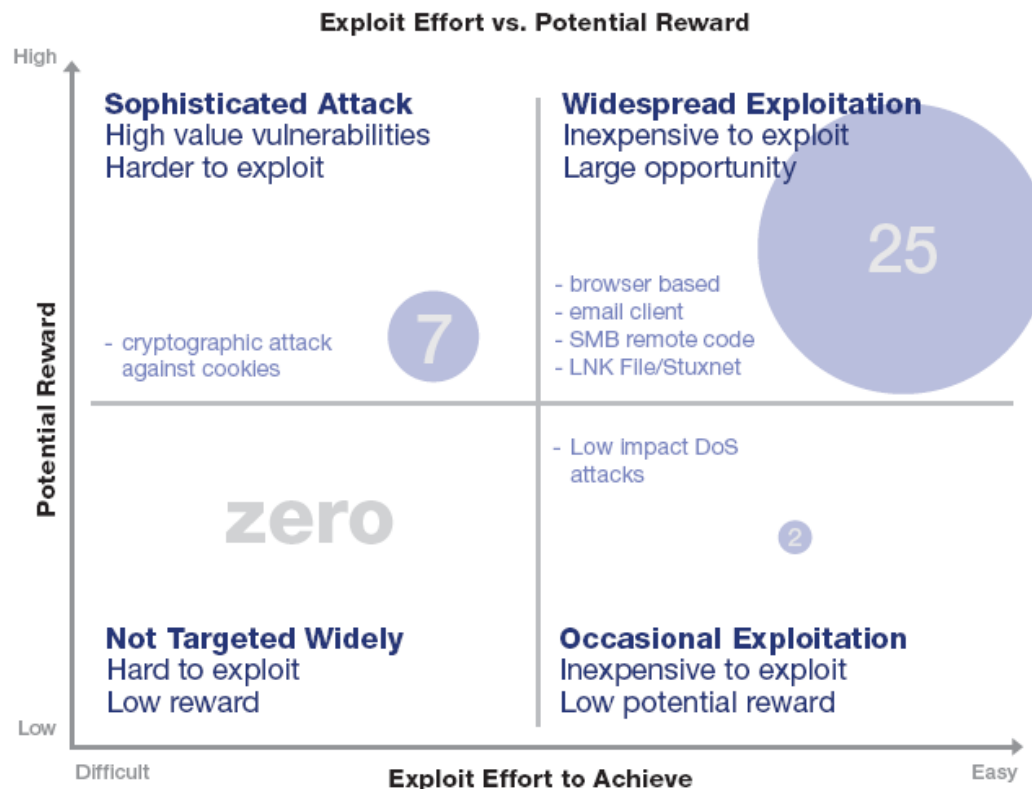


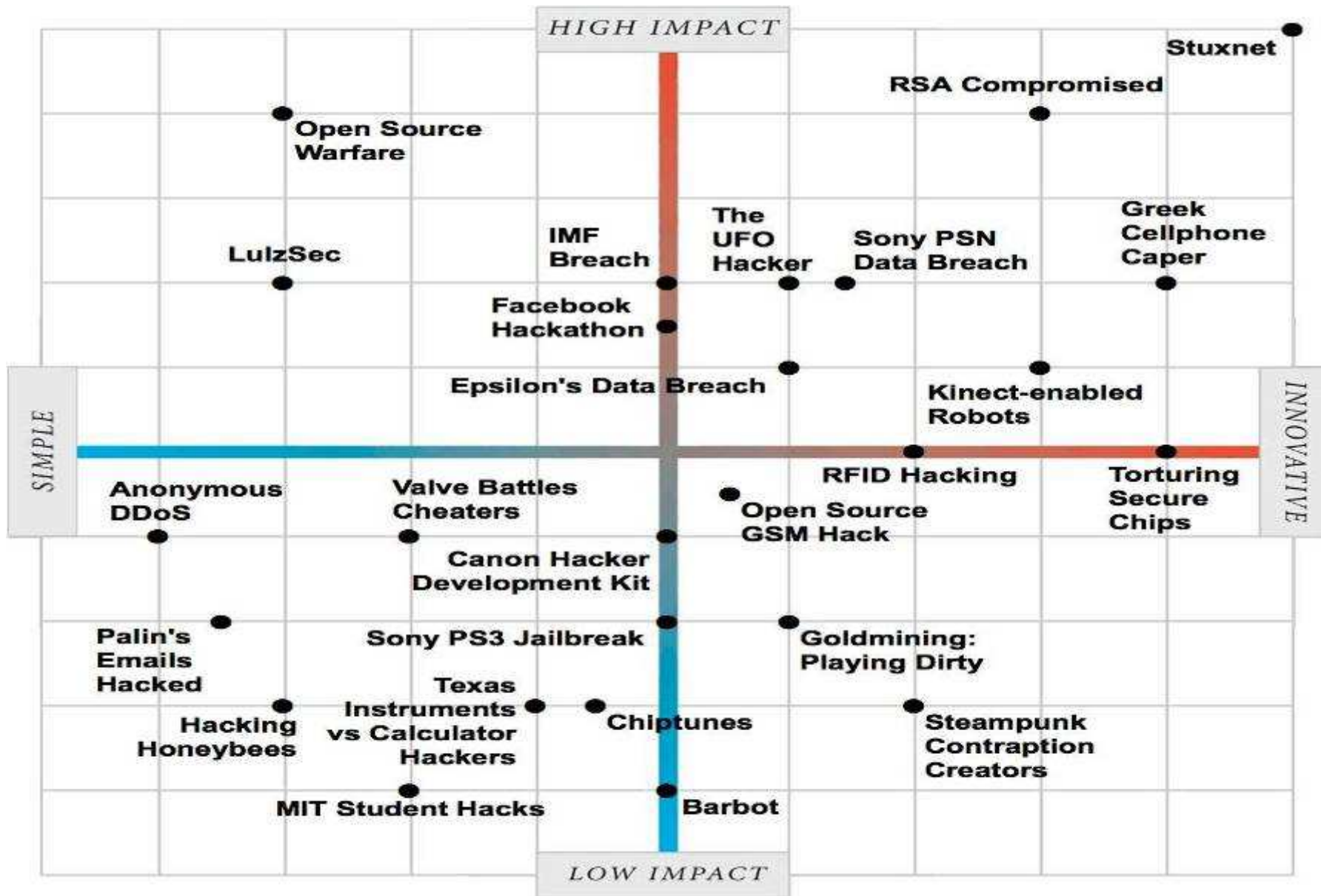
Figure 54: Public Exploit Disclosure Timing by Weeks – 2010

Exploit Timing	0 Days	1 Week	2 Weeks	3 Weeks	4 Weeks
0 Days	854	270	18	9	9

## Exploit Effort vs. Potential Reward

- Economics continue to play heavily into the exploitation probability of a vulnerability
- All but one of the 25 vulnerabilities in the top right are vulnerabilities in the browser, the browser environment, or in email clients.
- The only vulnerability in this category that is not a browser or email client side issue is the LNK file vulnerability that the Stuxnet worm used to exploit computers via malicious USB keys.





## Virtualization Security Increasingly a Focus

- 38% of server class vulnerabilities affect the hypervisor
- Virtualization Vulnerability Disclosures stay flat in 2010
  - Virtualization systems has added 259 new vulnerabilities to the network infrastructure over the last five years (80 virtualization vulnerabilities were disclosed in 2010).
  - This trend suggests that virtualization vendors have been paying more attention to security since a couple of years.

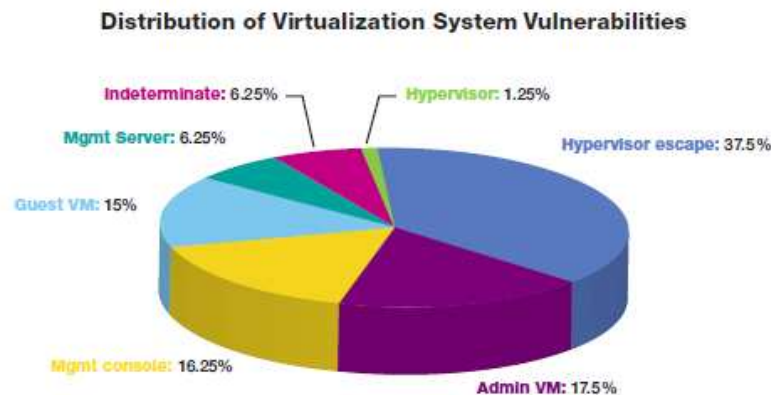
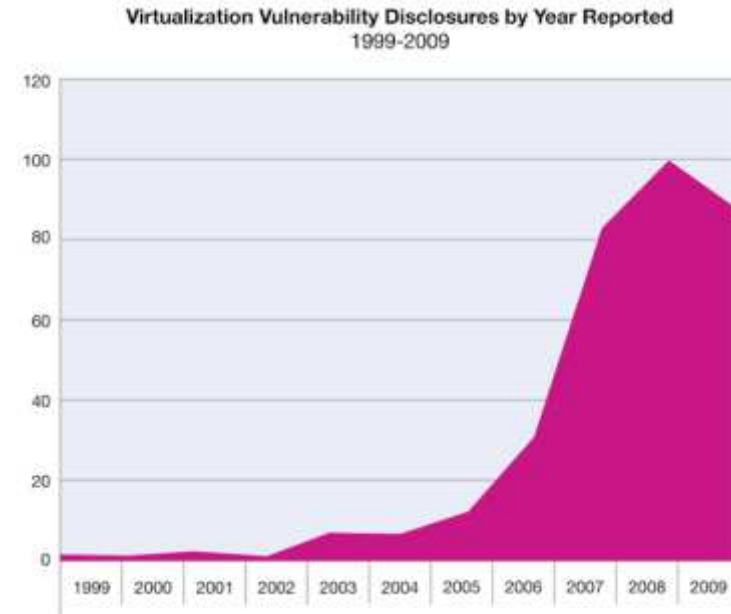


Figure 85: Distribution of Virtualization System Vulnerabilities



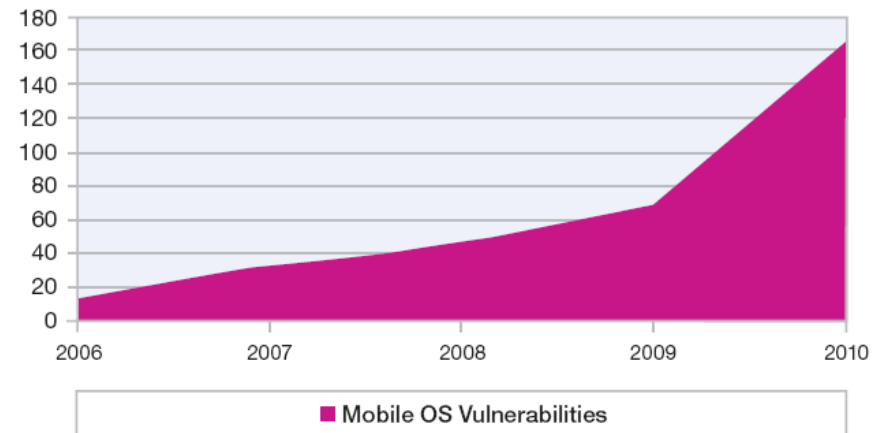
Virtualization systems have added 259 new vulnerabilities to the network infrastructure over the last five years.



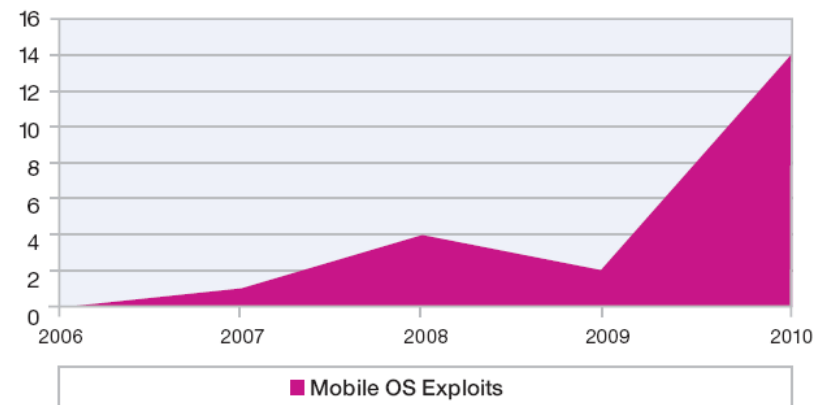
## Proliferation of Mobile Devices Raises Security Concerns

- 2010 saw significant increases in the number of vulnerabilities disclosed for mobile devices as well as number of public exploits released for those vulnerabilities.
  - Motivations of these exploit writers is to “jailbreak” or “root” devices.
  - Malicious applications were distributed in the Android app market.

**Total Mobile Operating System Vulnerabilities**  
2006-2010



**Total Mobile Operating System Exploits**  
2006-2010



## IPv6 and Cloud Computing Trends

### ■ IPv6 deployments -What is accelerating the trend to adopt these new networks?

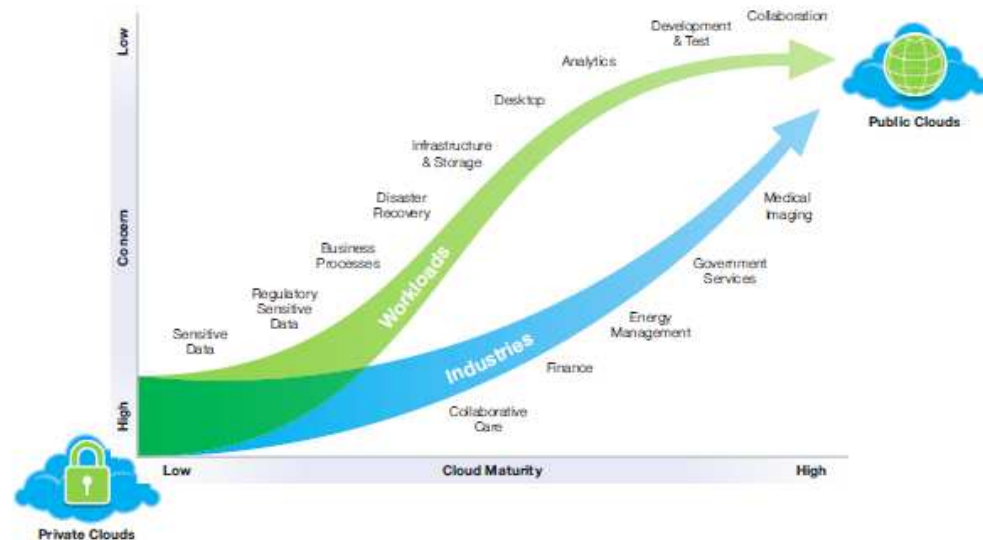
- Google recently reported that the United States is fifth in the world for IPv6 deployment, largely as a result of Apple Macs and wireless access points which are already enabled for IPv6 and which automatically connect through one of the established automatic transition tunnels.
- Some time ago, IPv6 was referred to as the “Next Generation” IP protocol. It could be argued that IPv6 is now the “Current Generation” IP protocol while IPv4 is becoming the “Old Show.”

■ Cloud computing is an emerging technology in which the vulnerabilities today are identical to those found in traditional emerging technology,

■ Adoption of cloud security continues to evolve and knowledge around this emerging technology increased.

-Providing an infrastructure that is secure by design with purpose-built security capabilities that meet the needs of the specific applications moving into the cloud.

-As more sensitive workloads move into the cloud, the security capabilities will become more sophisticated.

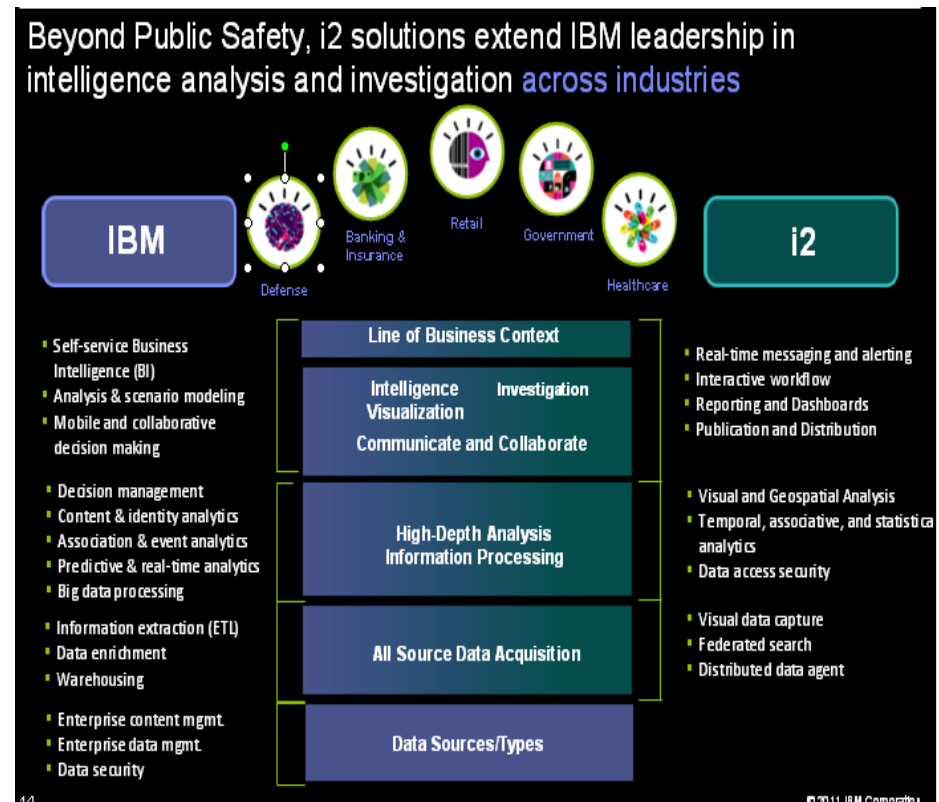


## IBM to Acquire i2 to Accelerate Big Data Analytics to Transform Global Cities (Analytics and Cyber Defense)

▪ Quick Highlights:

- Continues IBM's security leadership with a leading solution to combat advanced fraud and security threats
- Supports the IBM Security Framework with the ability to compliment other security assets
- Further positions IBM as a provider of Security Intelligence solutions, specifically i2 is focused on Smart Cities Public Safety and Enterprise Fraud
- Leverage Big Data for security and fraud analytics

- Targets clients in both public and private sectors



# Safety & Security per E&U



# Last week exploits published

**SC MAGAZINE** AUSTRALIAN EDITION SIGN IN JOIN

SECURE BUSINESS INTELLIGENCE POPULAR: password, scanner, management

HOME NEWS IN DEPTH REVIEWS EVENTS SC AWARDS

WHAT WE'RE FOLLOWING: Cyberwar • Jobs • Data breaches • Analysis

Home / Security News / Hackers

## Zero day industrial control system exploits published

By Darren Paul on Sep 15, 2011 6:37 PM  
Filed under Hackers

Power, water and waste SCADA systems affected.

Mi piace 56 persone. Registrazione per vedere cosa piace ai tuoi amici. Tweet 85 Share 14 9 Comments and 81

Reactions



A security researcher has disclosed a laundry list of unpatched vulnerabilities and detailed proof-of-concept exploits that allow hackers to completely compromise major industrial control systems.

Security researcher Luigi Auriemma disclosed the attacks against six SCADA (Supervisory Control and Data Acquisition) systems including US giant Rockwell Automation.

The step-by-step exploits allowed attackers to execute full remote compromises and denial of service attacks.

Keywords: scada, hacking, exploits, vulnerabilities

Sign up to receive SC Magazine email newsletters SIGN UP

FOLLOW US...

**sendQuick® ConeXa**  
Be the First to Be Informed



SMS OTP

**Most Read**

- Zero day industrial control system exploits



Audit reveals: A Bluetooth connection (PIN 0000) protected the water supply of Oslo

## Could have stopped the water supply of mobile

**\*\* Smashing, secret report reveals major weaknesses \*\* Ridiculously easy password protected water supply and sewerage system**



Treatment: Oset water treatment plant and other buildings that are critical for water and sewer system in Oslo could be up to our open using bluetooth technology. Photo: Heiko Junge / Scanpix.



## 'Morto' worm attacks SCADA

*Main | Beware of Using Public Cellular Carriers for Last Mile SCADA Communications »*

### 'Morto' worm tries weak passwords and default account names to spread using Remote Desktop Protocol

---

WEDNESDAY, AUGUST 31, 2011 AT 10:53AM

Most of our SCADA and Process Control clients have either already segmented their network architecture, or are in the process of segmenting their networks. Having defined networks for each functional area of the system is a great first step.

However, if you are using RDP (Remote Desktop Protocol) to jump or hop across network segments, **make sure that you have changed the default account names and passwords associated with the RDP logon process** because a new worm attack is live right now attempting to crawl through networks around the world, and it is taking a gamble that some have left default accounts and weak passwords in place.

Researchers working on the Morto worm say that it infects Windows workstations and Windows servers, and spreads by uploading a Windows DLL file to a targeted machine. The worm looks for weak administrator passwords in Remote Desktop on an organization's network, attempting everything from "12345" to "admin" and "password."

## Evolution of IT security vs. ICS security

Source: Idaho National Laboratory

Topic	Information Technology*	Industrial Control Systems
Anti-virus& Mobile Code Countermeasures	Common & widely used	Uncommon and difficult to deploy
Support Technology Lifetime	3-to-5 years	Up to 20 years
Outsourcing	Common & widely used	Rarely used
Application of Patches	Regular/scheduled	Slow (vendor specific)
Change Management	Regular/scheduled	Legacy based – unsuitable for modern security
Time Critical Content	Delays are generally accepted	Critical due to safety
Availability	Delays are generally accepted	24 x 7 x forever
Security Awareness	Good in both public and private sectors	General poor regarding cyber security
Security Testing/Audit	Scheduled and mandated	Occasional testing for outages
Physical Security	Secure	Very good, but often remote and unmanned

## End-to-end security perspective

Various standards bodies have published a list of ICS security documents

- Smart Grid Cyber Security Strategy and Requirements (NIST IR 7628 Draft 2)
- NIST Framework & Roadmap for Smart Grid Interoperability Standards, Release 1.0
- Security at the Information Technology standards level (ISO 27000 family, ISO 15408)
- Security at the Bulk Power System Protection level (NERC-CIP 001 – NERC CIP 009\*, NIST Special Publication (SP) 800-53, NIST SP 800-82 )
- Security at the Industrial Control System (SCADA) level (IEC 62443, IEC 62351 Parts 1-8 and NIST 800-82)
- Security for the Advanced Metering Infrastructure level (AMI-SEC System Security)
- Security for Home Area Network (OpenHAN and Zigbee)




**\* Equivalent non-US standards**

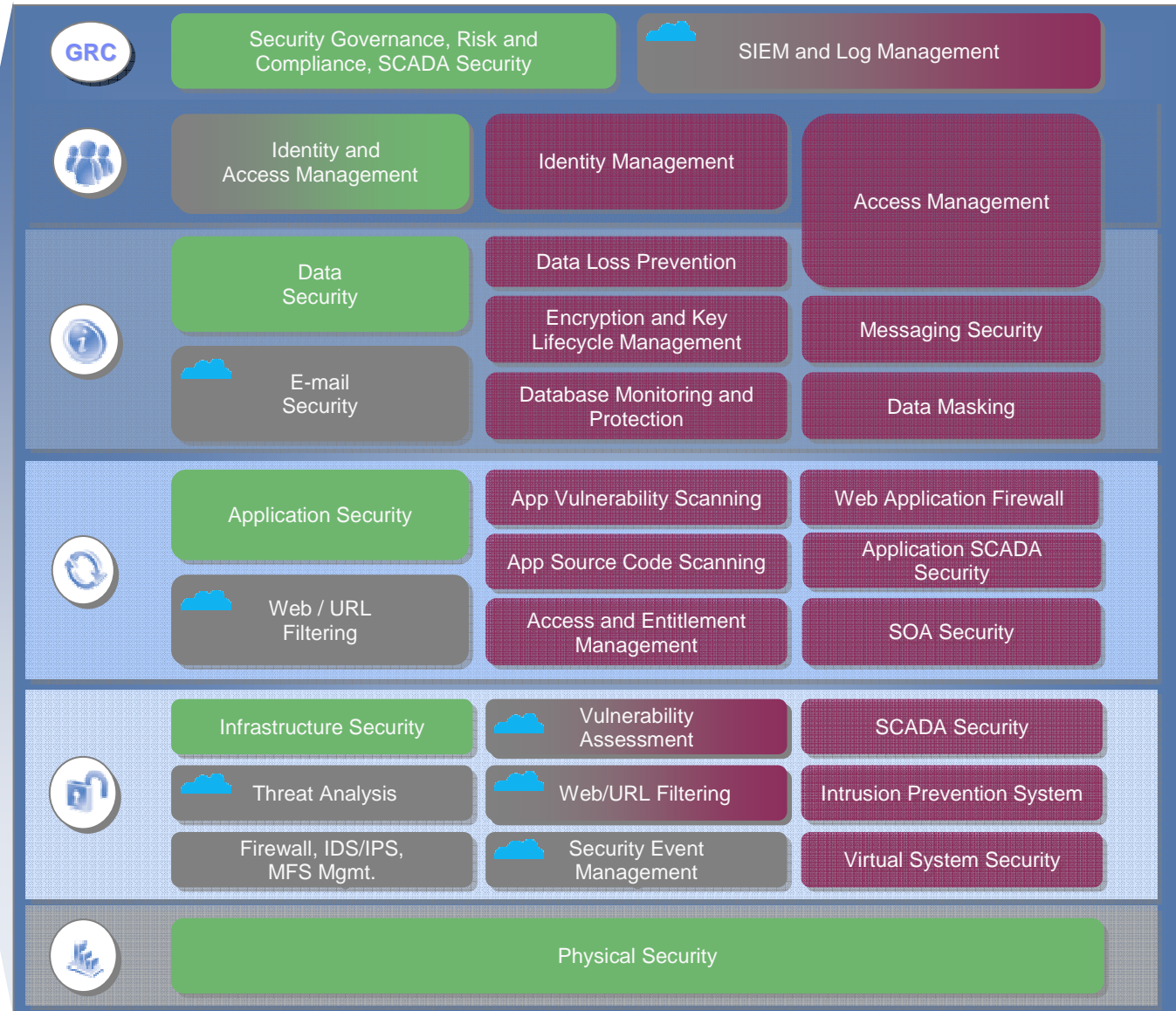
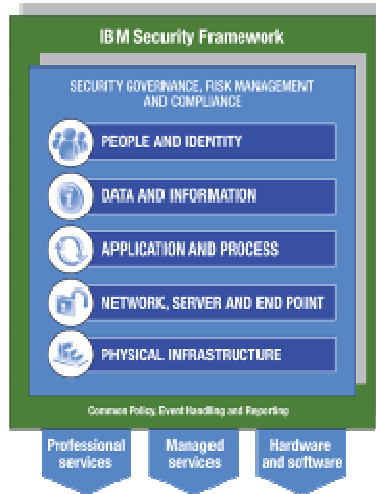
In the UK: The Center for Protection of National Infrastructure: <http://www.cpni.gov.uk/>

In the EU: European Network and Information Security Agency:

[http://www.enisa.europa.eu/pages/About\\_ENISA.htm](http://www.enisa.europa.eu/pages/About_ENISA.htm)

# IBM Security Portfolio

-  = Professional Services
-  = Cloud-based & Managed Services
-  = Products



# IBM Support for NERC-CIP standard

CIP Directive	NERC Objectives	Related IBM Security Framework Components	Current IBM Product and Service Offerings that address NERC-CIP Directive Objectives
<b>CIP-001</b>	Sabotage Reporting	Security Governance, Risk Management, and Compliance  Event Handling	<ul style="list-style-type: none"> <li>• Tivoli Service Request Manager</li> <li>• IBM Configuration Management Database</li> <li>• Tivoli Security Information and Event Manager</li> <li>• Tivoli zSecure</li> </ul>
<b>CIP-002</b>	Identification and Documentation of Critical Cyber Assets  Identification of Authorized Utility/Grid participants	Process, Security Governance, Risk Management, and Compliance People & Identity	<ul style="list-style-type: none"> <li>• IBM Tivoli Application Discovery and Dependency Manager</li> <li>• IBM Tivoli Asset Management for IT</li> <li>• IBM Configuration Management Database</li> <li>• IBM FileNet Content Manager</li> <li>• Rational Method Composer</li> <li>• IBM Trusted Identity framework</li> <li>• Tivoli Identity Manager</li> <li>• Tivoli Access Manager</li> </ul>
<b>CIP-003</b>	Security Management Controls	Network, Server and Endpoint Application and Process, Data and Information  Tivoli Professional Security Services	<ul style="list-style-type: none"> <li>• Tivoli Security Policy Manager</li> <li>• IBM Rational Appscan</li> <li>• Tivoli Access Manager for Operating Systems</li> <li>• IBM Tivoli Access Manager for Enterprise Single Sign-On</li> <li>• Tivoli Federated Identity Manager</li> <li>• IBM WebSphere DataPower</li> <li>• Tivoli Access Manager for e-Business</li> <li>• Tivoli Key Lifecycle Manager</li> <li>• IBM Change and Configuration Manager</li> </ul>
<b>CIP-004</b>	Personnel & Training	People and Identity	<ul style="list-style-type: none"> <li>• IBM WebSphere Process Server</li> <li>• Tivoli Identity Manager</li> <li>• Tivoli Directory Server</li> <li>• Tivoli Directory Integrator</li> <li>• IBM Lotus Learning Management System</li> </ul>
<b>CIP-005</b>	Electronic Security Perimeter	Network, Server and Endpoint and Professional Security Services	<ul style="list-style-type: none"> <li>• IBM ISS Proventia Intrusion Detection System</li> <li>• IBM ISS Proventia Anomaly Detection System</li> <li>• IBM ISS Global X-Force(Penetration Testing Services)</li> </ul>
<b>CIP-006</b>	Physical Security of Critical Cyber Assets	Physical Infrastructure	<ul style="list-style-type: none"> <li>• IBM Physical Security Services</li> <li>• IPSecurityCenter™</li> </ul>
<b>CIP-007</b>	Systems Security Management	Security Governance, Network, Server and Endpoint Application and Process, Data and Information	<ul style="list-style-type: none"> <li>• Tivoli Provisioning Manager</li> <li>• Tivoli Security Compliance Manager</li> <li>• Tivoli Identity Manager</li> <li>• IBM Rational Appscan</li> <li>• Tivoli Security Information and Event Manager</li> <li>• Tivoli zSecure</li> </ul>
<b>CIP-008</b>	Incident Reporting and Response Planning	Common Policy, Event Handling	<ul style="list-style-type: none"> <li>• Tivoli Service Request Manager</li> <li>• IBM Configuration and Change Management Database</li> </ul>
<b>CIP-009</b>	Recovery Plans for Critical Cyber Assets	Security Governance, Risk Management, and Compliance	<ul style="list-style-type: none"> <li>• Tivoli Asset Manager for IT</li> <li>• IBM Maximo Asset Management for Utilities</li> <li>• IBMTivoli Application Discovery and Dependency Manager</li> </ul>

## IBM Support for NIST 800-xx Guide to Industrial Control Systems Security

NIST recommendations	NIST objectives	IBM Security Framework component
NIST SP 800-12	Security Policies and Procedures	Application & Process
NIST SP 800-53	Security Controls- Configuration Management Access Management	Application & Process
NIST SP 800-94	Guidance on Intrusion Detection/Prevention Systems	Network, Server, Endpoint
NIST SP 800-61	Guidance on Incident Handling and Reporting	Process
NIST SP 800-73/76	Guidance on Personal Identity Verification	People and Identity
NIST SP 800-63	Guidance on Remote Electronic Authentication	Application, Process
NIST SP 800-64	Guidance on Security considerations for System Development Lifecycle	Governance, Compliance
NIST SP 800-61	Guidance on Incident Handling/Audit Log Retention	Process
NIST SP 800-56/57	Guidance on Cryptographic Key Establishment and Management	Application, Data & Information
NIST SP 800-52	Guidance on TLS implementation	Application, Data & Information



## IBM Security Network IPS



- **Blocco delle minacce di rete e garanzia di convergenza della sicurezza nei segmenti principali, perimetrali e remoti della rete**
- IBM Proventia Network IPS è progettato per bloccare le minacce provenienti da Internet prima che possano danneggiare l'azienda e per offrire protezione per tutti i tre livelli direte: segmenti principali, perimetrale e remoti. E' disponibile la protezione preventiva (in grado di anticipare l'attacco) di IBM ISS (Internet Security Systems) grazie alla combinazione proprietaria di velocità di linea, di un sistema di sicurezza intelligente, un motore di protezione modulare che garantisce convergenza della sicurezza
- Il team di ricerca e sviluppo ISS X-Force ha progettato il sistema di protezione Proventia IPS e fornito l'aggiornamento dei contenuti in grado di garantire una protezione preventiva dalle minacce. Il team di X-Force ha inoltre progettato i moduli di protezione, tra cui:
  - *Il modulo di gestione virtuale delle patch*
  - *Il modulo di rilevamento e prevenzione delle minacce*
  - *Il modulo di protezione dalla perdita di dati*
  - *Il modulo di protezione delle applicazioni Web*
  - *Il modulo per garantire la sicurezza di rete.*
- Tali moduli consentono a Proventia Network IPS di proteggere le reti da qualsiasi forma di attacco e minaccia, tra cui:
  - *Worm – Spyware -P2P (Peer To Peer)*
  - *DOS (Denial Of Service) e DDOS(Distributed Denial Of Service) –Botnet -Attacchi mirati contro applicazioni Web*
  - *Dati proprietari o sensibili che escono dalla rete - XSS (Cross-Site Scripting)*
  - *SQL injection -Buffer overflow - Web Directory Traversal.*

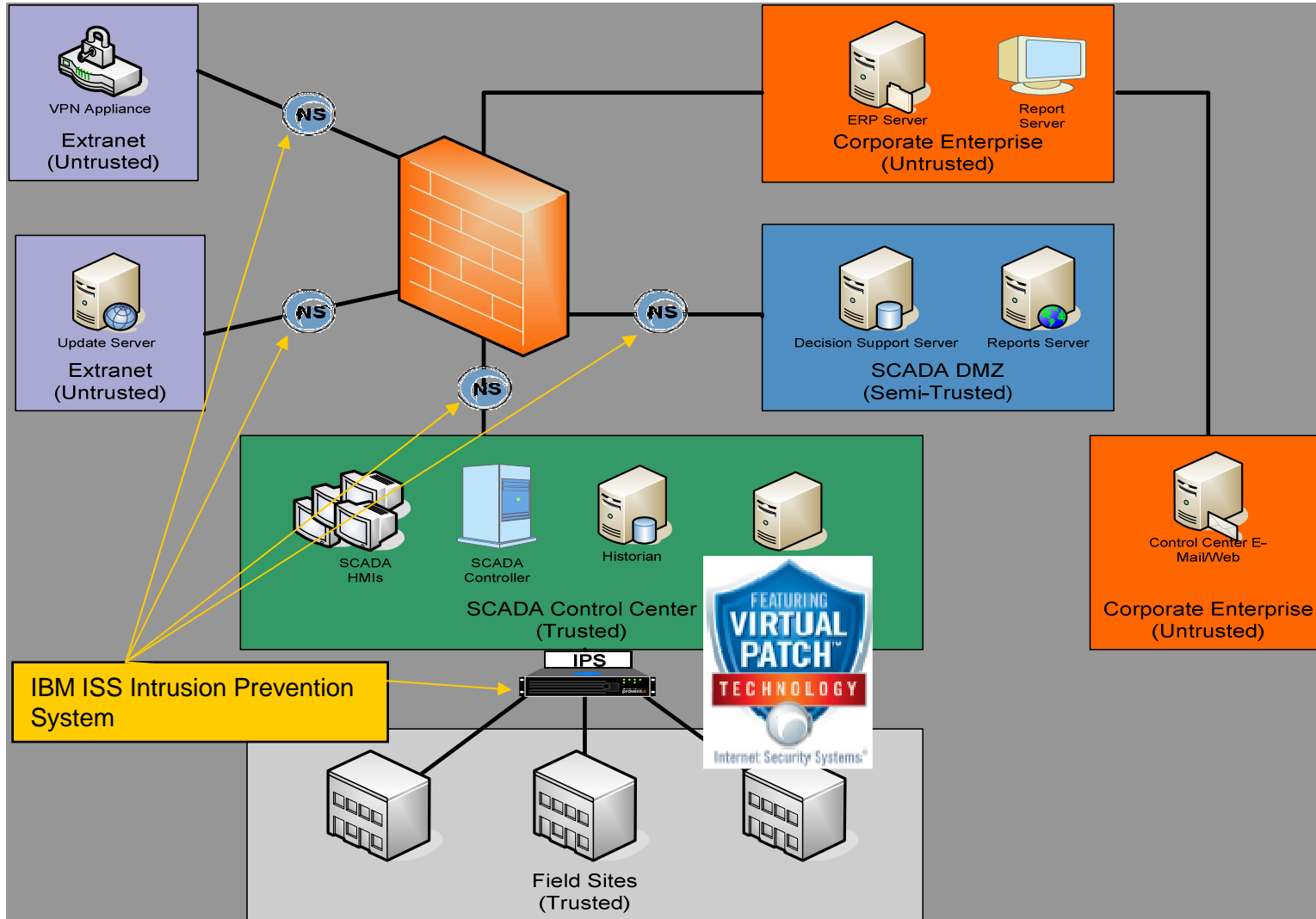
## IBM Protezione per Ambienti SCADA : subset

- Scada\_DNP\_Malformed
- Scada\_ICCP\_Long\_TPDU
- Scada\_Modbus\_TooLarge
- Scada\_Modbus\_SlaveBusyDelay
- Scada\_DNP\_Unknown\_Protocol
- Scada\_DNP\_DisableUnsolResponses
- Scada\_DNP\_ColdRestart
- Scada\_DNP\_WarmRestart
- Scada\_Modbus\_ClearRegisters
- Scada\_Modbus\_ReadDeviceID
- Scada\_Modbus\_ForceListenOnly
- Scada\_DNP\_BroadcastRequest
- Scada\_Modbus\_RestartCommunications
- Scada\_Modbus\_IncorrectLength
- Scada\_Modbus\_AckExceptionDelay
- Scada\_DNP\_StopApplication
- Scada\_Modbus\_ReportSlaveID

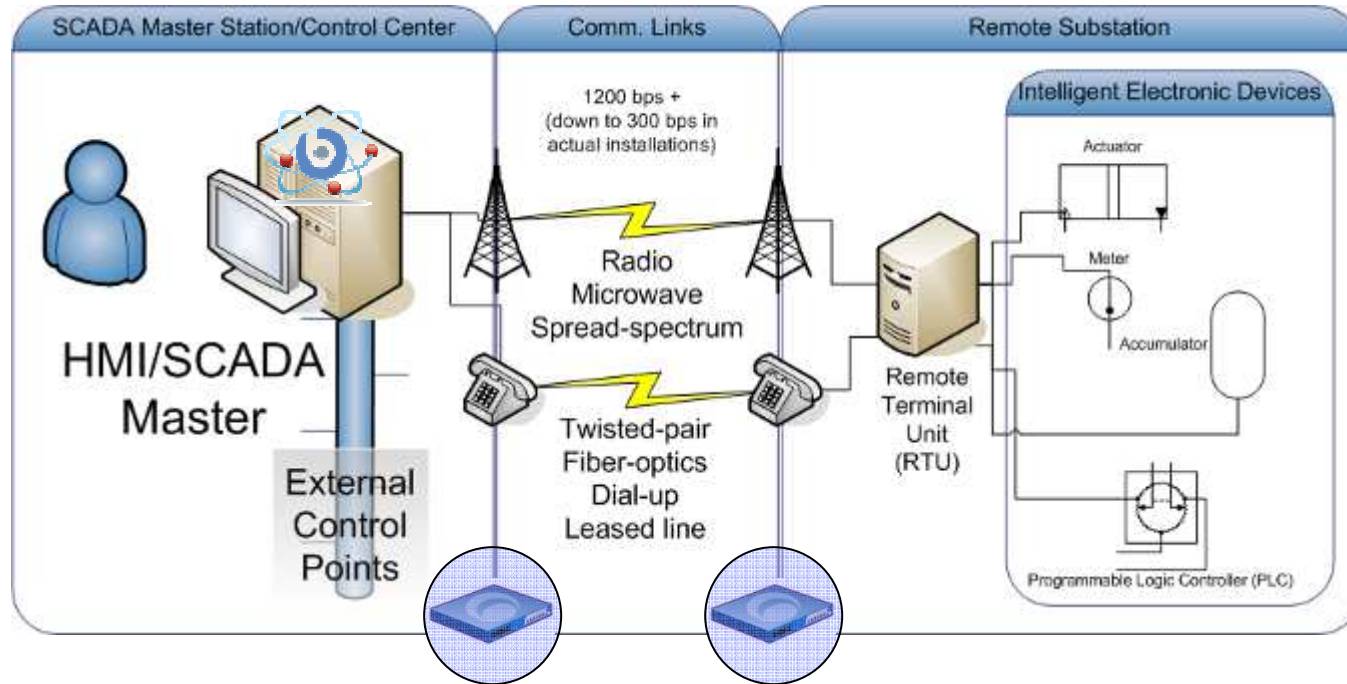
**And many more areas of protection for business critical applications and infrastructure, including protection for :**

- Scanning
- Denial of service
- Application server attacks
- Client-based attacks
- Messaging infrastructure

# Esempio di protezione architettura SCADA



# Threat Mitigation solutions for SCADA



Manage and report  
SiteProtector



## Protect

1. IBM Security Network Intrusion Prevention System
2. IBM Security TEM – Tivoli Endpoint Manager

# For More IBM X-Force Security Leadership



## X-Force Trend Reports

The IBM X-Force Trend & Risk Reports provide statistical information about all aspects of threats that affect Internet security,. Find out more at <http://www-935.ibm.com/services/us/iss/xforce/trendreports/>



## X-Force Security Alerts and Advisories

Only IBM X-Force can deliver preemptive security due to our unwavering commitment to research and development and 24/7 global attack monitoring. Find out more at <http://xforce.iss.net/>



## X-Force Blogs and Feeds

For a real-time update of Alerts, Advisories, and other security issues, subscribe to the X-Force RSS feeds. You can subscribe to the X-Force alerts and advisories feed at <http://iss.net/rss.php> or the Frequency X Blog at <http://blogs.iss.net/rss.php>

*Grazie*

**Fabio Panada**  
fabio.panada@it.ibm.com