SOFTWARE SECURITY ASSURANCE SUMMIT

September 12, 2011 | HP Protect at Gaylord National | Washington D.C.

SSA Trends and Insights

Rob Roy

Federal CTO

T.E.N. TECH EXEC NETWORKS *presented by* HP Enterprise Security

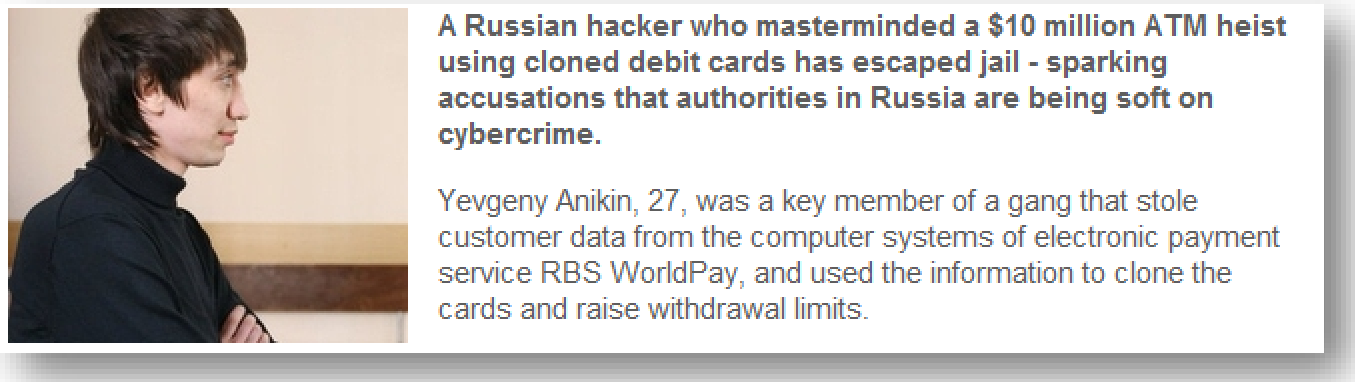
Cloudy Out There

2011 VA EARTHQUAKE
WE WILL REBUILD

Somebody Wants Our Stuff

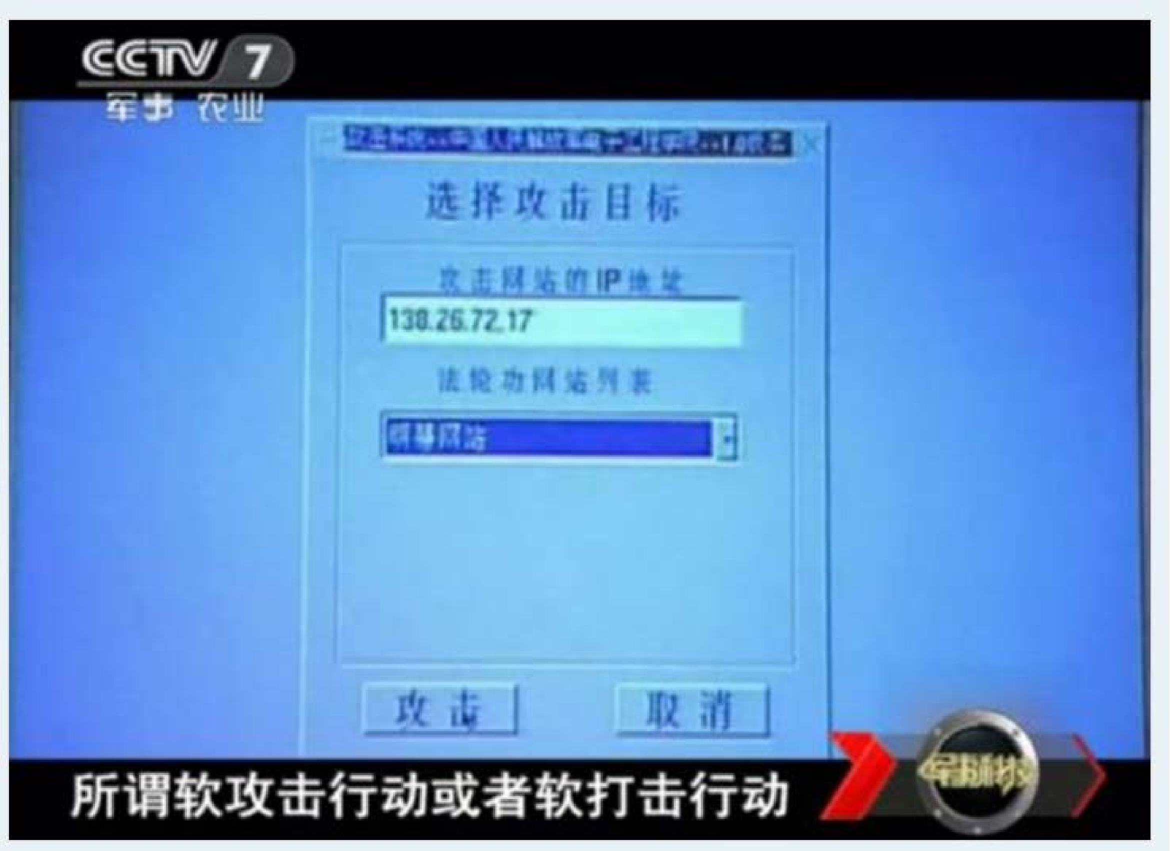
This Adversary Wants Secrets

While This One Wants Money



A Russian hacker who masterminded a $10 million ATM heist using cloned debit cards has escaped jail - sparking accusations that authorities in Russia are being soft on cybercrime.

Yevgeny Anikin, 27, was a key member of a gang that stole customer data from the computer systems of electronic payment service RBS WorldPay, and used the information to clone the cards and raise withdrawal limits.



[illegible]

选择攻击目标

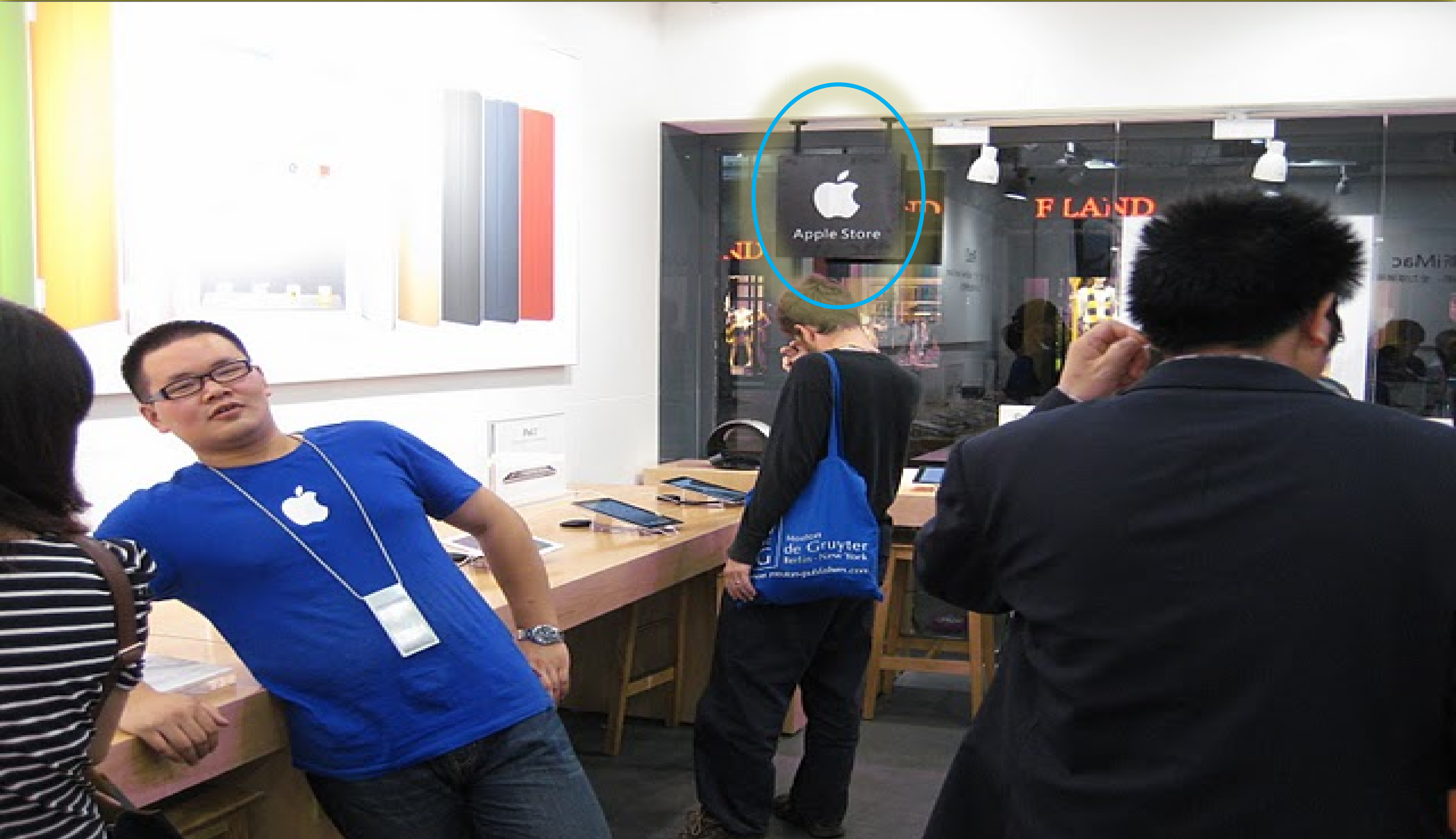
攻击网站的IP地址

138.26.72.17

法轮功网站列表

明慧网站

所谓软攻击行动或者软打击行动

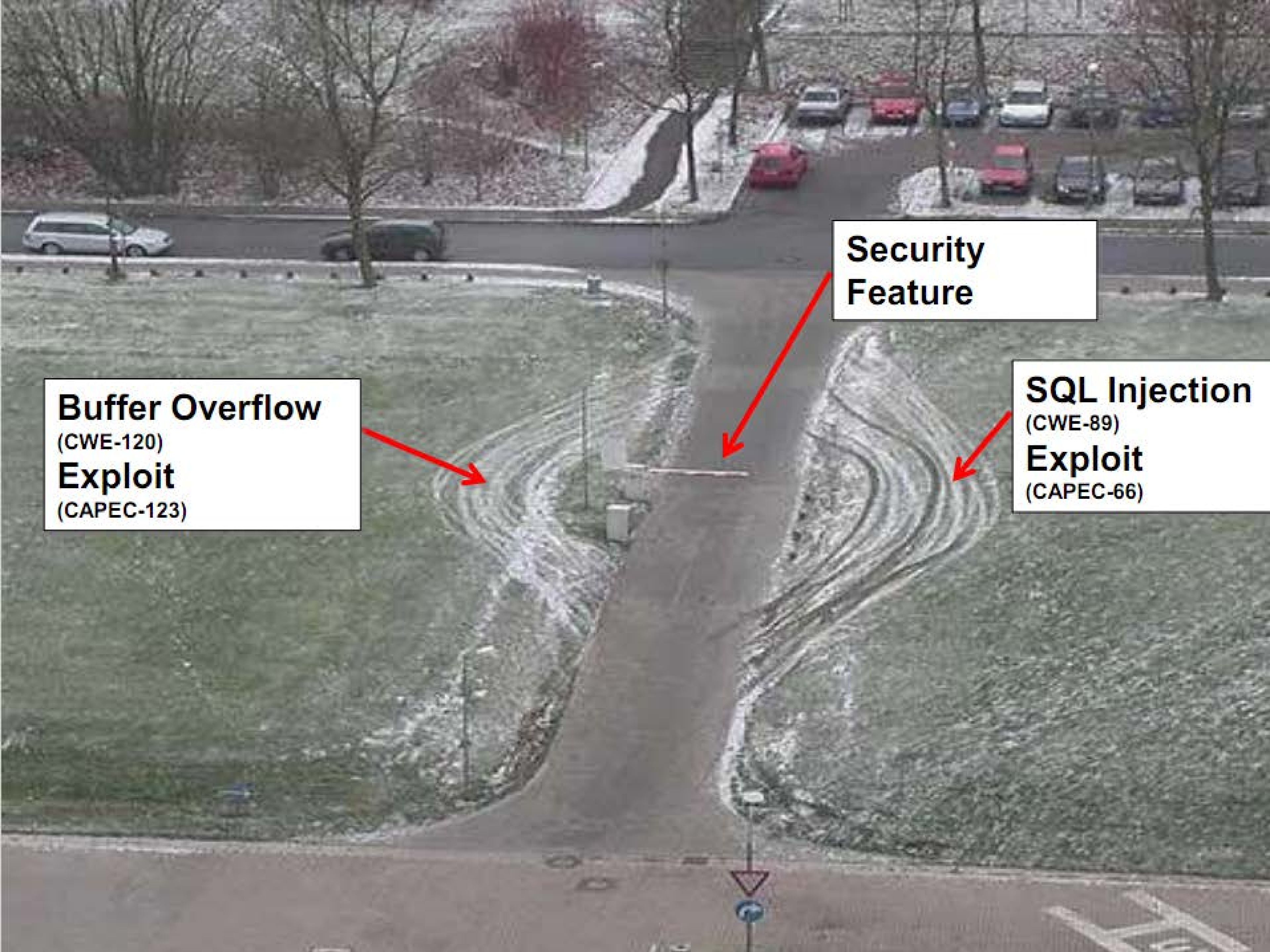

Apple Store
F LAND
iMac
de Gruyter
Berlin · New York

Software Complexity is Rising

Application	Lines of Code - Millions
1981 Cadillac	.05
F22 Raptor Avionics	1.7
Space Shuttle	2
Microsoft Word	2
F35 Joint Strike Fighter	5.7
Boeing 787 Dreamliner	6.5
Mercedes Radio w/Nav	20
Premium Car	100

Where is software actually developed?

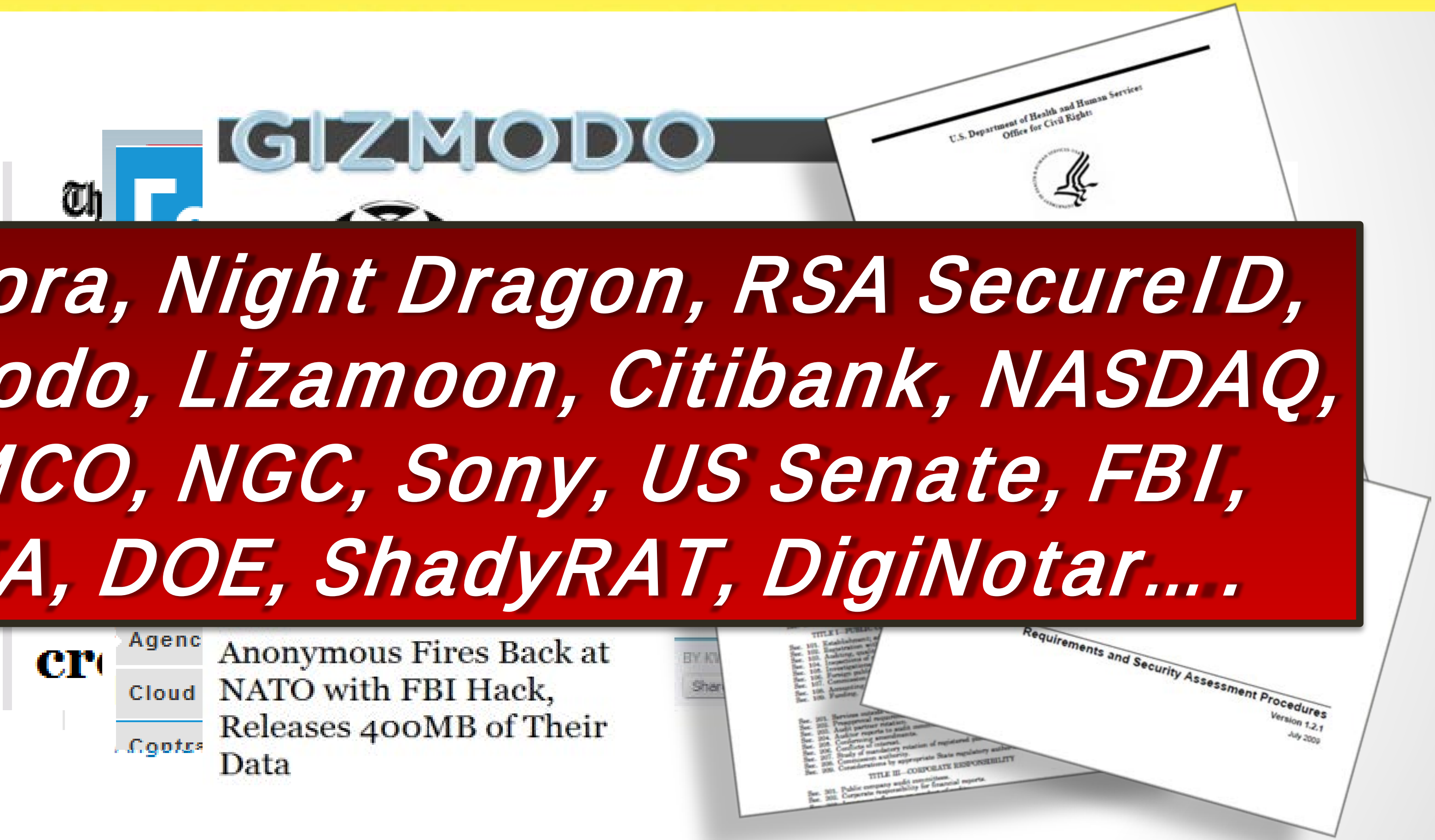
How do you know what's in it?



Security Feature

Buffer Overflow (CWE-120) Exploit (CAPEC-123)

SQL Injection (CWE-89) Exploit (CAPEC-66)



Anonymous Fires Back at NATO with FBI Hack, Releases 400MB of Their Data

U.S. Department of Health and Human Services
Office for Civil Rights

Requirements and Security Assessment Procedures
Version 1.2.1
July 2009

Aurora, Night Dragon, RSA SecureID, Comodo, Lizamoon, Citibank, NASDAQ, LMCO, NGC, Sony, US Senate, FBI, CIA, DOE, ShadyRAT, DigiNotar….

Risks increasing as threats grow more complex

ATTACKS

85% OF ALL U.S. COMPANIES EXPERIENCED ONE OR MORE ATTACKS

FINANCIAL LOSS

$7.2M AVERAGE COST ASSOCIATED WITH DATA BREACH

REPUTATION DAMAGE

30% MARKET CAP REDUCTION AS A RESULT OF RECENT EVENTS

ASYMMETRY

3¢ COST TO ANONYMOUSLY RENT AMAZON EC2 SERVICE FOR ONE HOUR

Source: HP internal data., Ponemon Institute

How do we fix the software issue?

99.6%

Federal IT Security Budget - Networks

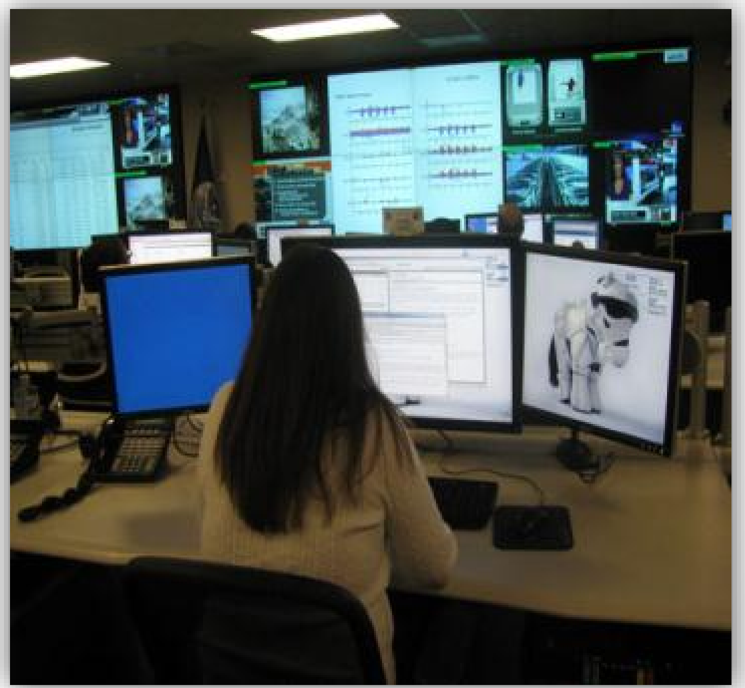
.4%

Federal IT Security Budget - Software

Funding

Requirements

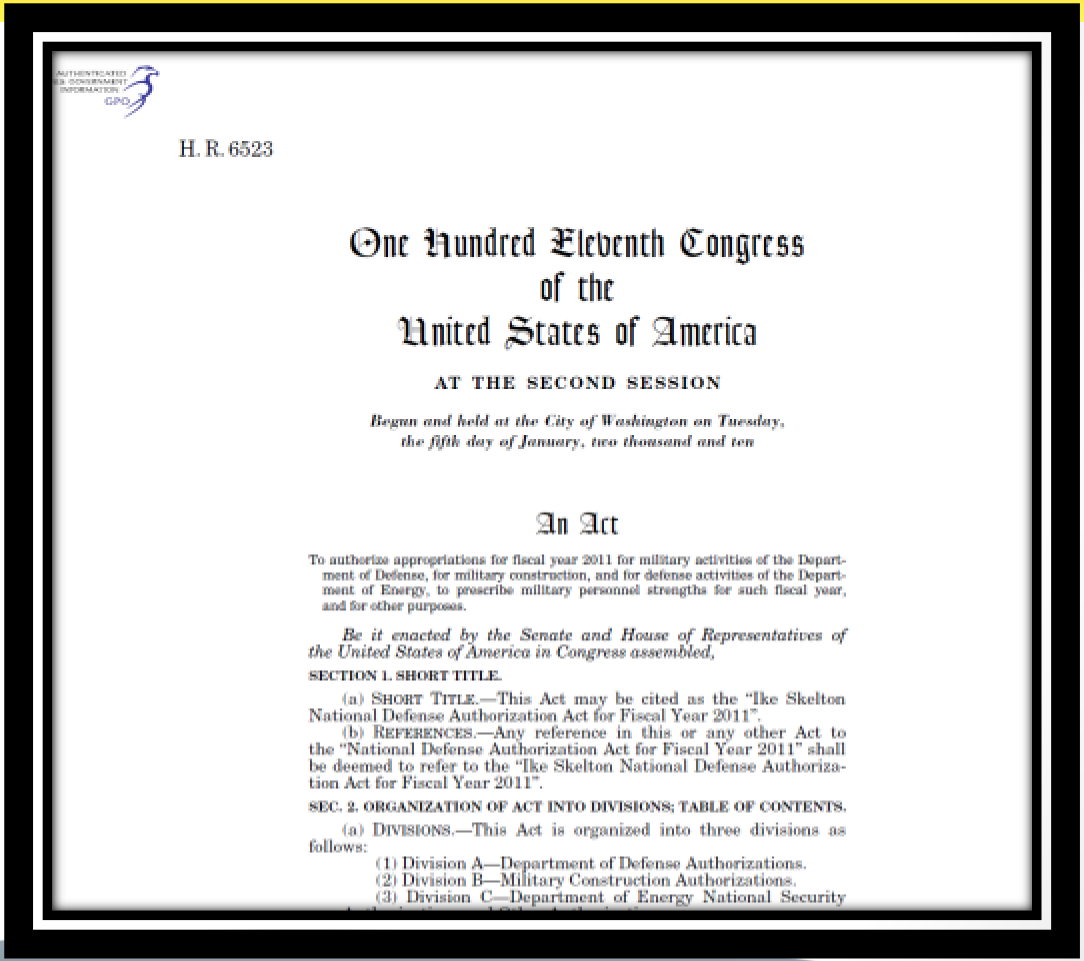
Laws



DHS' Cyber-Coordination HQ

Software Security Assurance Summit

September 12, 2011 | HP Protect at Gaylord National | Washington D.C.



AUTHENTICATED U.S. GOVERNMENT INFORMATION GPO

H. R. 6523

One Hundred Eleventh Congress of the United States of America

AT THE SECOND SESSION

Begun and held at the City of Washington on Tuesday, the fifth day of January, two thousand and ten

An Act

To authorize appropriations for fiscal year 2011 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

(a) SHORT TITLE.—This Act may be cited as the "Ike Skelton National Defense Authorization Act for Fiscal Year 2011".

(b) REFERENCES.—Any reference in this or any other Act to the "National Defense Authorization Act for Fiscal Year 2011" shall be deemed to refer to the "Ike Skelton National Defense Authorization Act for Fiscal Year 2011".

SEC. 2. ORGANIZATION OF ACT INTO DIVISIONS; TABLE OF CONTENTS.

(a) DIVISIONS.—This Act is organized into three divisions as follows:

(1) Division A—Department of Defense Authorizations.

(2) Division B—Military Construction Authorizations.

(3) Division C—Department of Energy National Security

TEN

presented by

HP Enterprise Security

"The committee emphasizes the importance of developing new technologies for the ***automated analysis of software code*** *for vulnerabilities and for detecting attempted intrusions.* ***It is not practical to manually examine all the lines of code in all of DOD's critical information systems****."*

(F) Remediation in legacy systems of critical software assurance deficiencies that are defined as critical in accordance with the Application Security Technical Implementation Guide of the Defense Information Systems Agency.

…

(3) Mechanisms for protection against compromise of information systems through the supply chain or cyber-attack by acquiring and improving automated tools for--

(A) assuring the security of software and software applications during software development;

(B) detecting vulnerabilities during testing of software; and

(C) detecting intrusions during real-time monitoring of software applications.

…

(7) A funding mechanism for remediation of critical software assurance vulnerabilities in legacy systems

Perfect Security Automation

- Finds all the vulnerabilities (no false negatives)
- Never wrong (no false positives)
- Runs fast
- Easy to use
- Easy to know you’re using it correctly
- Free

Black-Box Testing

- System-level tests
- No assumptions about implementation
- Example: fuzzing
- Good: concrete results
- Bad: a losing game

White-Box Testing

- Examine implementation
- Test components in isolation
- Example: static analysis
- Good: thorough
- Bad: too thorough
- Bad: no “show me” exploits

Gray-Box Testing

- System-level tests (like black-box)
- Examine implementation (like white-box)

HP WebInspect™ *Real-Time*

Find More

- Analyze more of the application
  - Automatic attack surface identification
- Detect new types of vulnerabilities
  - Privacy violation, Log Forging

Fix Faster

- Reduce False Positives
  - Confirm vulnerabilities
- Provide Actionable Details
  - Stack trace/Line of code
- Collapse Duplicate Issues
  - Identify root cause

ADVERSITY
Impossible odds makes achievements even more satisfying.

Thank You!