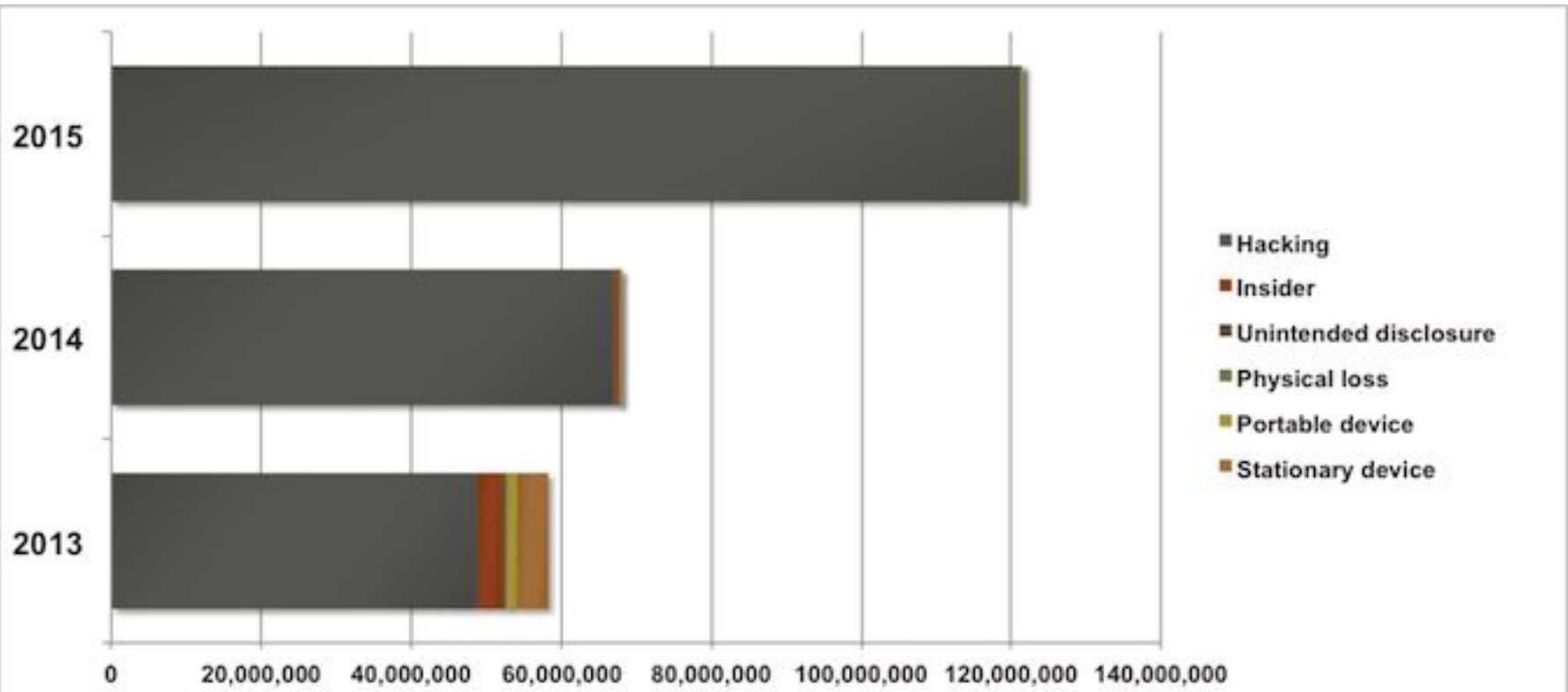


# ECP 611 Network Security

Introduction to the state of information Security

Sherif El-Kassas

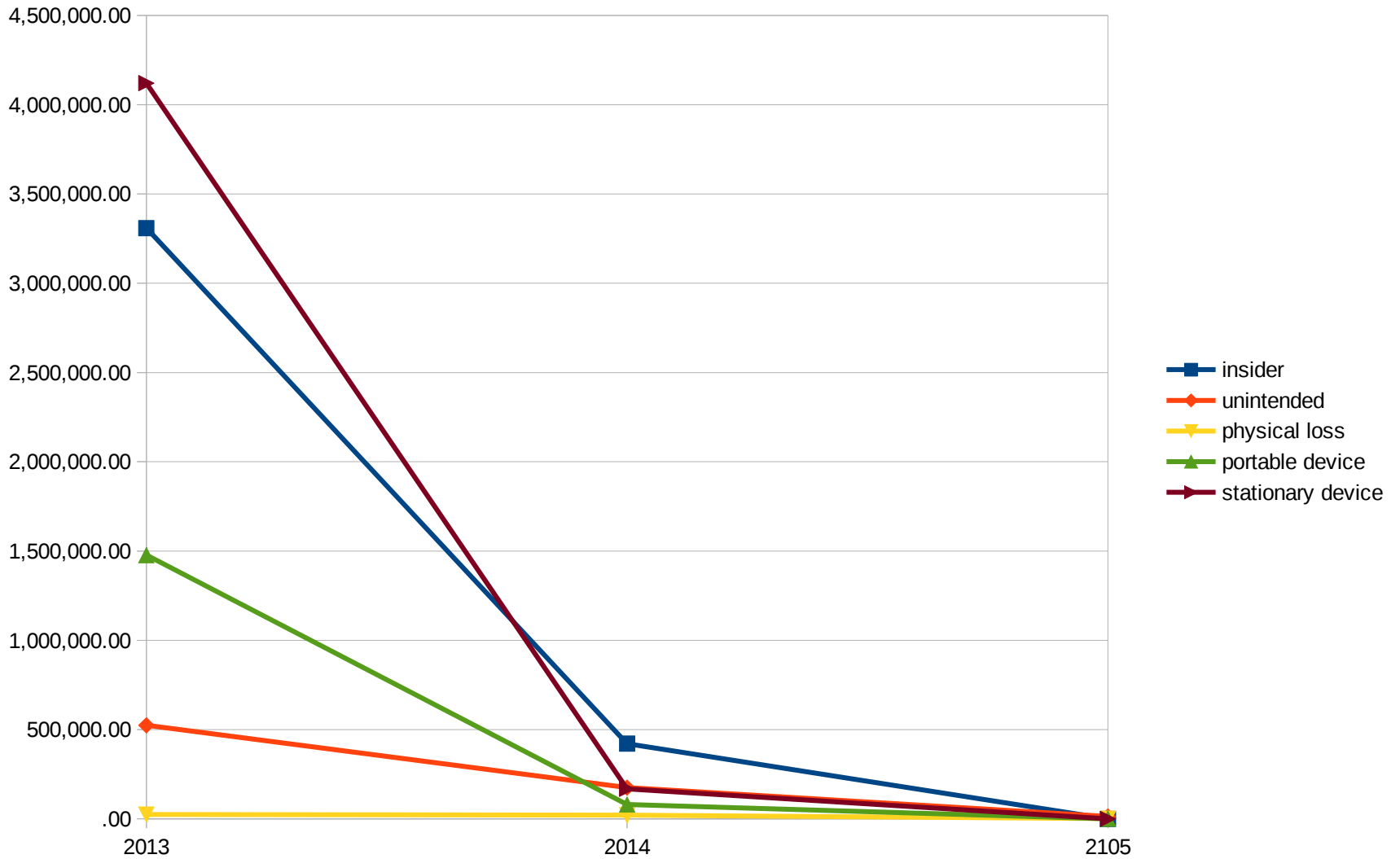
**trends**



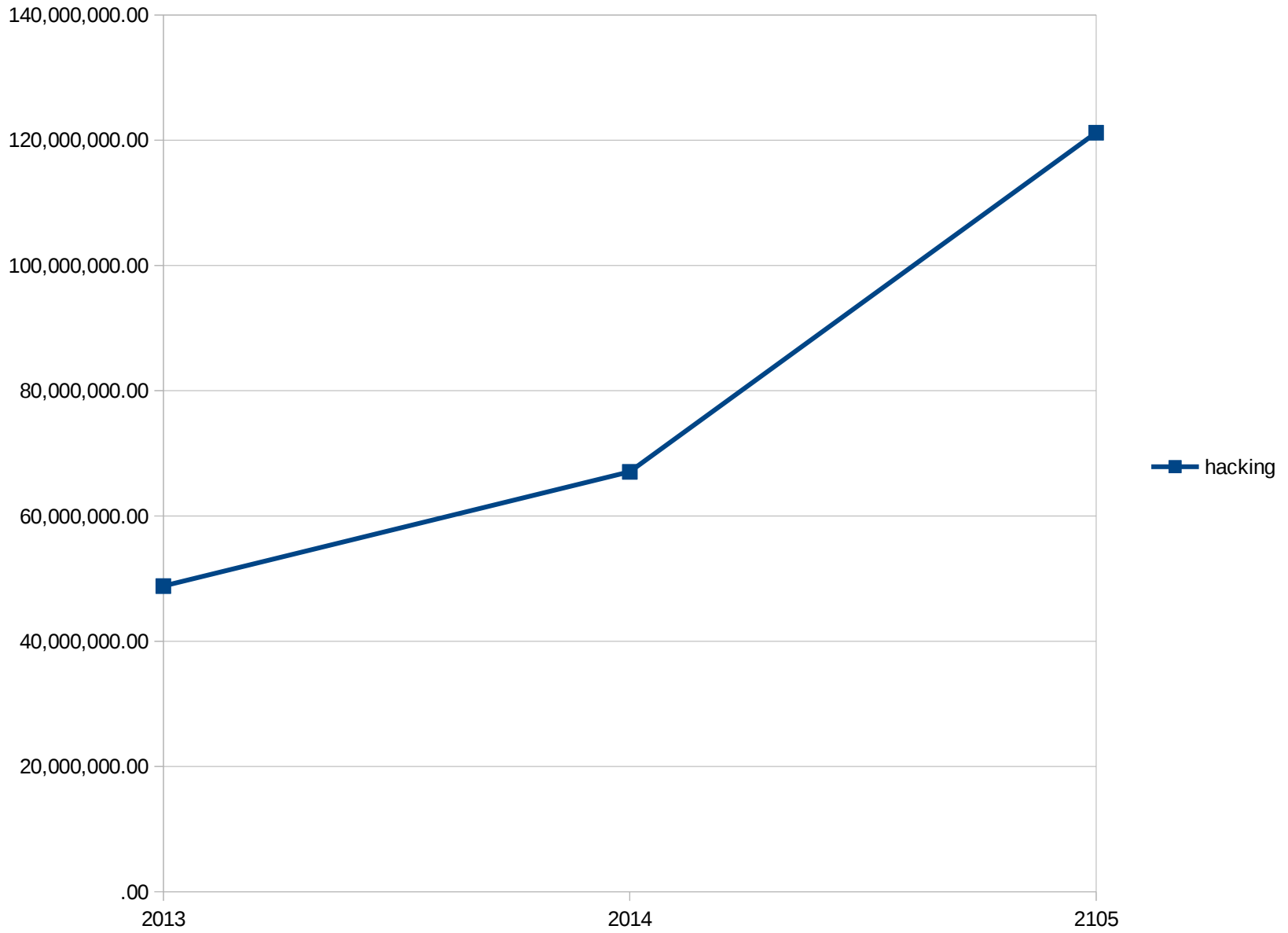
	2013	2014	2015
■ Hacking	48,805,382	67,057,537	121,199,741
■ Insider	3,308,885	421,341	100
■ Unintended disclosure	524,137	175,004	13,162
■ Physical loss	24,533	20,358	1,100
■ Portable device	1,477,386	80,520	604
■ Stationary device	4,120,844	168,125	0

“Data Breaches by the Numbers,” <http://www.securityweek.com/data-breaches-numbers>

See Also: <http://www.privacyrights.org/data-breach>



“Data Breaches by the Numbers,” <http://www.securityweek.com/data-breaches-numbers>

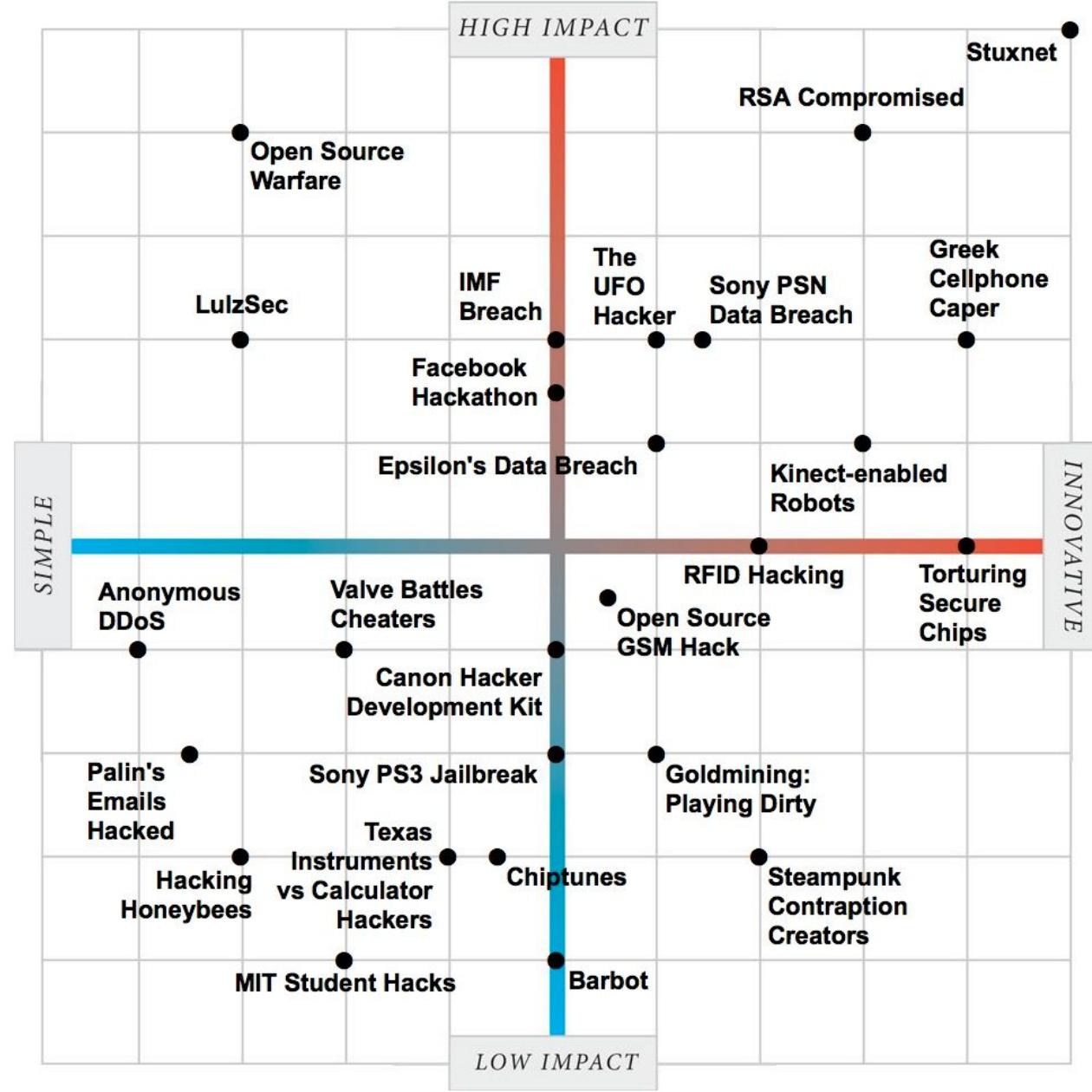


“Data Breaches by the Numbers,” <http://www.securityweek.com/data-breaches-numbers>

<http://spectrum.ieee.org/static/hacker-matrix>

Last updated 6 July, 2011

# The Two Faces of Hacking



Cyber-security

# The cost of immaturity

## The business of protecting against computer-hacking is booming

Nov 7th 2015 | From the print edition



THE average time between an attacker breaching a network and its owner noticing the intrusion is 205 days. Like most statistics touted by the cyber-security industry, such as the supposed annual \$575 billion global cost of 90m cyber-attacks, it is little more than a guesstimate. But there is no doubt that criminals and pranksters are thriving by attacking computers and networks (see [article](#)), that companies are struggling to cope and that businesses offering answers are charging fat fees.

**examples**



# Hackers down German government websites

By Alanna Petroff @AlannaPetroff January 7, 2015: 11:16 AM ET


 Recommend 385



PHOTO-ILLUSTRATION: SHUTTERSTOCK/GNNMONEY

Various German government websites were not working Wednesday.

# Sony Hackers Threaten 9/11 Type Attack at Theaters Showing 'The Interview' Movie

Tuesday, December 16, 2014 Swati Khandelwal

[g+1](#) 69 [f Like](#) 1.4k [f Share](#) 1119 [t Tweet](#) 244 [r Reddit](#) 1 [in Share](#) 7 [ShareThis](#) 1514



# eLS All-Access-Pass

Lifetime-access to all our hands-on IT Security training courses.



## Hackers Can Read Your Private SMS and Listen to Phone Calls

Friday, December 19, 2014 Swati Khandelwal

g+1

195

Like

3.8k

Share

3324

Tweet

593

Reddit

91

Share

118

ShareThis

4748



See Also: Hassan Mourad, "The Fall of SS7—How Can the Critical Security Controls Help?," <https://www.sans.org/reading-room/whitepapers/critical/fall-ss7--critical-security-controls-help-36225>

# KASPERSKY FINDS NEW NATION-STATE ATTACK—IN ITS OWN NETWORK



Inside the headquarters of Kaspersky Lab in Moscow, Dec. 9, 2014.

ALEXANDER

ZEMLIANICHENKO JR./BLOOMBERG/GETTY IMAGES

[https://www.schneier.com/blog/archives/2015/01/hacking\\_attack\\_.html](https://www.schneier.com/blog/archives/2015/01/hacking_attack_.html)

## **Hacking Attack Causes Physical Damage at German Steel Mill**

This sort of thing is still very rare, but I fear it will become more common:

...hackers had struck an unnamed steel mill in Germany. They did so by manipulating and disrupting control systems to such a degree that a blast furnace could not be properly shut down, resulting in "massive" -- though unspecified -- damage.

## Cisco IP Phones Vulnerable To Remote Eavesdropping

Monday, March 23, 2015 Swati Khandelwal

[g+1](#) 174 [Like](#) 2.3k [Share](#) 1542 [Tweet](#) 318 [Reddit](#) 326 [Share](#) 40 [ShareThis](#) 2430



A critical vulnerability in the firmware of Cisco small business phones lets an unauthenticated attacker to remotely eavesdrop on private conversation and make phone calls from vulnerable devices without needing to authenticate, Cisco warned.



**NEWS** **VIDEO** **PEOPLE** **VOICES** **SPORT** **TECH** **LIFE** **PROPERTY** **ARTS + ENTS** **TRAVEL** **MONEY** **INDYBEST** **STUDENT** **OFFERS**

Fashion | Food and Drink | Health & Families | History | [Gadgets and Tech](#) | Motoring | Dating | Crosswords | Gaming | Competitions

Life > Gadgets and Tech > News

## Stingray fake phone masts placed around London to listen in on all calls

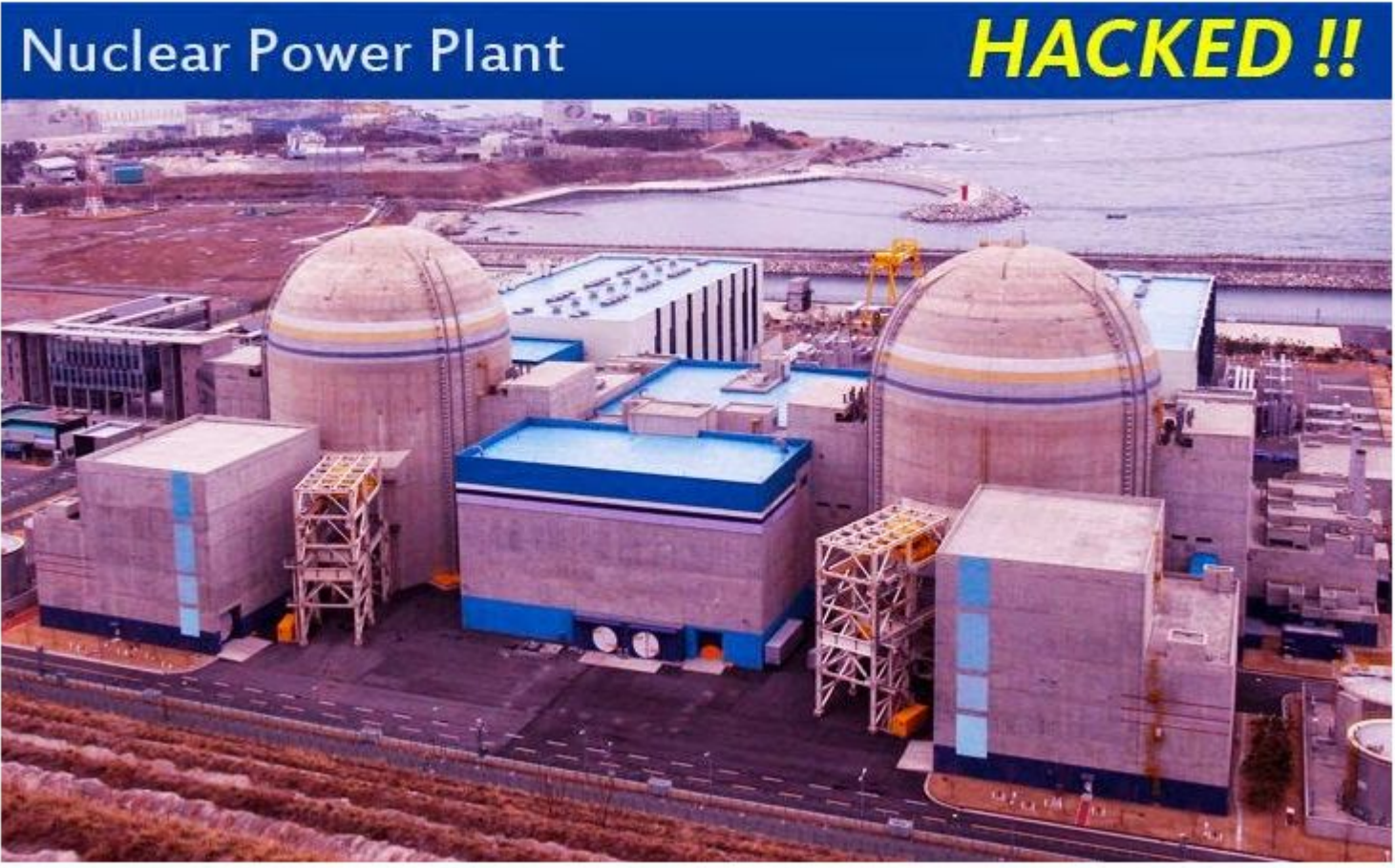


More than 20 fake phone towers, which indiscriminately Hoover up information from phones, were found

# South Korean Nuclear Power Plant Hacked

Wednesday, December 24, 2014 Swati Khandelwal

[G+](#) 176 [Like](#) 2.5k [Share](#) 1740 [Tweet](#) 518 [Reddit](#) 837 [Share](#) 71 [ShareThis](#) 3521





# Why Hacker Gang 'Lizard Squad' Took Down Xbox Live And PlayStation Network

DAVE SMITH | 0 | DEC 26, 2014, 07.19 PM



Like

5



Share



Tweet

7



+1

0



Submit



reddit this!



Email



# Hackers steal \$5M in bitcoin currency during Bitstamp exchange attack

By Fred O'Connor | [Follow](#)

IDG News Service | Jan 6, 2015 10:25 AM PT

RELATED



Top 10 Tech stories 2014:

## Gogo In-flight Internet issues Fake SSL Certificates to its own Customers

Tuesday, January 06, 2015 Swati Khandelwal

<https://firstlook.org/theintercept/2015/02/19/great-sim-heist/>

**THE // INTERCEPT**

FEATURES

GREENWALD

FROOMKIN

DOCUMENTS

STAFF

CONTACT

//



# ***THE GREAT SIM HEIST***

**HOW SPIES STOLE THE KEYS TO THE ENCRYPTION CASTLE**

# Computer hackers targeting cars to expose vulnerability



By [Eduardo Arrufat](#)  
Jul 27, 2013 in [Technology](#)

LIKE THIS ARTICLE

18



<http://www.digitaljournal.com/article/355222>

## This 'Killer USB' can make your Computer explode

Thursday, March 12, 2015 Swati Khandelwal

[g+1](#) 546 [Like](#) 8.5k [Share](#) 13.3K [Tweet](#) 1084 [Reddit](#) 29 [Share](#) 89 [ShareThis](#) 16K



Can Hackers turn a remote computer into a bomb and explode it to kill someone, just like they do in hacker movies? Wait, wait! Before answering that, Let me tell you an interesting story about Killer USB drive:



SIEM Insight



When Minutes Count: How experts fight advanced threats

MORE +

[Home](#) > [Security](#)

# Cisco warns of default SSH keys shipped in three products


# Barracuda appliances contain backdoors

By Dan Kaplan on Jan 25, 2013 6:32 AM

Filed under *Applications*

**Spam and Virus Firewall, Web Application Firewall, Web Filter and SSL VPN.**

 Like 10

 Tweet 5

6

 Share 12

*Comment Now*



A slew of products from security provider Barracuda Networks contain a backdoor that could enable outsiders to remotely access accounts and steal information.

"Undocumented operating system user accounts", or backdoors, can be accessed via Secure Shell (SSH), a protocol that permits encrypted remote login and communication.

<http://www.scmagazine.com/barracuda-appliances-susceptible-to-backdoor-access/article/277391/>



# CVE-2015-7755: Juniper ScreenOS Authentication Backdoor

Posted by [hdmoore](#) in [Information Security](#) on Dec 20, 2015 6:00:44 PM

On December 18th, 2015 Juniper issued an [advisory](#) indicating that they had discovered unauthorized code in the ScreenOS software that powers their Netscreen firewalls. This advisory covered two distinct issues; a backdoor in the VPN implementation that allows a passive eavesdropper to decrypt traffic and a second backdoor that allows an attacker to bypass authentication in the SSH and Telnet daemons. Shortly after Juniper posted the advisory, an employee of Fox-IT [stated](#) that they were able to identify the backdoor password in six hours. A quick [Shodan search](#) identified approximately 26,000 internet-facing Netscreen devices with SSH open. Given the severity of this issue, we decided to investigate.

Juniper's advisory mentioned that versions 6.2.0r15 to 6.2.0r18 and 6.3.0r12 to 6.3.0r20 were affected. Juniper provided a new 6.2.0 and 6.3.0 build, but also rebuilt older packages that omit the backdoor code. The rebuilt older packages have the "b" suffix to the version and have a minimal set of changes, making them the best candidate for analysis. In order to analyze the firmware, it must be unpacked and then decompressed. The firmware is distributed as a ZIP file that contains a single binary. This binary is a decompression stub followed by a gzip-compressed kernel. The x86 images can be extracted easily with binwalk, but the XScale images require a [bit more work](#). ScreenOS is not based on Linux or BSD, but runs as a single monolithic kernel. The SSG500 firmware uses the x86 architecture, while the SSG5 and SSG20 firmware uses the XScale (ARMB) architecture. The decompressed kernel can be loaded into IDA Pro for analysis. As part of the analysis effort, we have made decompressed binaries available in a [GitHub repository](#).

Although most folks are more familiar with x86 than ARM, the ARM binaries are significantly easier to compare due to minimal changes in the compiler output. In order to load the SSG5 (ssg5ssg20.6.3.0r19.0.bin) firmware into IDA, the ARMB CPU should be selected, with a load address of 0x80000 and a file offset of 0x20. Once the binary is loaded, it helps to identify and tag common functions. Searching for the text "strcmp" finds a static string that is referenced in the *sub\_ED7D94* function. Looking at the strings output, we can see some interesting string references, including *auth\_admin\_ssh\_special* and *auth\_admin\_internal*. Searching for "auth\_admin\_internal" finds the *sub\_13DBEC* function. This function has a "strcmp" call that is not present in the 6.3.0r19b firmware:

<https://community.rapid7.com/community/infosec/blog/2015/12/20/cve-2015-7755-juniper-screenos-authentication-backdoor>



# Et tu, Fortinet? Hard-coded password raises new backdoor eavesdropping fears

Discovery comes a month after competitor Juniper disclosed unauthorized code.

by Dan Goodin - Jan 12, 2016 11:10pm EET

Share

Tweet

Email

34



<http://arstechnica.com/security/2016/01/et-tu-fortinet-hard-coded-password-raises-new-backdoor-eavesdropping-fears/>

**ATMs**

# Researcher Demonstrates ATM 'Jackpotting' at Black Hat Conference

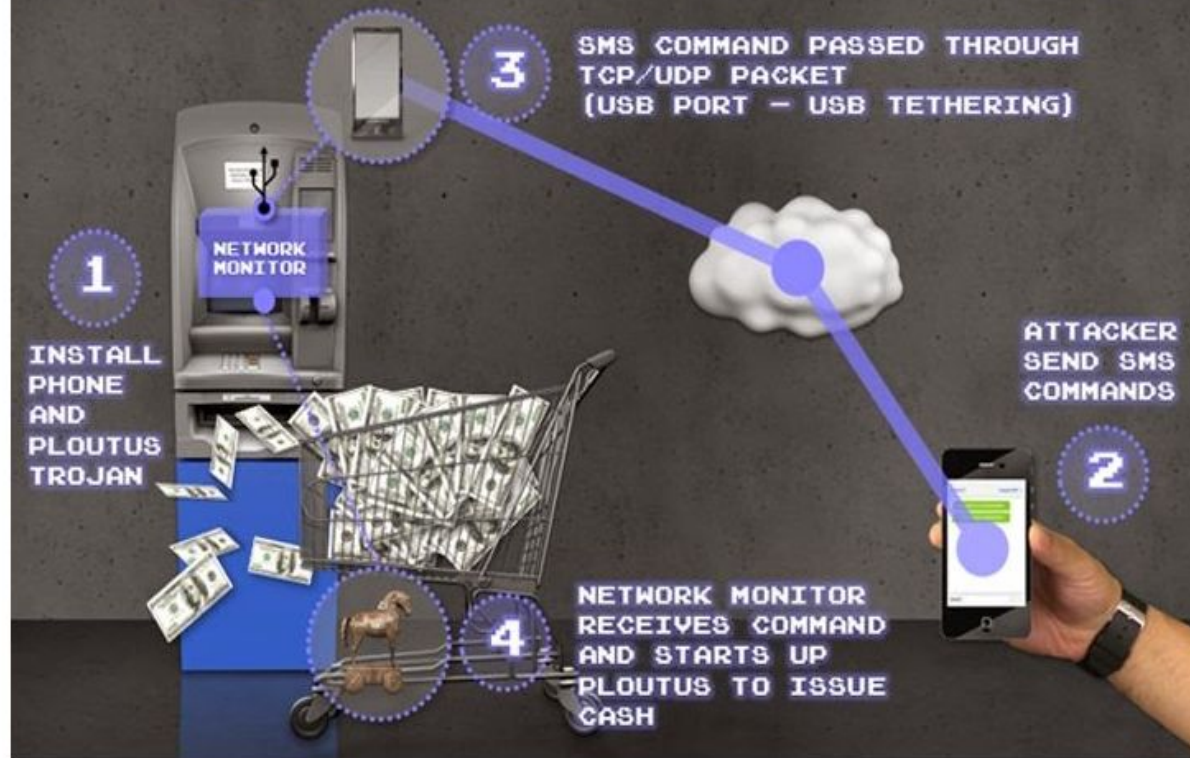
By Kim Zetter   July 28, 2010 | 8:37 pm | Categories: [Black Hat Conference](#), [Cybersecurity](#), [Hacks and Cracks](#)

 [@KimZetter](#) · 3,017 followers



<http://www.wired.com/threatlevel/2010/07/atms->

# Hacking ATMs with Just a Text Message



As we reported earlier, Microsoft will stop supporting the Windows XP operating system after 8th April, apparently 95% of the world's 3 million ATM machines are run on it. Microsoft's decision to [withdraw support for Windows XP](#) poses critical security threat to the economic infrastructure worldwide.

“What was interesting about this variant of Ploutus was that it allowed cybercriminals to simply send an SMS to the compromised ATM, then walk up and collect the dispensed cash. It may seem incredible, but this technique is being used in a number of places across the world at this time.”

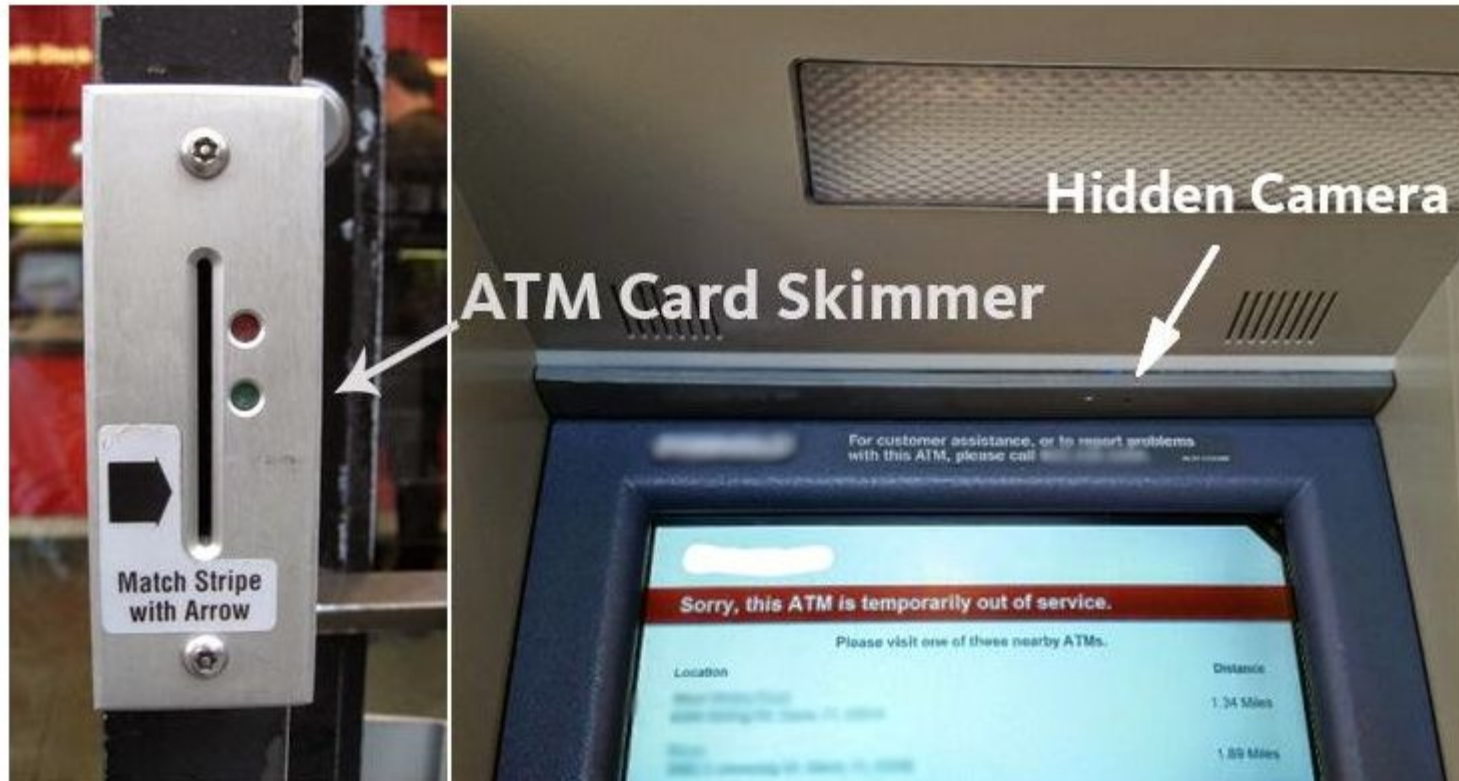
<http://thehackernews.com/2014/03/hacking-atm-machines-for-cash-with-just.html?m=1>

# Beware of Skimming Devices Installed on the ATM Vestibule

## Doors

Wednesday, March 18, 2015 Wang Wei

[g+1](#) [127](#) [Like](#) [1.1k](#) [Share](#) [1630](#) [Tweet](#) [188](#) [Reddit](#) [217](#) [Share](#) [21](#) [ShareThis](#) [2214](#)



Despite anti-skimmer ATM Lobby access control system available in the market, we have seen a number of incidents in recent years where criminals used card skimmers at ATM doors.


Few years back, cyber criminals started using **card skimmers on the door of the ATM vestibule**, where customers have to slide their credit or debit cards to gain access to the ATM.

**It's for your own good!**

# Carrier IQ faces federal probe into allegations software tracks cellphone data

By Sari Horwitz, December 14, 2011



 **View Photo Gallery** - Privacy on the Web: In recent years, lawmakers and advocacy groups have...

Federal investigators are probing allegations that Carrier IQ software found on about 150 million cellphones tracked user activity and sent the information to cellphone companies without informing consumers, according to government officials.

Executives from Carrier IQ traveled to Washington on Tuesday and met with officials at the Federal Trade Commission, which is responsible for protecting consumers and enforcing privacy laws. The executives also met with Federal Communications Commission officials.

The controversy over the software company, based in Silicon Valley, erupted a few weeks ago when security researcher Trevor Eckhart discovered evidence that a piece of software developed by the company and found on smartphones captured every keystroke and text message written by users and sent the information on the handsets to carriers.

[http://articles.washingtonpost.com/2011-12-14/business/35287129\\_1\\_carrier-iq-andrew-coward-trevor-eckhart](http://articles.washingtonpost.com/2011-12-14/business/35287129_1_carrier-iq-andrew-coward-trevor-eckhart)

**Trusting organization**



# The Athens Affair

How some extremely smart hackers pulled off the most audacious cell-network break-in ever

By VASSILIS PREVELAKIS, DIOMIDIS SPINELLIS / JULY 2007



Page 1 2 3 4 5 6 // View All



**On 9 March 2005**, a 38-year-old Greek electrical engineer named Costas Tsalikidis was found hanged in his Athens loft apartment, an apparent suicide. It would prove to be merely the first public news of a scandal that would roil Greece for months.

The next day, the prime minister of Greece was told that his cellphone was being bugged, as were those of the mayor of Athens and at least 100 other high-ranking dignitaries, including an employee of the U.S. embassy [see sidebar "[CEOs, MPs, & a PM.](#)"]

<http://spectrum.ieee.org/telecom/security/the-athens-affair>

**motive**

# Motive

“While security for the user might mean the repulse of `evil hackers [...]

security for the vendor means growing the market and crushing the competition.”

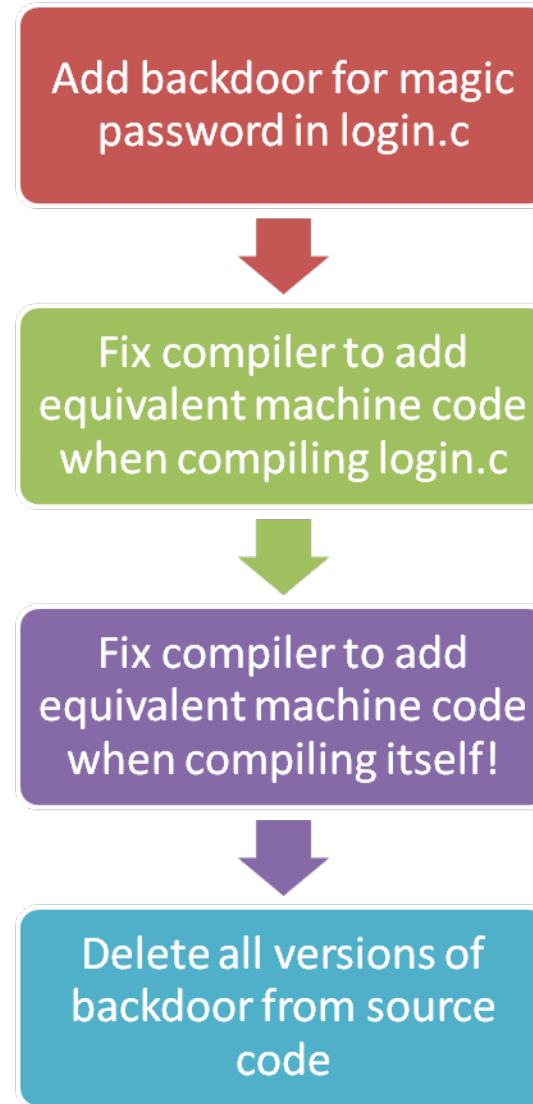
- Ross Anderson, "Security in Open versus Closed Systems - The Dance of Boltzmann, Coase and Moore", Open Source Software : Economics, Law and Policy, Toulouse, France, June 20-21, 2002.

**opportunity**

# Opportunity

## Reflections on Trusting Trust Ken Thompson

Communication of the ACM, Vol. 27, No. 8,  
August 1984



# Opportunity

## Reflections on Trusting Trust Ken Thompson

Communication of the ACM, Vol. 27, No. 8,  
August 1984

“The moral is obvious. You can't trust code that you did not totally create yourself. (Especially code from companies that employ people like me.)”

Add backdoor for magic password in login.c



Fix compiler to add equivalent machine code when compiling login.c



Fix compiler to add equivalent machine code when compiling itself!

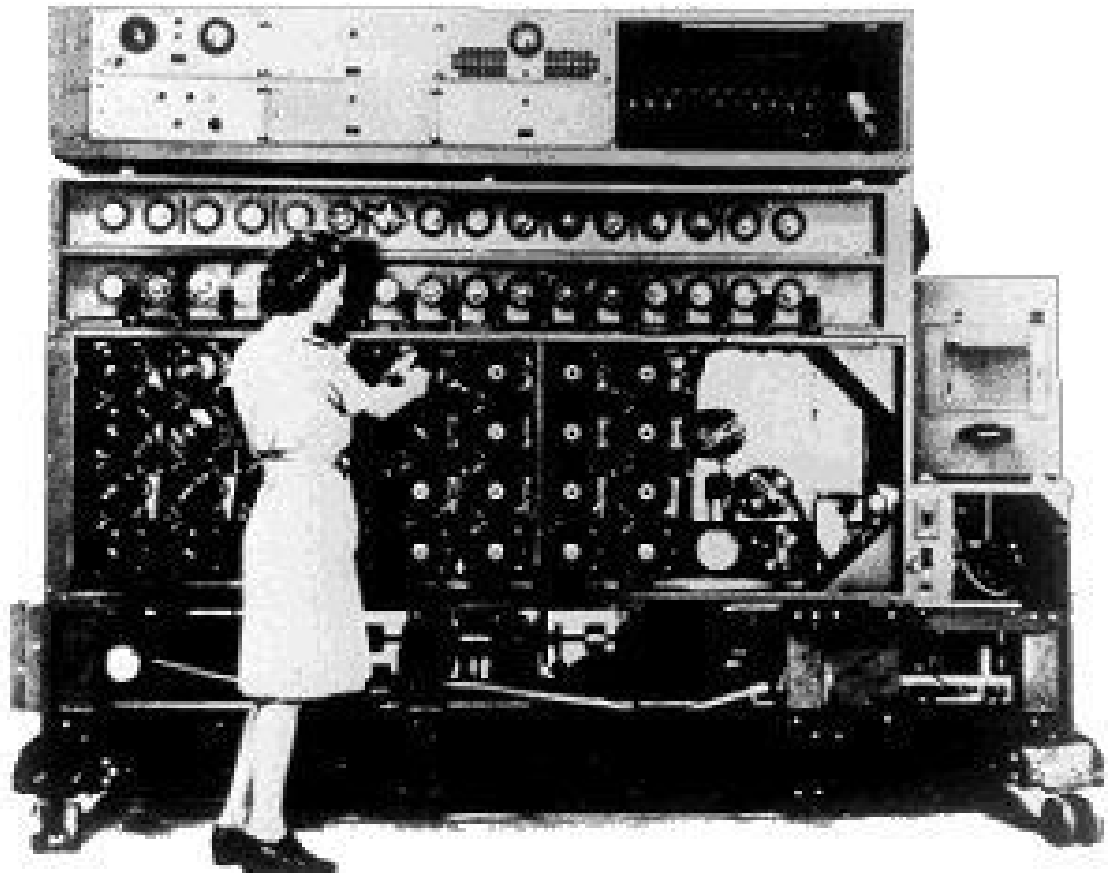
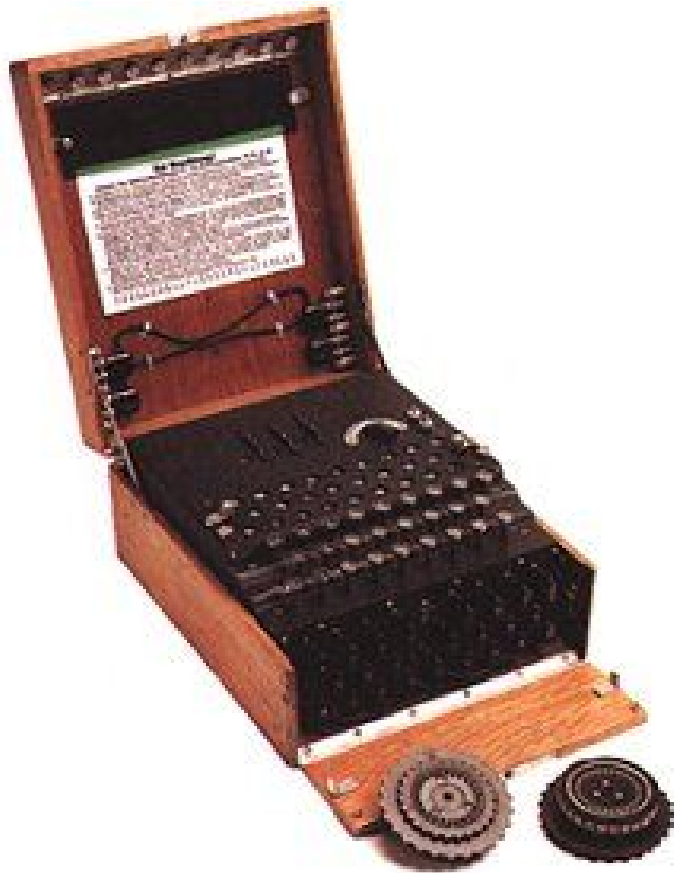


Delete all versions of backdoor from source code

**War stories**

# enigma

+AND+THE+CODE+BREAKERS



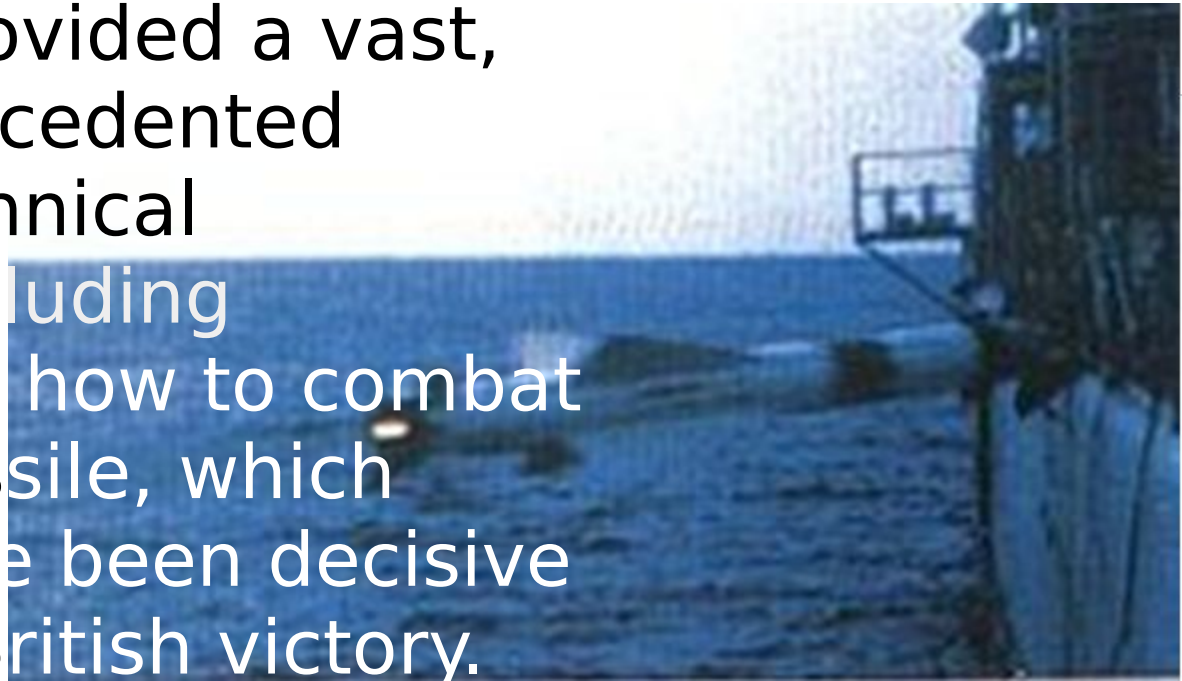
<http://www.quadibloc.com/crypto/ro0204.htm>

<http://www.iwm.org.uk/online/eniga/eni-intro.htm>



# French Weapons in the Falklands

- France manufactured the Exocet [...]
  - France also provided a vast, virtually unprecedented amount of technical assistance, including information on how to combat the Exocet missile, which well have been decisive assuring a British victory.



<http://www.time.com/time/magazine/archive/1996/dom/960909/exclusive.html>

<http://en.wikipedia.org/wiki/Exocet>

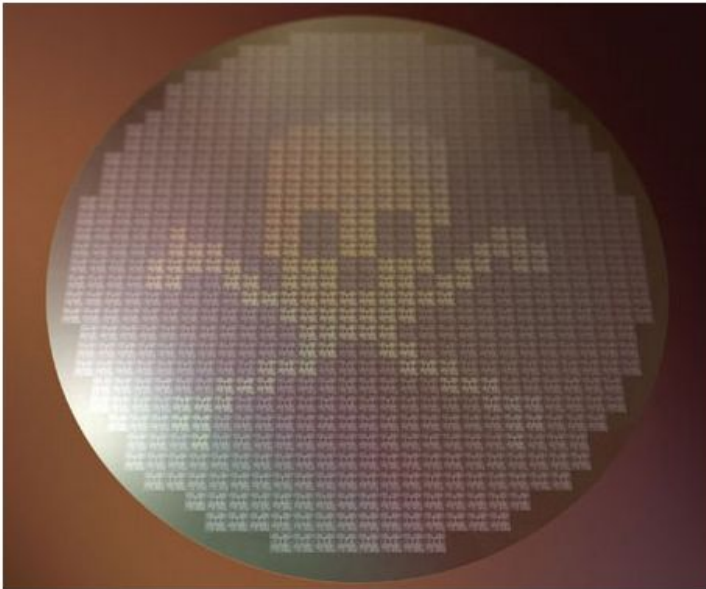
**Kill switches!**

## FEATURE

# The Hunt for the Kill Switch

Are chip makers building electronic trapdoors in key military hardware?  
The Pentagon is making its biggest effort yet to find out

By SALLY ADEE / MAY 2008



**Last September**, Israeli jets bombed a suspected nuclear installation in northeastern Syria. Among the many mysteries still surrounding that strike was the failure of a Syrian radar—supposedly state-of-the-art—to warn the Syrian military of the incoming assault. It wasn't long before military and technology bloggers concluded that this was an incident of electronic warfare—and not just any kind.

[spectrum.ieee.org/may08/6171](http://spectrum.ieee.org/may08/6171)

# Conspiracies

<http://www.f-secure.com/weblog/archives/00002226.html>

<<<

Friday, August 26, 2011

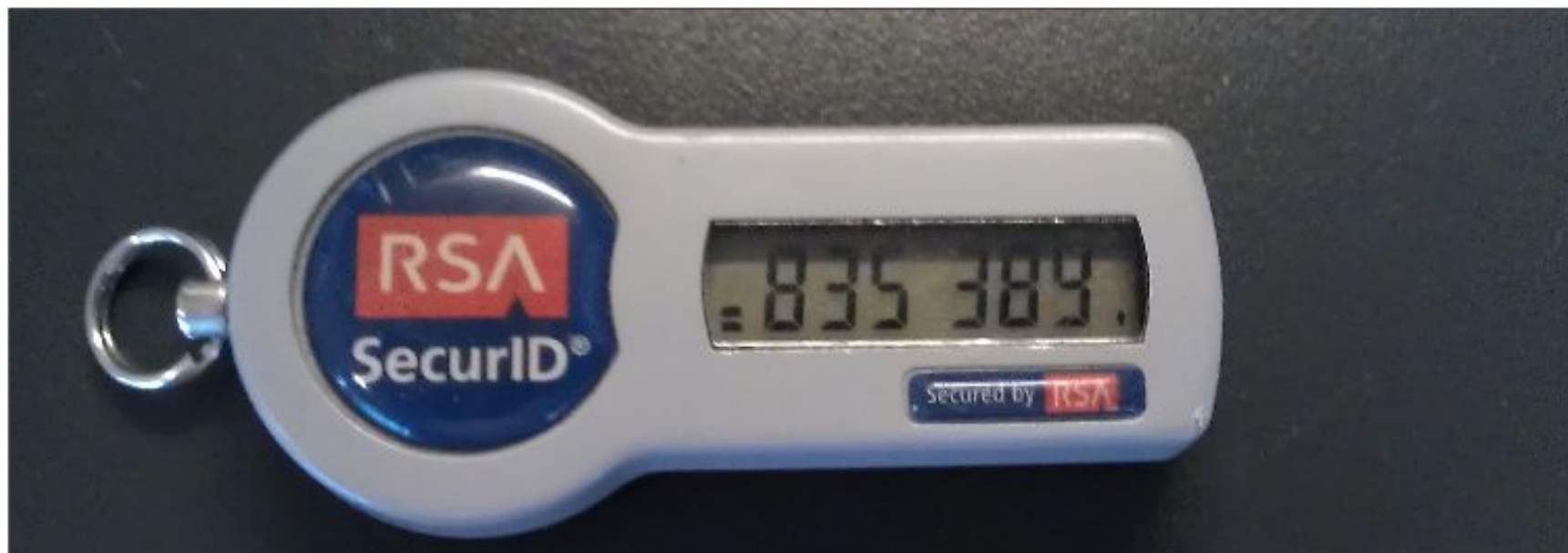
>>>

## How We Found the File That Was Used to Hack RSA

Posted by Mikko @ 09:29 GMT | Comments

RSA was hacked in March. This was one of the biggest hacks in history.

The current theory is that a nation-state wanted to break into **Lockheed-Martin** and **Northrop-Grumman** to steal military secrets. They couldn't do it, since these companies were using **RSA SecurID tokens** for network authentication. So, the hackers broke into RSA with a targeted e-mail attack. They planted a backdoor and eventually were able to gain access to SecurID information that enabled them to go back to their original targets and successfully break in. In the aftermath of the attack, RSA was forced to replace SecurID tokens for their customers around the world.



[http://news.cnet.com/8301-27080\\_3-20068836-245/china-linked-to-new-breaches-tied-to-rsa/](http://news.cnet.com/8301-27080_3-20068836-245/china-linked-to-new-breaches-tied-to-rsa/)

# China linked to new breaches tied to RSA



by [Elinor Mills](#) | June 6, 2011 4:00 AM PDT

Recent attacks on three U.S. defense contractors could be tied to cyberespionage campaigns waged from China, several security experts told CNET.

<http://www.bbc.co.uk/news/technology-13078297>

## FBI closes in on zombie PC gang

**US crime-fighters are closing in on a gang behind a huge botnet after taking control of the criminals' servers.**

It is the first time FBI investigators have used such a method.

The US Justice Department had to seek court permission from a judge to carry out the sting.

It enabled the authorities to issue its own commands effectively to control the machines.



It is an unusual move for police to take over criminal machines

« Misconfigured networks create huge security risks

More F.B.I. Privacy Breaches Reported »

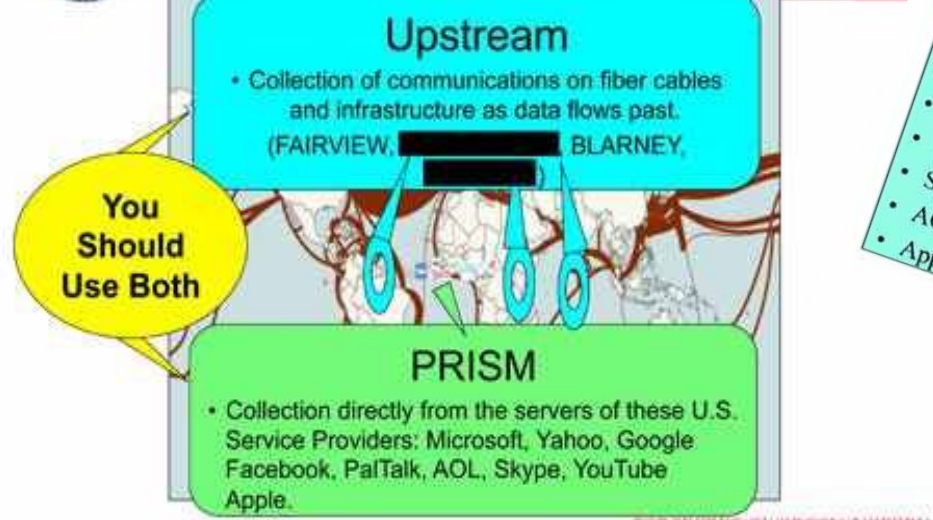
## **Chinese backdoors “hidden in router firmware”**

3:17PM, Tuesday 4th March 2008

The UK's communication networks could be at risk from Chinese backdoors hidden in firmware, according to a security company. SecureTest believes spyware could be easily built into Asian-manufactured devices such as switches and routers, providing a simple backdoor for companies or governments in the Far East to listen in on communications.

<http://vincentarnold.com/blog/chinese-backdoors-hidden-in-router-firmware/>





TOP SECRET//SI//ORCON//NOFORN

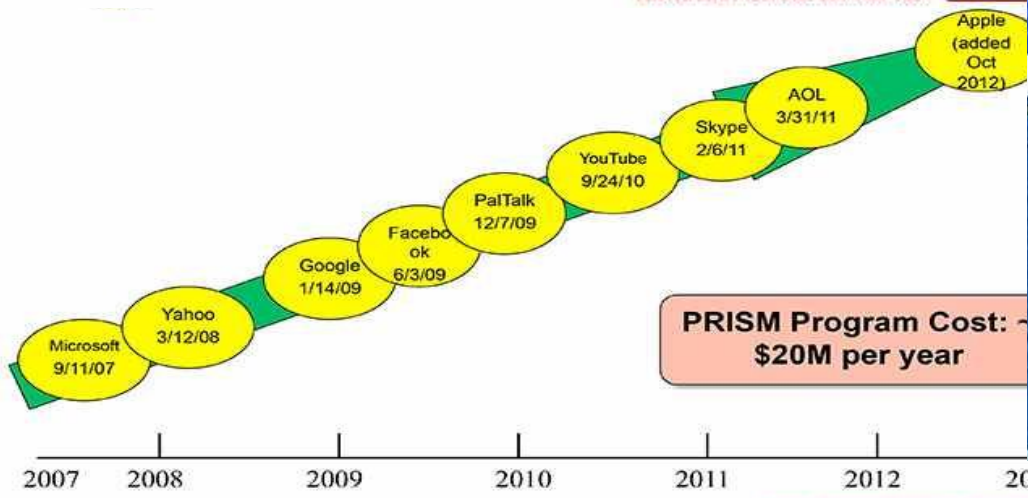
Current Providers

- Microsoft (Hotmail, etc.)
- Google
- Yahoo!
- Facebook
- PalTalk
- YouTube
- Skype
- AOL
- Apple

What Will You Receive in Collection (Surveillance and Stored Comms)? It varies by provider. In general:

- E-mail
- Chat – video, voice
- Videos
- Photos
- Stored data
- VoIP
- File transfers
- Video Conferencing
- Notifications of target activity – logins, etc.
- Online Social Networking details
- Special Requests**

Complete list and details on PRISM web page: Go PRISMFAA



TOP SECRET//SI//ORCON//NOFORN

This is from a Snowden document released by "Le Monde":

#### General Term Descriptions:

HIGHLANDS: Collection from Implants

VAGRANT: Collection of Computer Screens

MAGNETIC: Sensor Collection of Magnetic Emanations

MINERALIZE: Collection from LAN Implant

OCEAN: Optical Collection System for Raster-Based Computer Screens

LIFESAVER: Imaging of the Hard Drive

GENIE: Multi-stage operation: jumping the airgap etc.

BLACKHEART: Collection from an FBI Implant

[...]

DROPMIRE: Passive collection of emanations using antenna

CUSTOMS: Customs opportunities (not LIFESAVER)

DROPMIRE: Laser printer collection, purely proximal access  
(\*\*\*NOT\*\*\* implanted)

DEWSWEEPER: USB (Universal Serial Bus) hardware host tap that provides COVERT link over US link into a target network. Operates w/RF relay subsystem to provide wireless Bridge into target network.

RADON: Bi-directional host tap that can inject Ethernet packets onto the same targets. Allows bi-directional exploitation of denied networks using standard on-net tools.

There's a lot to think about in this list. RADON and DEWSWEEPER seem part

<https://www.documentcloud.org/documents/807030-ambassade.html#document/p1>

<https://www.schneier.com/crypto-gram-1311.html>

This is from a Snowden document released by "Le Monde":

General Term Descriptions:

HIGHLANDS: Collection from Implants

VAGRANT: Collection of Computer Screens

MAGNETIC: Sensor Collection of Magnetic Fields

MINERALIZE: Collection from LAN Implants

OCEAN: Optical Collection System  
Screens

LIFESAVER: Imaging of the Hard Drive

GENIE: Multi-stage operation: [unclear] gap etc.

BLACKHEART: Collection from an [unclear]

[...]

DROPMIRE: Passive collection of emanations using antenna

CUSTOMS: Customs opportunities (not LIFESAVER)

DROPMIRE: Laser printer collection, purely proximal access  
(\*\*\*NOT\*\*\* implanted)

DEWSWEEPER: USB (Universal Serial Bus) hardware host tap that  
provides COVERT link over US link into a target network.  
Operates w/RF relay subsystem to provide wireless Bridge into  
target network.

RADON: Bi-directional host tap that can inject Ethernet packets  
onto the same targets. Allows bi-directional exploitation of  
denied networks using standard on-net tools.

There's a lot to think about in this list. RADON and DEWSWEEPER seem part

<https://www.documentcloud.org/documents/807030-ambassade.html#document/p1>

<https://www.schneier.com/crypto-gram-1311.html>

**“Attacks only get better”**

## Former Microsoft Privacy Chief Says He No Longer Trusts The Company

Tuesday, October 01, 2013 - by [Joel Hruska](#)



Microsoft's onetime Chief Privacy Advisor, Caspar Bowden, has come out with a vote of no-confidence in the company's long-term privacy measures and ability or interest to secure user data in the wake of the NSA's PRISM program. From 2002 - 2011, Bowden was in charge of privacy at [Microsoft](#), and oversaw the company's efforts in that area in more than 40 countries, but claims to have been unaware of the PRISM program's existence while he worked at the company. In the two years since leaving Microsoft, Bowden has ceased carrying a cell phone and become a staunch open source user, claiming that he no longer trusts a program unless he can see the source.



"The public now has to think about the fact that anybody in public life, or person in a position of influence in government, business or bureaucracy, now is thinking about what the NSA knows about them. So how can we trust that the decisions that they make are objective and that they aren't changing the decisions that they make to protect their career? That strikes at any system of representative government."

As Bowden goes on to point out, if you aren't a US citizen, you have no protection whatsoever from [PRISM](#).

[hothardware.com/News/Former-Microsoft-Privacy-Chief-Says-He-No-Longer-Trusts-The-Company/](http://hothardware.com/News/Former-Microsoft-Privacy-Chief-Says-He-No-Longer-Trusts-The-Company/)

- Stallman: How Much Surveillance Can Democracy Withstand?

Robust Protection for Privacy Must Be Technical

[wired.com/opinion/2013/10/a-necessary-evil-what-it-takes-for-democracy-to-survive-surveillance/](http://wired.com/opinion/2013/10/a-necessary-evil-what-it-takes-for-democracy-to-survive-surveillance/)



# Physical vs. Digital world

- what Morpheus might have said
  - “Do you believe that my being stronger or faster has anything to do with my muscles in this place?”
- mediation, proxies, and trust

# Internationally

- “Top Digital Security trends”:
  - Software-Defined Security
  - Big data security Analytics
  - Intelligent / Context-aware security Analytics
  - Application isolation
  - Endpoint threat detection & response
  - Website protection
  - Adaptive access
  - People-centric security
  - Securing the Internet of Things



# Internationally

- “Top Digital Security Trends to Watch Out For”
  - Software-defined security
  - Big data security
  - Intelligent security
  - Application security
  - Endpoint threat protection
  - Website protection
  - Adaptive access control
  - People-centric security
  - Securing the Internet of Things

**Trust management**