

SysSec

Security Challenges for the Future Internet

Evangelos Markatos

Distr. Computing Systems Laboratory

FORTH-ICS



RoadMap of the talk

Security Challenges: What is the problem?

Hackers are getting more sophisticated

The impact of cyberattacks is getting larger

What have we done?

FORWARD: study emerging threats

What will we do?

SysSec: 4-year NoE to consolidate Research in managing threats for the Future Internet



RoadMap

Security Challenges: What is the problem?

Hackers are getting more sophisticated

The impact of cyberattacks is getting larger

What have we done?

FORWARD: study emerging threats

What will we do?

SysSec: 4-year NoE to consolidate Research in managing threats for the Future Internet



New attack pathways

Hackers use new ways to attack

Social Networks (e.g. Facebook users)

Twitter

Search Engines (e.g. Google users)

Corrupt ordinary



Do you trust your “friends” on social networking sites?

www.gartner-brasscom.com

COMPUTERWORLD Security

Home News Blogs In Depth Reviews White Papers Newsletters IT Jobs

Google™ Custom Search **SEARCH**

News

- + Blogs
- + Shark Bait
- Knowledge Centers
 - + Operating Systems
 - + Networking & Internet
 - + Mobile & Wireless
 - **Security**
 - Cybercrime & Hacking
 - Spam, Malware & Vulnerabilities
 - Security Hardware & Software
 - Standards & Legal Issues
 - Privacy
 - Intellectual Property & DRM
 - Disaster Recovery
 - + Storage

Koobface worm to users: Be my Facebook friend

New variant steals log-in credentials for Facebook, MySpace, other social networking sites

By Gregg Keizer
March 2, 2009 12:00 PM ET

Comments (5) Recommended (107) Digg Twitter Share/Email

Computerworld - A worm that hit Facebook last December has resurfaced, a security researcher said today, and is now hijacking user accounts -- not only for that social networking service, but also for MySpace, Friendster, LiveJournal and others.

The Koobface worm is again making the rounds on Facebook, said Jamz

Come and discover a place where technological wealth matches natural wealth.

Come and discover Brazil.



Symbol Get Quote Keyword Search

- Subscribe to Money
- Free Trial
- Magazine Customer Service

Home Business News Markets Personal Finance Retirement Technology Luxury Small Business Fortune Video My Preferences CNN.com

Hackers launch Facebook phishing attack

Perpetrators broke into some member accounts and sent messages to friends urging them to click on fake Web sites.

May 14, 2009: 7:16 PM ET

EMAIL | PRINT | SHARE | RSS

BOSTON (Reuters) -- Hackers launched an attack on Facebook's 200 million users Thursday, successfully gathering passwords from some of them in the latest campaign to prey on members of the popular social networking site.

Facebook spokesman Barry Schnitt said Thursday that the site was in the process of cleaning up damage from the

Quick Vote

Do you think the changes being made at Chrysler and General Motors will save the companies?

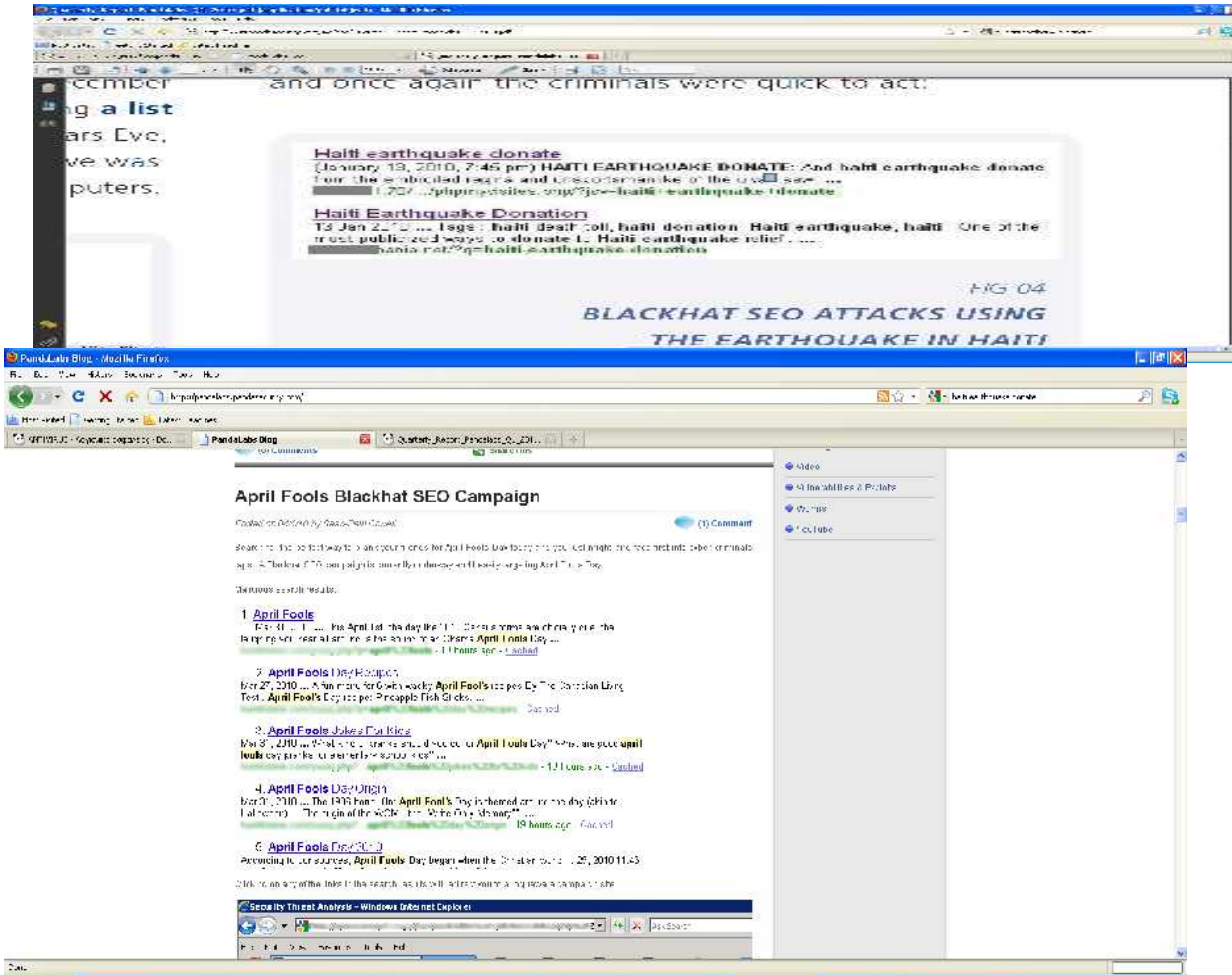
- Yes, both of them
- Only GM
- Only Chrysler
- Neither

Top Stories Most Popular Stories Most Popular Videos

1. Million-dollar homes and gardens
2. Twitter nabs top app maker
3. Angry Schwab bond-fund customers win in court
4. Here come the profit reports
5. 'Young invincibles' imperil health reform



Are you really getting what you Googled for?



Source: PANDA SECURITY



Can birds tweet malware?

Twitter message could be cyber criminal at work - CNN.com - Windows Internet Explorer

http://edition.cnn.com/2009/06/21/cyber.criminals/index.html

INTERNATIONAL
CNN.com/technology

HOME ASIA EUROPE U.S. WORLD WORLD BUSINESS TECHNOLOGY ENTERTAINMENT WORLD SPORT TRAVEL ON TV VIDEO IREPORT CNN MOBILE

Hot Topics » Planet In Peril • Eco Solutions • iPhone • Digital Biz • more topics »

Weather Forecast Edition: U.S. | Arabic | Set Pref

digitalbiz IN ASSOCIATION WITH KONICA MINOLTA

Twitter message could be cyber criminal at work

June 22, 2009 -- Updated 2036 GMT (0436 HKT)

STORY HIGHLIGHTS

- Some officials say cyber crime has eclipsed drug trade as a money maker
- Latest ploy is planting malicious software in intriguing Twitter topics
- Some companies give in to extortion and remain silent, officials say
- Skimmed credit card numbers can be found for sale on Web sites

Next Article in Technology »

By Kevin Voigt
CNN

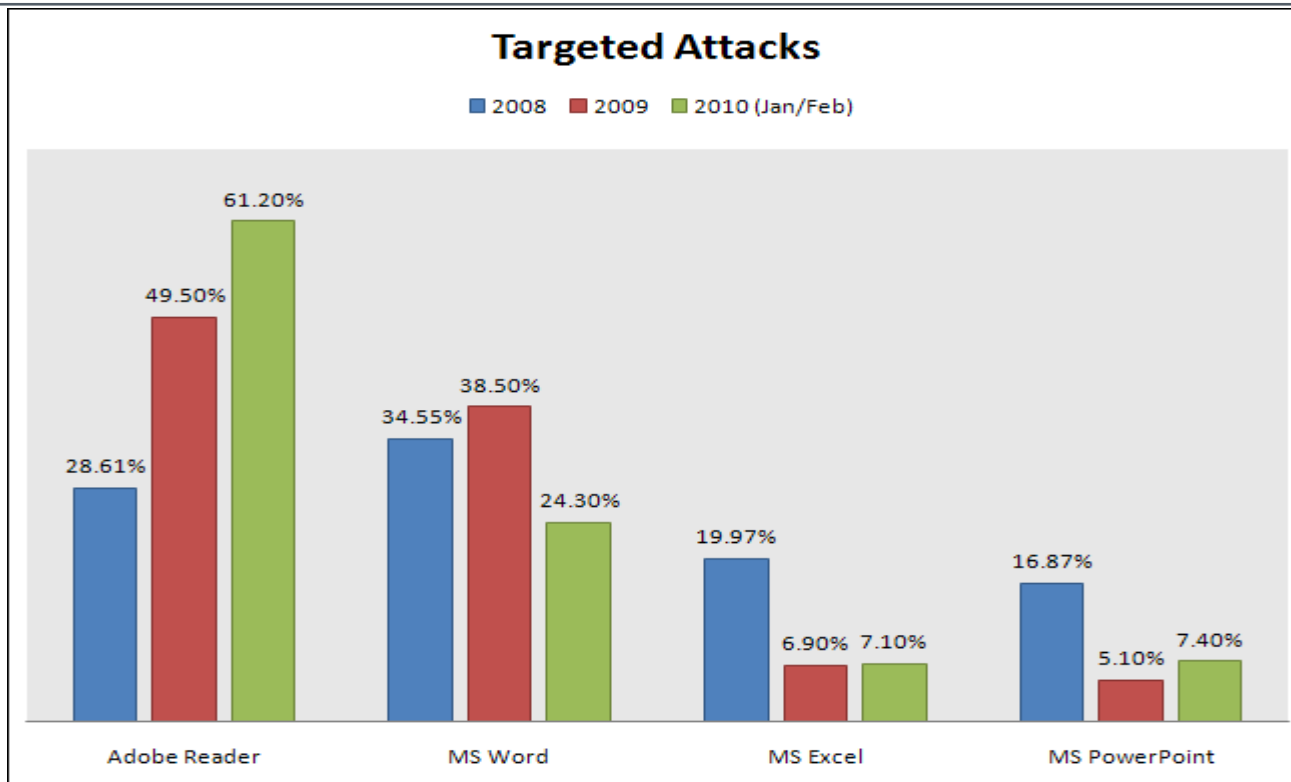
(CNN) -- Cyber criminals are setting snares that move at the speed of news.

Panda Security, a Spain-based antivirus maker, has been monitoring an onslaught of links with malicious software, or "malware," on Twitter that tag

Most Popular on CNN

Internet 150%

Exploits do not come only in .exe files



Hackers use ordinary documents (e.g. PDF, WORD) to deliver exploits

Source: F-Secure

RoadMap

Security Challenges: What is the problem?

Hackers are getting more sophisticated

The impact of cyberattacks is getting larger

What have we done?

FORWARD: study emerging threats

What will we do?

SysSec: 4-year NoE to consolidate Research in managing threats for the Future Internet



What is the impact of attacks?



*“... potential (cyber)attacks against network infrastructures may have widespread and devastating consequences on our daily life:
no more electricity or water at home, rail and plane accidents,
hospitals out of service”*

Viviane Reding

Government: The Parliament under attack

Click to edit Master text styles

Second level

Third level

Fourth level

Fifth level

Houses of Parliament computers infected with Conficker virus

The Houses of Parliament IT system has become infected with the Conficker computer virus, it has emerged, raising questions about possible security flaws at the Palace of Westminster.

By Malina Mumtaz
Published: 7:00AM GMT 27 Mar 2008

TECHNOLOGY TOPICS

- Microsoft in depth
- Technology picks and politics
- Apple in depth
- Google in depth
- Sony in depth
- Nintendo in depth

TELEGRAPH.CO.UK ON DIGG

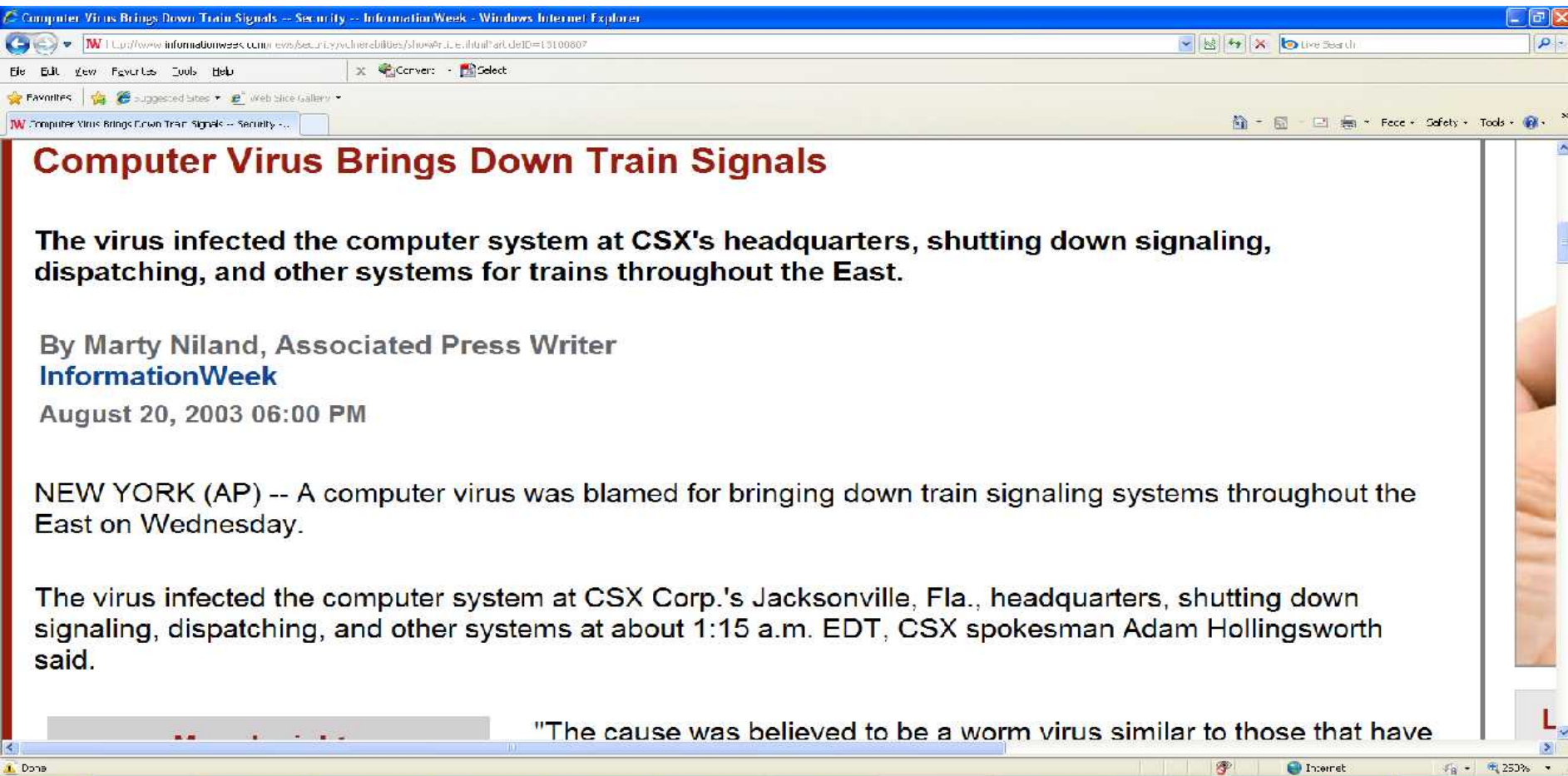
Popular today | Upcoming | Related

- 771 Dug-free inmates put on methadone before they can be released
- 484 Scientists find new species of zaid with colorful genes
- 308 King of the Amur, the national anthem in Amur and Africa (PAC)
- 129 Ranking the nations
- 104 Viewers think new 'Cinderella' is 'too easy'
- 268 'Sexual' lies about 'rehabilitating' suicide

Powered by Telegraph.co.uk powered by digg

Anti Viruses
Computer Virus (Clean)

Transportation: No train signals



Computer Virus Brings Down Train Signals -- Security -- InformationWeek - Windows Internet Explorer

http://www.informationweek.com/ews/security/vulnerabilities/showArticle.html?articleID=13100807

Computer Virus Brings Down Train Signals

The virus infected the computer system at CSX's headquarters, shutting down signaling, dispatching, and other systems for trains throughout the East.

By Marty Niland, Associated Press Writer
InformationWeek
August 20, 2003 06:00 PM

NEW YORK (AP) -- A computer virus was blamed for bringing down train signaling systems throughout the East on Wednesday.

The virus infected the computer system at CSX Corp.'s Jacksonville, Fla., headquarters, shutting down signaling, dispatching, and other systems at about 1:15 a.m. EDT, CSX spokesman Adam Hollingsworth said.

"The cause was believed to be a worm virus similar to those that have

Energy: No electricity

The screenshot shows a Windows Internet Explorer browser window displaying a UPI.com news article. The browser's address bar shows the URL: http://www.upi.com/Science_News/Resource_Wars/2009/10/02/Computer-virus-in-Australian-power-grid/11000TL054514968/. The UPI.com header includes navigation links for Mobile UPI, About UPI, UPI en Español, UPIU - University Media Alliance, and My Account. A search bar is located on the right. Below the header is a navigation menu with categories: Home, Top News, Entertainment, Odd News, Business, Sports, Science, Health, Real Estate, Photos, and Videos. The article's main content area features the title 'Computer virus in Australian power grid' and a sub-header 'Energy Resources'. The article text begins with 'SYDNEY, Oct. 2 (UPI) -- A "sinister" computer virus has infected computers controlling Australia's Integral Energy power grid'. To the right of the article is a large advertisement for PROINSO solar panels, featuring images of solar panels, inverters, and a worker. The ad includes the text 'IMMEDIATE AVAILABILITY!', 'SECURE YOUR PROJECT', and 'BOOK YOUR MODULES AND INVERTERS NOW'. The ad also lists '11000 TL SMA' and '230 Wp Poly Trinasolar'. The browser's taskbar at the bottom shows the system tray with the time 15:03 and a 150% zoom level.

Defense: fighter planes grounded

French fighter planes grounded by computer virus - Telegraph - Windows Internet Explorer

http://www.telegraph.co.uk/news/worldnews/europe/france/457649/france-fighter-planes-grounded-by-computer-virus.html

Home Edit View Favorites Tools Help

Convert Select

Home

French fighter planes grounded by computer virus - I...

Telegraph.co.uk

SEARCH

ENHANCED BY Google

Home News Election 2010 Sport Finance Lifestyle Comment Travel Culture Fashion Jobs Dating Subscriber Offers

UK World Celebrities Obituaries Weird Earth Science Health News Education Topics News Blogs News Video

USA Barack Obama Europe Asia China Middle East Africa and Indian Ocean Australia and the Pacific

HOME > NEWS > WORLD NEWS > EUROPE > FRANCE

French fighter planes grounded by computer virus

French fighter planes were unable to take off after military computers were infected by a computer virus, an intelligence magazine claims.

by Kim Willsher in Paris
Published: 11:43AM GMT 07 Feb 2009

663 diggs digg it

0 twit

Email Print

Text Size + -

EUROPE NEWS

- France news
- German news
- Italy news
- Spanish news
- Russian news
- European Union

INTERNATIONAL JOBS

National Account Manager / Commercial ...
Fleet, £50000

Infrastructure Architect
Sydney, On Application

Avaya Voice Engineer
Sydney, On Application



What about our lives? Are they next?

The screenshot shows a Windows Internet Explorer browser window displaying the 'Future Crimes' website. The address bar shows the URL: <http://www.futurecrimes.org/2010/04/hacking-human-heart-subject-to-technical-attack/>. The page features a green banner with the text 'FUTURE CRIMES: ANTICIPATING TOMORROW'S CRIMES TODAY'. Below the banner is a navigation menu with links for HOME, ABOUT, RESOURCES, and CONTACT. A search bar is located on the right side of the page. The main content area displays the article title 'Hacking the Human Heart: Medical Devices Found Subject to Technical Attack' and a sub-header 'The Crimes'. The article text begins with 'Since the dawn of the 1970's television action show the Six Million Dollar Man, the public has been fascinated by bionics and the integration of technology into the human body. What once seemed to be a far-off science fiction fantasy, is increasingly, however, becoming real. For years, surgeons have been replacing human'. The sidebar on the left lists various crime categories: Artificial Intelligence/Automated Crime (1), Biological and Human Genome (2), Biometrics (2), Cloud Computing (2), Critical-Infrastructure (3), and GPS/Location. The bottom of the page shows a 'Share This Page' section with social media icons and a 'Join the Conversation' link.

RoadMap

Security Challenges: What is the problem?

Hackers are getting more sophisticated

The impact of cyberattacks is getting larger

What have we done?

FORWARD: study emerging threats

What will we do?

SysSec: 4-year NoE to consolidate Research in managing threats for the Future Internet



What are we doing?

2008-2010: created the FORWARD Coordination and Support Action:

Managing Emerging Threats in ICT Infrastructures

Created three working groups (think-tanks) involving experts from Europe/USA/Asia:

- Malware and Fraud
- Smart Environments
- Critical Systems



Their job was to:

Create a list of threats for the future Internet

Rank the threats:

- High, medium, low

Present Po



Threats in Malware and Fraud

Threat	Impact	Likelihood	Oblivious	R&D	Priority
Underground Economy	H	H	L	H	H
Social Networks	H	H	M	H	H
Routing	H	H	L	M	M
New Attack Vectors	M	H	M	H	M
Advanced Malware	M	H	M	M	M
Virtualization and Clouds	H	M	H	M	M
IPv6	M	H	M	M	L
DNS and naming	L	H	M	L	L
Targeted Attacks	M	H	M	L	L
Online Games	L	H	M	L	L

Underground Economy

Dramatic change in goals and models of hackers

shift from **hacking for fun to making profit**

underground economy flourishing

- SPAM, phishing, click fraud, DOS attacks, illegitimate web hosting, botnets

Support structures

underground markets (flow of information, sales, ...)

bullet-proof hosting and “rogue” networks

Possible solutions

attack transactions (flood with useless data)

large scale tracking and data correlation to identify market places



Social Networks

Social networks are attractive targets

huge number of users

large basis of trust among users

detailed information about users

opportunities for fraud and spreading malware

Third-party applications with unrestricted access

They can read private data from a user's disk (i.e. upload files)

Possibility for de-anonymization attacks

Possible solutions

protections from social network providers

- e.g. fine-grain access models, stronger authentication, ...



AV industry in 1998



AV industry in 2008



Image Copyright: IKARUS Security Software GmbH

Threat	Impact	Likelihood	Oblivious	R&D	Priority
Threats due to parallelism	M	M	H	M	H
Threats due to scale	H	M	H	M	H
Mobile device malware	H	H	M	H	H
Denial of service	H	H	L	M	M
False sensor data	H	M	H	M	M
Privacy and ubiquitous sensors	M	M	M	M	M
System maintainability and verifiability	M	H	M	M	M
Sensors and RFID	M	H	M	H	L
Malicious hardware	M	L	H	M	L

Threats due to **parallelism**

Multi-core and multi-threaded technologies

Order of **hundreds of H/W threads** on a single chip

Humans are poor at handling parallelism

Significant increase in

Bugs, security vulnerabilities due to race conditions

Similar technologies are adopted by “weak devices”

Possible solutions:

Invest in building new secure languages, apps, libraries and OSes designed with parallelism in mind

Virtualization and hardware isolation may help



Threats due to **scale**

...The real transformation will be with a future Internet connecting billions of objects, sensors and devices.

Neelie Kroes, Vice President of the European Commission Commissioner for the Digital Agenda

Internet has grown to a 100-million node network

Not counting “weak devices”

Our models are still client-server

We are vulnerable to attacks that leverage and amplify minor vulnerabilities

e.g. Puppetnets, Anti-social Networks

A 100-billion node network will transform what was considered “old” vulnerabilities - DDoS, worms, etc.

Possible solutions

Study and understand interdependencies between systems, model larger systems in security evals, form boundaries



Mobile Device Malware

(Almost) same hardware as regular computers

Face, or will be facing, similar threats as home computers

Run on battery power

PC solutions may not be too heavyweight

Mobility and high connectivity

Attacks from anywhere (i.e. **airports, wifi hotspots**) and propagate on different networks

Easy to lose

Physical security an issue

Possible solutions:

App. analysis in sandbox, intrusion detection in the network, server replication of phone-



RoadMap

Security Challenges: What is the problem?

Hackers are getting more sophisticated

The impact of cyberattacks is getting larger

What have we done?

FORWARD: study emerging threats

What will we do?

SysSec: 4-year NoE to consolidate Research in managing threats for the Future Internet



What's next?

SysSec: managing threats and vulnerabilities for the future Internet

a Network of Excellence (2010-2014)

Why?

- We need to work towards solutions
- We need to collaborate
 - At a European level
 - With our international colleagues
 - Around the world

No country is an island

wrt. Internet security



What is SysSec?

SysSec proposes a *game-changing* approach to cybersecurity:

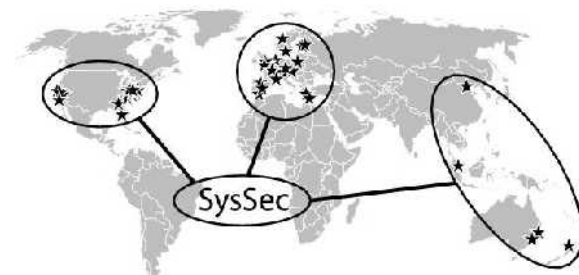
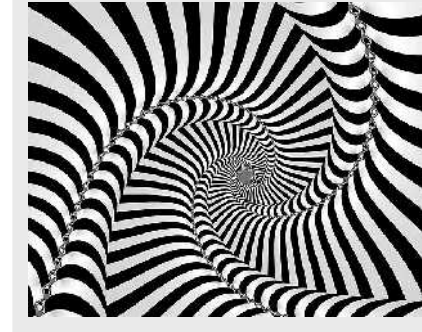
Currently Researchers are mostly reactive:

- they usually track cyberattackers *after* an attack has been launched
- thus, researchers are always one step behind attackers

SysSec aims to break this vicious cycle

Researchers should become more *proactive*:

- Anticipate attacks and vulnerabilities
- Predict and prepare for future threats
- Work on defenses *before* attacks materialize.



SysSec Aim and Objectives (I)

Create an active, vibrant, and collaborating **community of Researchers** with

the expertise, capacity, and determination to anticipate and mitigate the emerging threats and vulnerabilities on the Future Internet.

SysSec aims

to create a **sense of ``community''** among those researchers,

to **mobilize** this community,

to **consolidate** its efforts,

to **expand their collaboration** internationally, and

become **the single point of reference** for Systems Security research in Europe.



SysSec Aim and Objectives (II)

Advance European Security Research well beyond the state of the art

research efforts have been scattered

SysSec aims to **provide a research agenda** and

align their research activities with the agenda

make SysSec a leading player in the international arena.



SysSec Aim and Objectives (III)

Create a **virtual distributed Center of Excellence** in the area of emerging threats and vulnerabilities.

By forming a critical mass of European Researchers and by aligning their activities,

Have the gravitas needed to play a **leading role internationally**, empowered to undertake large-scale, ambitious and high-impact research efforts.

Create a **Center of Academic Excellence** in the area

create an education and training program targeting young researchers and the industry.

lay the foundations for a common graduate degree in the area with emphasis on Systems Security.



SysSec Aim and Objectives (IV)

Maximize the impact of the project by proactive **dissemination** to the appropriate stakeholders.

disseminate its results to international stakeholders so as to form the needed strategic partnerships (with similar projects and organizations overseas) to play a major role in the area.

dissemination within the Member States will

- reinforce SysSec's role as a center of excellence and
- make SysSec a beacon for a new generation of European Researchers.

Create Partnerships and **transfer technology to the European Security Industry.**

create a close partnership with Security Industry

facilitate technology transfer wherever possible to further strengthen the European Market.

Conclusions

Hackers are getting more **sophisticated**

The impact of **cyberattacks** is getting higher

We need to collaborate in order to manage emerging threats on the future Internet

SysSec starts on Sept 1st.

Join us to break



SysSec

Security Challenges for the Future Internet

Evangelos Markatos

markatos@ics.forth.gr



Panel: Trust in the Future Internet

Research

Create defenses for new types of attacks

Education

Educate a new generation of security researchers

Use common sense

Don't talk to strangers

- that you meet on the Internet

Don't trust everyone calling you on the phone

- or sending you email on the Internet

Don't walk in dark alleys

- of the Internet

Back up slides

Critical Systems Overview

Threat	Impact	Likelihood	Oblivious	R&D	Priority
Wireless communication	H	H	M	M	M
Unforeseen cascading effects	H	M	H	H	M
User interface	M	H	M	H	M
The insider threat	M	H	M	H	M
Hidden functionality	M	M	H	M	M
Retrofitting security to legacy systems	M	M	M	L	M
Next Generation Networks	H	H	M	M	M
Safety takes priority over security	L	M	L	M	L
Use of COTS components	M	H	M	M	L