

# **SysSec: A European Network of Excellence in Managing Threats and Vulnerabilities in the Future Internet**

**Federico Maggi  
POLITECNICO DI MILANO**

# RoadMap of the talk

- Security Challenges: What is the problem?
  - Hackers are getting more sophisticated
  - The impact of cyberattacks is getting larger
- 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 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  
EU Commissioner for Justice

# Government: The Parliament under attack

**Telegraph.co.uk**  **SEARCH** ENHANCED BY Google

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

Technology Motoring Health Property Gardening Food and Drink Family Outdoors Active Relationships Expat

Technology News Reviews Topics Advice Video Games Blogs Video Technology Debate2010

HOME > TECHNOLOGY > MICROSOFT

## 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 Matthew Moore  
Published: 7:00AM GMT 27 Mar 2009



The Conficker virus has infected computers in the Houses of Parliament Photo: GETTY

**TECHNOLOGY TOPICS**

- Microsoft in depth
- Technology picture galleries
- Apple in depth
- Google in depth
- Sony in depth
- Nintendo in depth

**TELEGRAPH.CO.UK ON DIGG**

Popular Today Upcoming Related

- 271 Drug-free inmates put on methadone before they are released
- 494 Scientists find new species of lizard with double penis
- 306 Ring of fire: Annular solar eclipse in Asia and Africa [PIC]
- 329 Rocking the Taliban
- 304 Viewers think new Doctor Who is 'too sexy'
- 255 Stressed teachers 'considering suicide'

content by **Telegraph.co.uk** powered by **digg**

Microsoft News Politics UK News

Ads by Google

Anti Virus  
Computer Virus Clean

# Transportation: No train signals

## 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

# Transportation: No cars

**WIRED**

SUBSCRIBE >> SECTIONS >> BLOGS >> REVIEWS >> VIDEO >> HOW-TOS >>

Sign In | RSS Feeds

## THREAT LEVEL

PRIVACY, CRIME AND SECURITY ONLINE



### Hacker Disables More Than 100 Cars Remotely

By [Kevin Poulsen](#)  March 17, 2010 | 1:52 pm | Categories: [Breaches](#), [Crime](#), [Cybersecurity](#), [Hacks and Cracks](#)

More than 100 drivers in Austin, Texas found their cars disabled or the horns honking out of control, after an intruder ran amok in a web-based vehicle-immobilization system normally used to get the attention of consumers delinquent in their auto payments.

Police with Austin's High Tech Crime Unit on Wednesday arrested 20-year-old Omar Ramos-Lopez, a former Texas Auto Center employee who was laid off last month, and allegedly sought revenge by bricking the cars sold from the dealership's four Austin area lots



Done



# Energy: No electricity

Mobile UPI | About UPI | UPI en Español | UPIU - University Media Alliance | My Account

Search:  Stories  Type search term

**UPI.com**  
100 YEARS OF JOURNALISTIC EXCELLENCE

**PROINSO**  
IMMEDIATE AVAILABILITY!  
www.proinso.net

11000 TL SMA + 230 Wp Poly Trinasolar

**SECURE YOUR PROJECT**  
BOOK YOUR MODULES AND INVERTERS NOW  
www.proinso.net

Ads by Google

Home | Top News | Entertainment | Odd News | Business | Sports | Science | Health | Real Estate | Photos | Videos

Resource Wars | Global Water Issues

You are here: [Home](#) / [Energy Resources](#) / [Computer virus in Australian power grid](#)

## Energy Resources

View archive | RSS Feed | Receive Free UPI Newsletter

### Computer virus in Australian power grid

Published: Oct. 2, 2009 at 4:22 PM

Article Photos Listen Comments

SYDNEY, Oct. 2 (UPI) -- A "sinister" computer virus has infected computers controlling Australia's Integral Energy power grid

Email Share 1 retweet

**PROINSO**  
IMMEDIATE AVAILABILITY!  
www.proinso.net

**SECURE YOUR PROJECT**  
BOOK YOUR MODULES AND INVERTERS NOW  
www.proinso.net

11000 TL SMA + 230 Wp Poly Trinasolar

Ads by Google

Internet



# Defense: fighter planes grounded

Telegraph.co.uk

Home News Election 2010 Sport Finance Lifestyle Comment Travel Culture F  
UK World Celebrities Obituaries Weird Earth Science Health News Education Topics Ne  
USA Barack Obama Europe Asia China Middle East Africa and Indian Ocean Australi

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



Share | f


663 diggs digg it

0 tweet

Email | Print

Text Size + -

# What about our lives? Are they next?



FUTURE CRIMES: ANTICIPATING TOMORROW'S CRIMES TODAY

HOME ABOUT RESOURCES CONTACT

The future is already here - it is just unevenly distributed. ~


WEDNESDAY APRIL 14TH 2010

Search

### The Crimes

- Artificial Intelligence/Automated Crime (1)
- Biological and Human Genome (2)
- Biometrics (2)
- Cloud Computing (2)
- Critical-Infrastructure (3)
- GPS/Location

## Hacking the Human Heart: Medical Devices Found Subject to Technical Attack






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

### Future Crimes

*A futurist perspective on the effect of scientific and technological progress on crime, policing and the criminal justice system.*

### Share This Page

Share |   

### Join the Conversation

# RoadMap

- Security Challenges: What is the problem?
  - Hackers are getting more sophisticated
  - The impact of cyberattacks is getting larger
- *What will we do?*
  - *SysSec: 4-year NoE to consolidate Research in managing threats for the Future Internet*



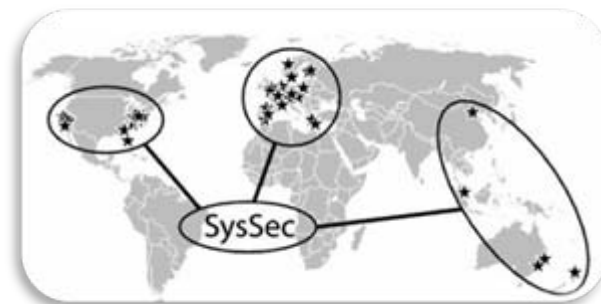
# What's next?

- **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
- 
- |                              |                       |                                |
|------------------------------|-----------------------|--------------------------------|
| ■ Politecnico di Milano (IT) | ■ IPP (Bulgaria)      | ■ UEKAE (Turkey)               |
| ■ Vrije Universiteit (NL)    | ■ TU Vienna (Austria) | ■ FORTH – ICS (Greece)         |
| ■ Institute Eurecom (FR)     | ■ Chalmers U (Sweden) | (see website for updated list) |



# 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 are fragmented
  - 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.

# SysSec: How can you collaborate

- Contribute to the **research roadmap/agenda**
  - Provide feedback on emerging threats
  - Share your ideas on future security issues
- Contribute to our “systems security” **University curriculum**
  - Contribute **homeworks/exams**
  - Contribute/use lab exercises
  - **Teach** some of the courses at your University
  - Share some of your course material
- Become an “Associated Partner” of the project
- <http://syssec-project.eu> and **@syssecproject**



# 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** started on Sept 1<sup>st</sup>.
  - Help us define future security threats
  - Help us teach our students “systems” security
  - Join us to break the vicious cycle of cyberattacks.



**syssec**  **www.syssec-project.eu**

## **SysSec: A European Network of Excellence in Managing Threats and Vulnerabilities in the Future Internet**

**@syssecproject**



**Federico Maggi  
POLITECNICO DI MILANO**