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

Evangelos Markatos
markatos@ics.forth.gr
Outline of the talk

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

- What are we doing about this?
  - SysSec: 4-year NoE to consolidate Research in managing threats for the Future Internet
Outline 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
Government: UK Parliament’s PCs infected

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
Transportation: Cars out of control

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.
Energy: No electricity

Energy Resources

Computer virus in Australian power grid

SYDNEY, Oct. 2 (UPI) -- A "sinister" computer virus has infected computers controlling Australia's Integral Energy power grid.
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.
Last but not least: Stuxnet!

Tailored specifically against SCADA systems, is the most recent demonstration that not only attacks are sophisticated, complex and well-coordinated.

It also demonstrates that the bad guys:
- are very well-equipped
- have ambitious goals (cyber-physical systems)
Rent-a-botnet!

The Day Before Zero
An Ongoing Conversation About Targeted Attacks

Want to rent an 80-120k DDoS Botnet?

Over recent weeks there has been a lot of interest in DDoS botnets – that is to say, rentable botnets that provide DDoS as a managed service. I’ve spoken to a number of people about how easy this is to do, and how practically anyone who happens to know how to use a popular Internet search engine can probably locate the sellers or the hacking message boards they hang around. Perhaps one of the finer points missing about the discussion of renting DDoS botnets pertains to the size.

A fairly typical rate for DDoS botnet rental hovers around the $200 for 10,000 bot agents per day. The rate per day is fairly flexible, and influenced by the actual size of the botnet that the bot master is trying to section off for DDoS services.

There is even a free 3-minute trial!
Outline 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
Predicting “what’s next”

- **SysSec**: managing threats and vulnerabilities for the future Internet
  - a NoE, 2010-2014
  - General approach
    - **Proactive solutions**
    - **Collaborate**
      - At a European level
      - With our international colleagues

- Politecnico di Milano (IT)
- Vrije Universiteit (NL)
- Institute Eurecom (FR)
- BAS (Bulgaria)
- TU Vienna (Austria)
- Chalmers U (Sweden)
- TUBITAK (Turkey)
- FORTH – ICS (Greece)
(see website for updated list)
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.
1. 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 researchers,
     - to mobilize this community,
     - to consolidate its efforts,
     - to expand their collaboration internationally, and
     - become the single point of reference for system security research in Europe.
2. 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)

3. 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,
   - A **leading role internationally**, empowered to undertake **large-scale**, ambitious and high-impact research efforts.

4. 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.
5. 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.

6. 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.
1st SysSec Workshop

By the numbers:

- 23 position papers
  - i.e. where is the security research going?
- 6 (longer) Student/Research papers
- 95 authors
- 36 organizations
- One session on INCO strategy
  - In trustworthy ICT
  - Organized by the BIC project
1st SysSec Workshop – International?
Research Roadmap

- Cyberattacks
- Mobile
- Mobile rootkits
- Phishing
- SCADA vulnerabilities
- Online fraud
- Identity theft
- DDoS
- Mobile malware
- Social networks
- Drive-by downloads
- Botnets
- Scareware Trojans
- Mobility
- Malware
- Underground economy
- Privacy
- Memory corruption
How to collaborate with SysSec?

- Join our constituency (mailing list):
  - http://www.syssec-project.eu

- Contribute to the research roadmap
  - Provide feedback on emerging threats
  - Share your ideas on future security issues

- Contribute to our systems security University curriculum
  - Contribute homeworks/exams, lab exercises
  - Teach some of the courses at your University
  - Share some of your course material

- Send your students to the partners
  - with SysSec Scholarships

- Send your graduates to the SysSec partners
  - With SysSec Marie Curie Fellowships

- Become an Associated Partner
Summary

- Hackers are getting more sophisticated
- The impact of cyberattacks is getting higher
- We need to collaborate to manage emerging threats on the future Internet
  - **SysSec** started on Sept 1st.
  - Help us define future security threats
  - Help us teach our students system security
  - **Join us** to break the vicious cycle of cyberattacks.
SysSec: A European Network of Excellence in Managing Threats and Vulnerabilities in the Future Internet

http://www.syssec-project.eu
http://twitter.com/syssecproject

Evangelos Markatos
FORTH-ICS