

CHALMERS

# Mitigating Cyber Attacks

Magnus Almgren  
Göteborg, 2010-10-19



Postdoc, finansierad av MSB

## 15—20 years ago ...

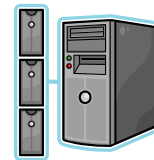
- Internet starting to reach a wider audience
  - most people did not have emails
  - computer security – an afterthought
- The typical hacker, often portrayed as
  - teenager,
  - attack a "chess game"
  - **goal:** some esoteric fame ...
- And today ?

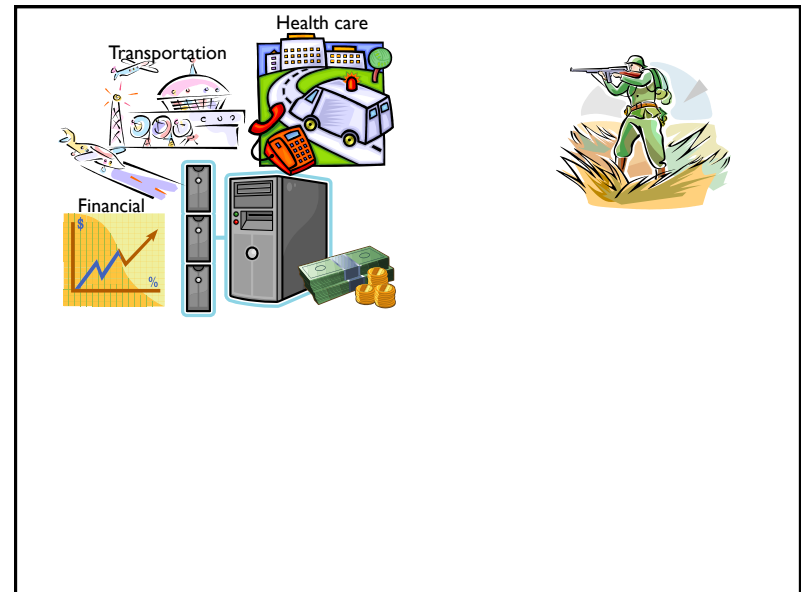
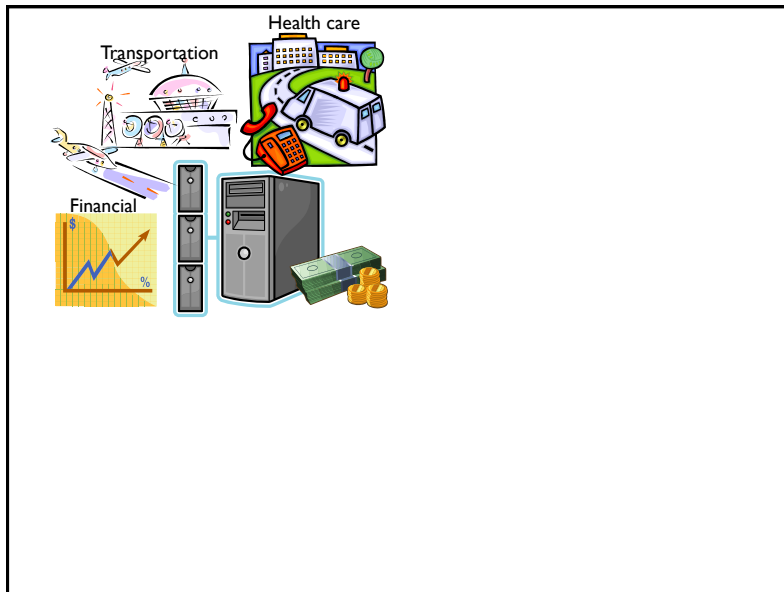


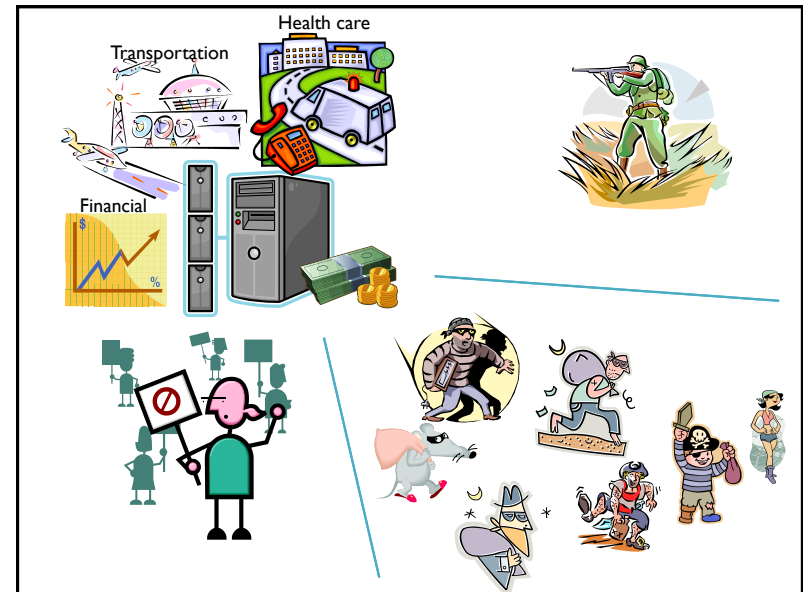
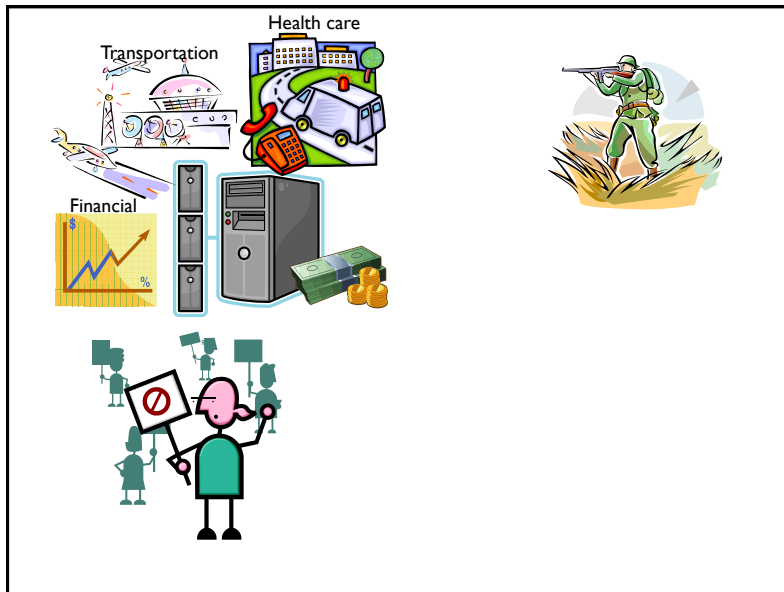
SVT Documentary oct-10, 2010: Att hacka en stormakt (<http://goo.gl/12rd>)

## Outline

- Status today
- Monitoring traffic
- Research Activities
  - Reasoning with alerts from several sensors
  - Monitoring backbone traffic
- European network: SysSec

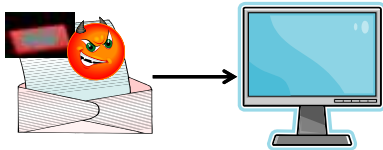






## Malicious Code

- **Many users say:**  
*I would never download unsecure content!*
- But what type of content is safe?

A screenshot of the VFP-SECURE website. The website has a dark blue header with the text 'VFP-SECURE' in white. Below the header, there is a dark blue main content area with some text and links. An orange text box is overlaid on the bottom right of the screenshot, containing the following text:

**Targeted attacks**

- 48% of exploits target Adobe Acrobat / Adobe Reader
- Adobe begins a quarterly patch cycle
- Health Check statistics show that Adobe Reader is among the top unsecured applications

<http://home.mcafee.com/AdviceCenter/most-dangerous-celebrities>

## Dangerous People (!!!)



Cameron Diaz Searches Yield Ten Percent  
Chance of Landing on a Malicious Site



Cyberattack on Google Said to Hit Password System - NYTimes.com <http://www.nytimes.com/2010/04/15/technology/20google.html?pagewanted=all>

The New York Times *Reprints*

This copy is for your personal, noncommercial use only. You can order presentation-ready copies for distribution to your colleagues, clients or customers here or use the "Reprints" tool. This appears next to any article. Visit [www.nytimes.com/reprints](http://www.nytimes.com/reprints) for complete and additional information. Contact a representative at the address below.

REPRINTS: 1-800-421-8503  
INTERNET: [www.nytimes.com/reprints](http://www.nytimes.com/reprints)

APR 15, 2010

**CYRUS**  
JULY 9

### Cyberattack on Google Said to Hit Password System

By JOHN MARKOFF

Ever since Google disclosed in January that Internet intruders had stolen information from its computers, the exact nature and extent of the theft has been a closely guarded company secret. But a person with direct knowledge of the investigation now says that the losses included one of Google's crown jewels, a password system that controls access by millions of users worldwide to almost all of the company's Web services, including e-mail and business applications.

The program, code named Gaia for the Greek goddess of the earth, was attacked in a lightning raid taking less than two days last December, the person said. Described publicly only once at a technical conference four years ago, the software is intended to enable users and employees to sign in with their password just once to operate a range of services.

<http://doi.ieeecomputersociety.org/10.1109/MC.2010.237>

TECHNOLOGY NEWS

# Researchers Fight to Keep Implanted Medical Devices Safe from Hackers

Neal Leavitt

Implantable medical devices have become increasingly popular, and a growing number are equipped with wireless communications technology to increase their usefulness. However, this could make the devices susceptible to hackers.

Implantable medical devices—such as insulin pumps, cardiac pacemakers, and cardiac defibrillators—have become increasingly popular since being introduced about 10 years ago.

a research scientist at the US Department of Energy's Oak Ridge National Laboratory (ORNL).

All this convenience may come with unintended risks: the possibility that hackers could break into these devices and

However, the risk is growing, as is the number of patients using IMDs in part because of the aging of the population.

"The time to prevent future attack scenarios is now," said Paul.

<http://www.zdnetasia.com/malware-link-to-air-crash-inconclusive-62202513.htm>

ZDNet News Security

# Malware link to air crash inconclusive

By Vivian Yeo, ZDNet Asia on August 30, 2010 (4 hours 44 minutes ago)

**Summary**

Still too early to draw direct link between malware and deadly Spanair disaster, say security experts who note proper checks should be reinforced to reduce risk of crash.

Although malware was recently identified as a contributing factor in a Spanair crash two years ago, it is still too early to draw definitive conclusions or panic over possible links to cyberterrorism, security experts say.

A Spanish newspaper reported that the airline's central computer had been infected with Trojans at the time of the disaster, causing a failure to flag technical faults. Spanair's flight 3X 5022, which was said to have taken off with flaps and slats on its wings retracted, crashed shortly after takeoff killing 154 people.

Findings by independent air crash investigators indicated that apart from human oversight, the failure of the system to trigger alerts of the problems led to the tragic incident.

Paul Duddlin, Sophos' head of technology for the Asia-Pacific region, told ZDNet Asia in an e-mail interview, this is possibly the first case of malware being mentioned in relation to a plane crash. However, to what extent the infection contributed to the crash is "not yet clear" as more details of the investigation will only be released in December, Duddlin pointed out.

Whilst there may be public anxiety over just how safe aircraft and airline systems are in the wake of the report, he said carriers and travellers should not be overly concerned about the role of cyberterrorism or cyberwarfare.

"The word 'cyberwarfare' is on a lot of lips lately...so anything which might be malware and, by association, cyberwarfare into the area of civilian aviation sounds as though it is worth worrying about," he said.

**Topics**

reiko hypponen, paul duddlin, accidents and disasters, air disasters, computer security, computer technology, science and technology, spyware and adware, technology, telecommunications

WIRED
SUBSCRIBE
SECTIONS
BLOGS
REVIEWS
VIDEO
HOW
April 10, 2010

THREAT LEVEL
PROTECT, DRIVE AND SECURITY ONLINE

PREVIOUS POST
NEXT POST

### Hacker Disables More Than 100 Cars Remotely

By Kevin Poulsen | March 10, 2010 | 1:02 pm | Categories: [Business](#), [Crime](#), [Cybersecurity](#), [Hacks](#), and [Criminals](#)

More than 100 drivers in Austin, Texas found their cars disabled as the horns blaring 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 26-year-old Omar Ramos-Lopez, a former Texas Auto Center employee who was laid off last month, and allegedly sought revenge by knocking the cars sold from the dealership's lot Austin area lots.

"We initially diagnosed it as mechanical failure," says [Texas Auto Center](#) manager Martin Garcia. "We started having a rash of up to a hundred customers at one time complaining. Some customers complained of the horns going off in the middle of the night. The only option they had was to remove the battery."

The dealership used a system called Webtech Plus as an alternative to repossessing vehicles that haven't been paid for. Operated by Cleveland-based [Pay Technologies](#), the system lets car dealers

smh.com.au
The Sydney Morning Herald
MEGA SHOW PART 1
Gifts + H...
26-27 October

Technology
News, Bio Tech, Security, Enterprise, Sci Tech, Blogs, Digital Life, Computers & Games

You are here: Home » Technology » Security » malware

### 'Sinister' Integral Energy virus outbreak a threat to power grid

Robert Rowan  
October 1, 2009

Comments (25)

Join the conversation  
You're the only person reading this over 74 days' silence  
0 / 20 comments  
Comment on Twitter  
1 Read more

Also by Google  
[Trojan Remover Download](#) [www.virusshare.com](#)  
Free Trojan Scan. Winner of the Best Anti-Spyware. Rated 5 Stars.

#### Top Technology articles

1. US address Australia cyber war
2. Social network using other's data to estimate stress or threat
3. Web site from disorganized
4. iPad becomes top target for malware
5. Developer joins war for 'kill switch' for iPod

» More Technology articles

Latest Comment  
"An update for 'Reader' totally

A virus outbreak is wreaking havoc with Integral Energy's computer network, forcing it to rebuild all 1000 of its desktop computers before the "particularly sinister" bug spreads to the machines controlling the power grid.

A spokesman for Integral Energy, a major energy supplier, confirmed that the company had called in external information security experts to "rebuild all desktop computers to contain and remove the virus".

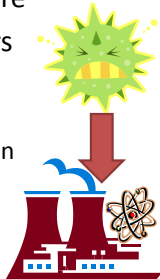
The malware had not affected power supplies to customers or business data and was "contained within Integral Energy's information technologies network", the spokesman said.





## New Era 2010: Stuxnet

- Advanced Malware
  - target specifically Programmable Logic Controllers: Siemens SIMATIC Step 7 software
  - Lots of rumors of goal and who creators
    - designed and released by a government
      - the U.S. or Israel ???
    - **Target:** Bushehr nuclear power plant in Iran (60% of infected hosts in Iran)



Symantec oct-2010: W32.Stuxnet Dossier (<http://goo.gl/pP7S>)

## Stuxnet: Pandora's box ?

- Stuxnet is advanced and one of the first wild malware's targeting PLCs.

- 6—8 people about 6 months to create.

- PLCs exists in many industries

- factory assembly lines, amusement rides, or lighting fixtures.

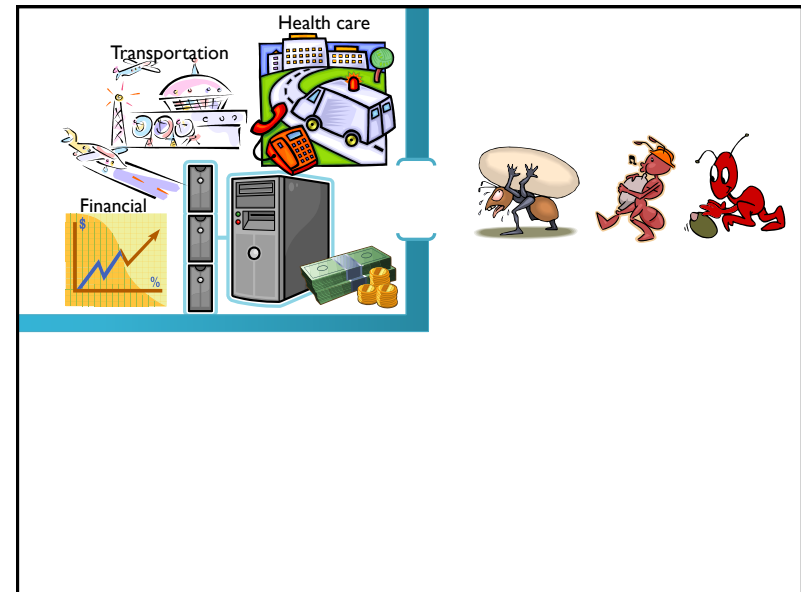
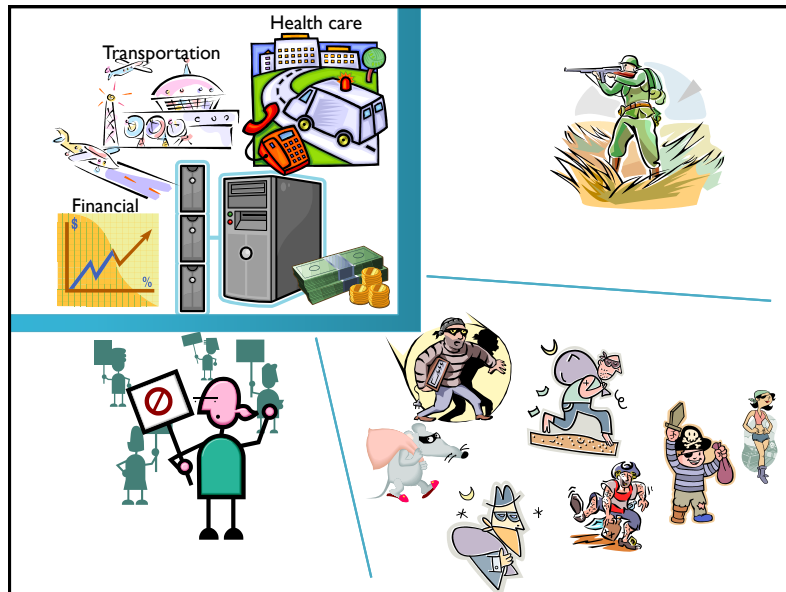


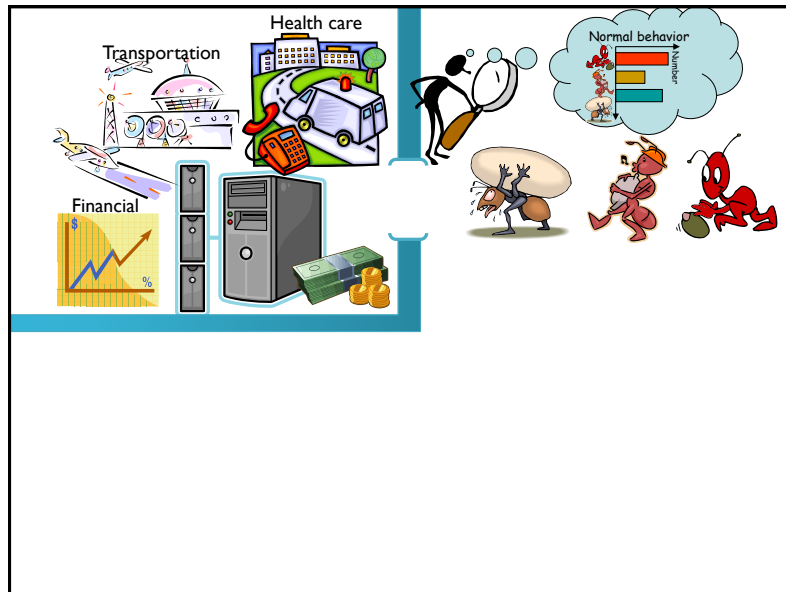
*now blueprint to create malware targeting PLCs*

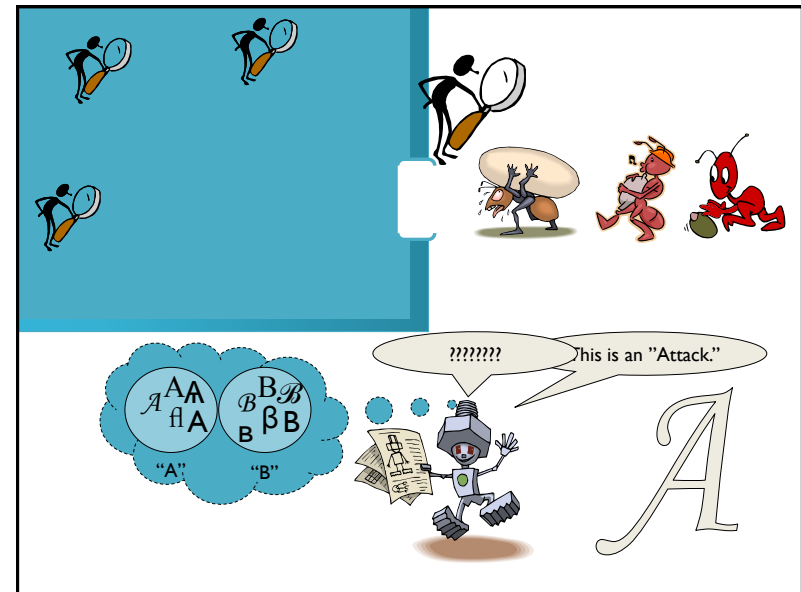
- Compare this with the *Loveletter* virus (2000)
  - 2003/11 there existed 82 different variants of *Loveletter*.
  - It is claimed that more than 5,000 attacks are carried out every day.

Status today

**Monitoring traffic:** *Intrusion Detection Systems*  
Research Activities





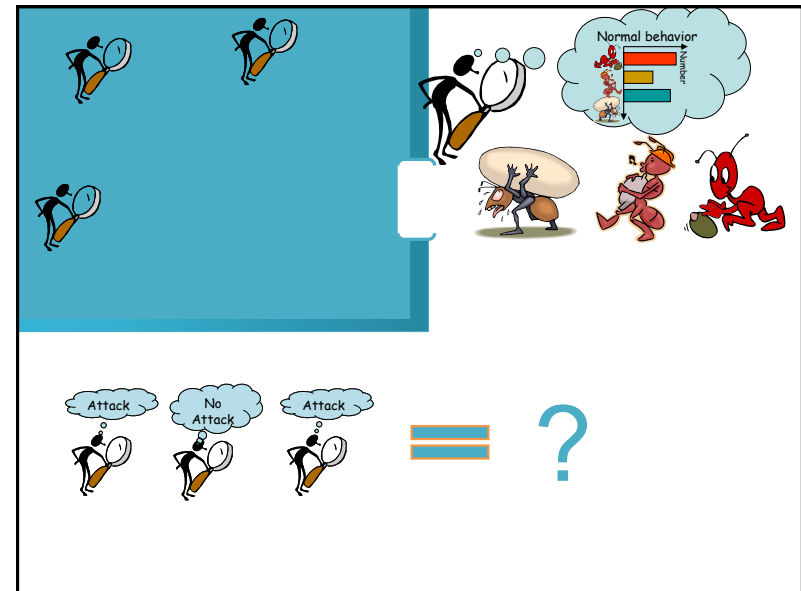


Status today

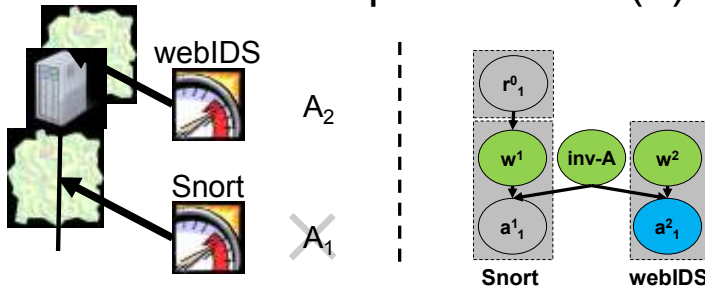
Monitoring traffic

**Research Activities:**

1. Reasoning with alerts from several sensors
2. Monitoring backbone traffic

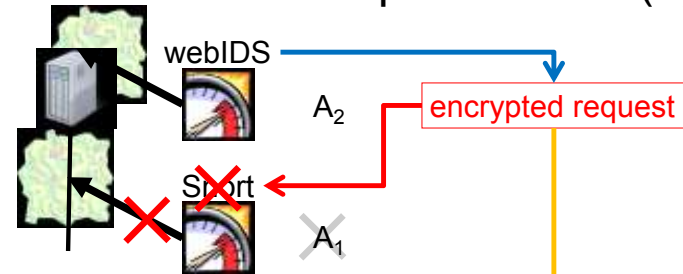


## Scenario multiple sensors (1)



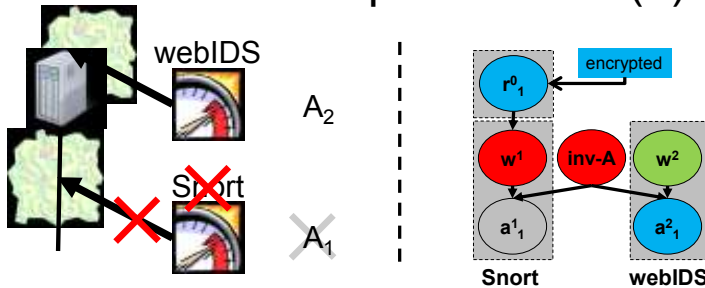
- Normal phf access (no attack)
  - $P(inv-A \mid \dots) = 0.20 = \text{don't investigate}$

## Scenario multiple sensors (2)



- Normal phf access (no attack)
  - $P(inv-A \mid \dots) = 0.20 = \text{don't investigate}$

### Scenario multiple sensors (3)



- Normal phf access (no attack)
  - $P(\text{inv-A} \mid \dots) = 0.20 = \text{don't investigate}$
- **Snort sensor defunct, this may be an attack!**
  - $P(\text{inv-A} \mid \dots) = 0.54 = \text{investigate}$
  - $P(w^1 \mid \dots) = 0.01 = \text{sensor broken}$

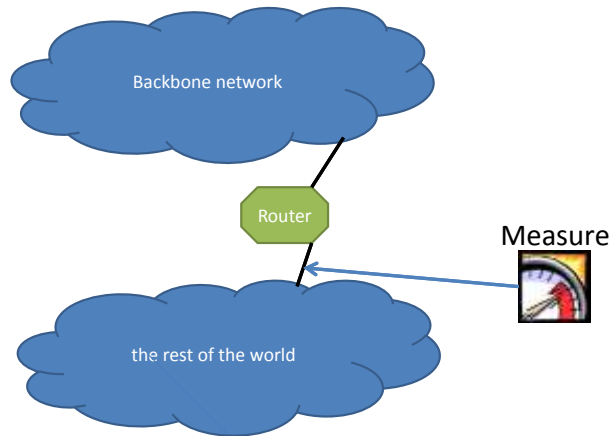
### Analysis of malicious backbone traffic

- Looking for attacks on a backbone network
  - 10 Gbps (=fast!)
  - Problems:
    - speed of network link
    - amount of data
    - routing
    - user privacy – anonymize data (key feature!)

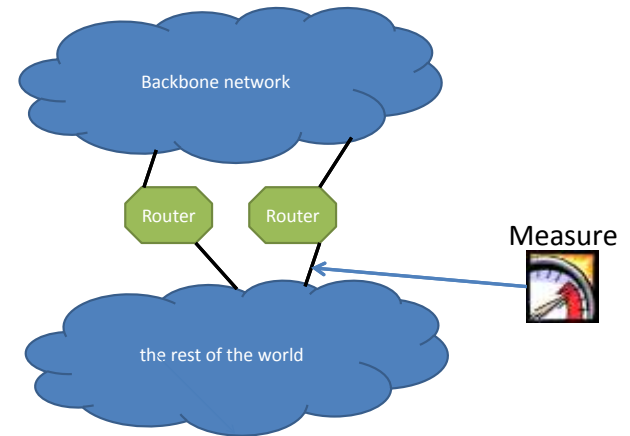




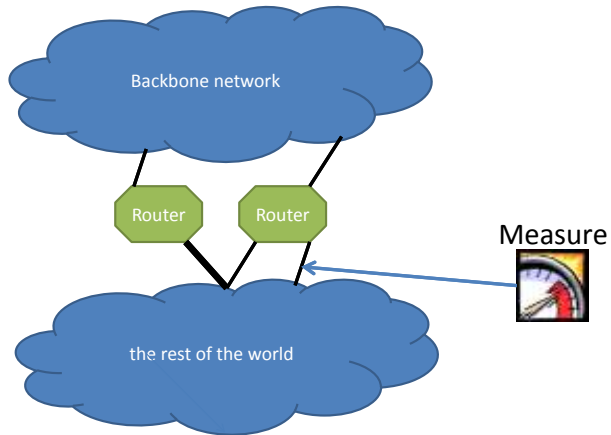
### Measurement Setup (simplified)



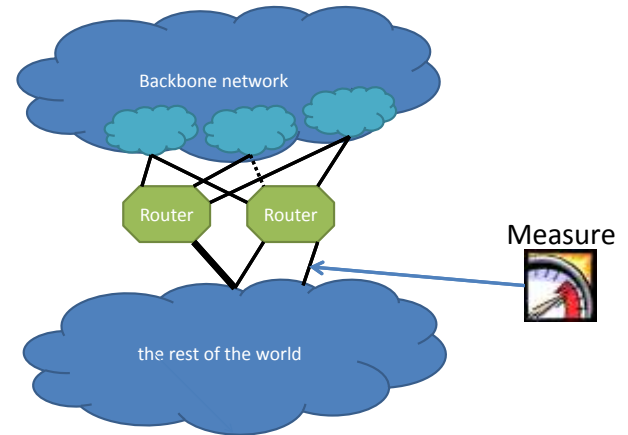
### Measurement Setup (simplified)



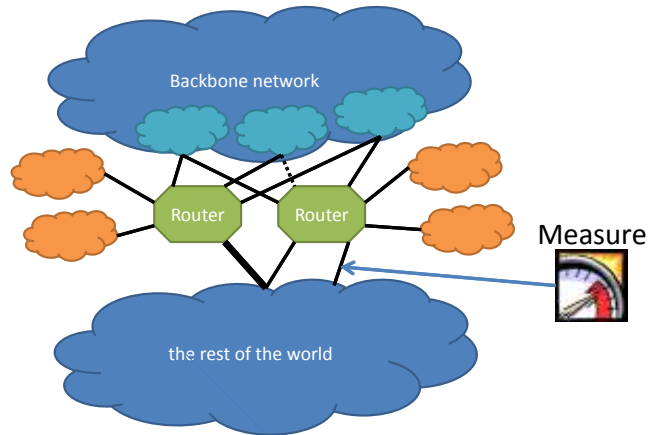
## Measurement Setup (simplified)



## Measurement Setup (simplified)

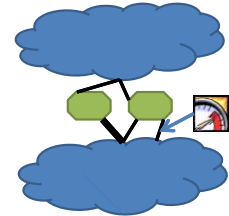


## Measurement Setup (simplified)

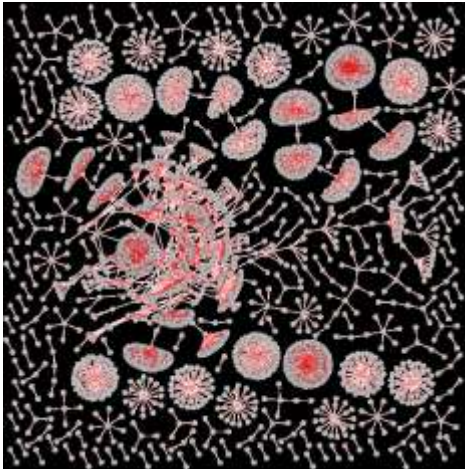


## Statistics

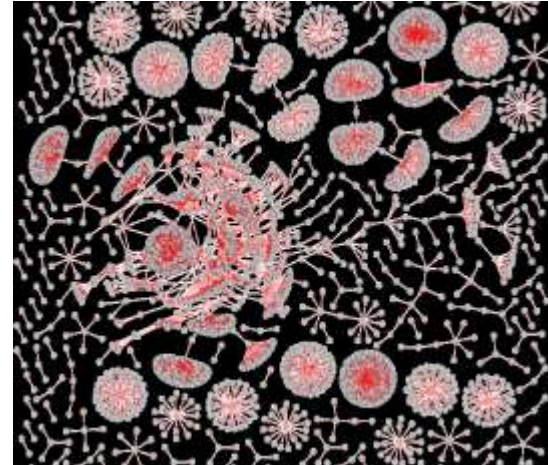
- 23,600 **inside hosts** initiating communication with 18,780,894 on the outside.
- 24,587,096 **outside hosts** trying to reach (scan) 970,149 inside hosts.



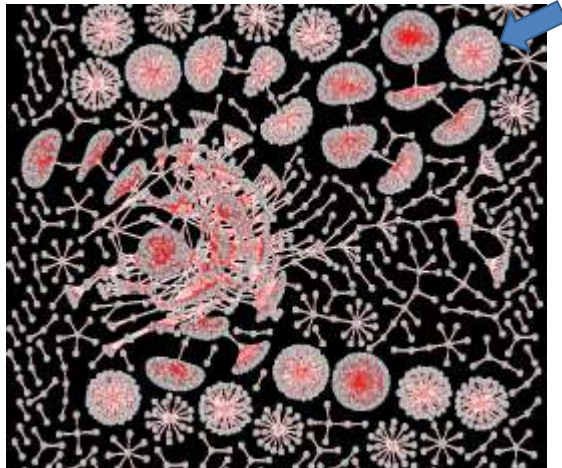
Analysis of backbone data



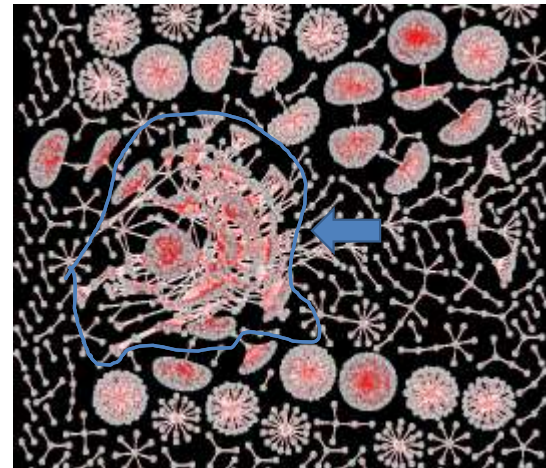
Analysis of backbone data



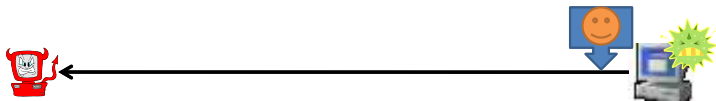
Analysis of backbone data



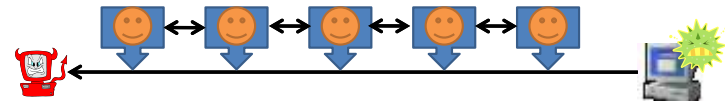
Analysis of backbone data



## Timing Behavior of Malicious Hosts

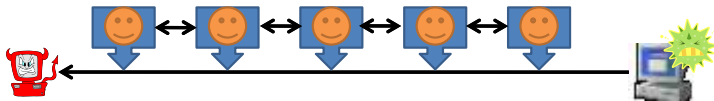


## Timing Behavior of Malicious Hosts



## Timing Behavior of Malicious Hosts

Simple refresh: once every 43min (once every 30 min)



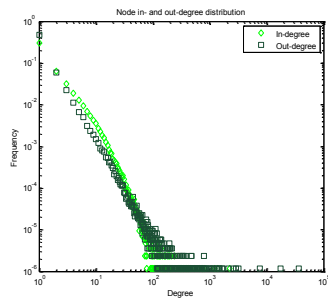
## Timing Behavior of Malicious Hosts

Exponential backoff: 111s, 222s, 333s, 666s, 1332s, 2664s

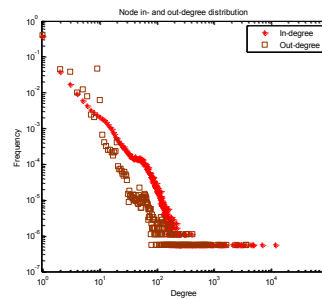


## Identifying **SPAM** from data traffic

Legitimate email (Ham)



Unsolicited email (Spam)



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

- a Network of Excellence (2010-2014)
- To work towards solutions and collaborate
  - At a European level
    - Poli. di Milano (IT)
    - Vrije Universiteit (NL)
    - Institute Eurecom (FR)
    - IPP (Bulgaria)
    - TU Vienna (Austria)
    - Chalmers U (Sweden)
    - UEKAE (Turkey)
    - FORTH – ICS (Greece)
  - and with international colleagues around the world

<http://www.syssec-project.eu/>



## Links

- *SVT Documentary oct-2010:*
  - *Att hacka en stormakt* (<http://goo.gl/1Zrd>)
- *Symantec oct-2010:*
  - *W32.Stuxnet Dossier* (<http://goo.gl/pP7S>)
- *Uppdrag granskning oct-2010:*
  - *Kapade nätverk* (<http://svt.se/granskning>)
  - *SysSec*: <http://www.syssec-project.eu/>