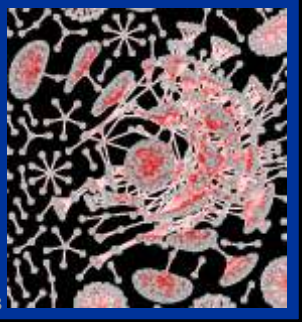
CHALMERS

Mitigating Cyber Attacks

Magnus Almgren
Göteborg, 2010-10-19



Postdoc, finansierad av MSB

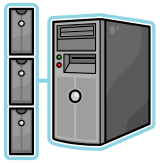
15—20 years ago …

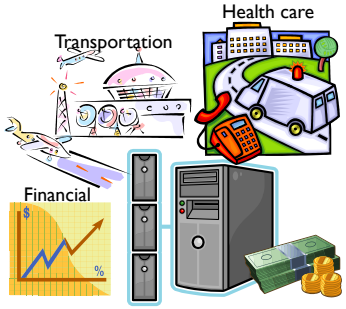
- Internet starting to reach a wider audience
  - most people did not have emails
  - computer security – an afterthought
- The typical hacker, often portrayed as
  - teenager,
  - attack a ”chess game”
  - **goal:** some esoteric fame …
- And today ?

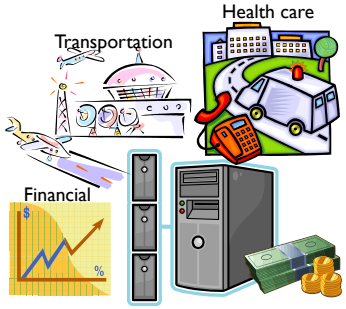
SVT Documentary oct-10, 2010: Att hacka en stormakt (http://goo.gl/1Zrd)

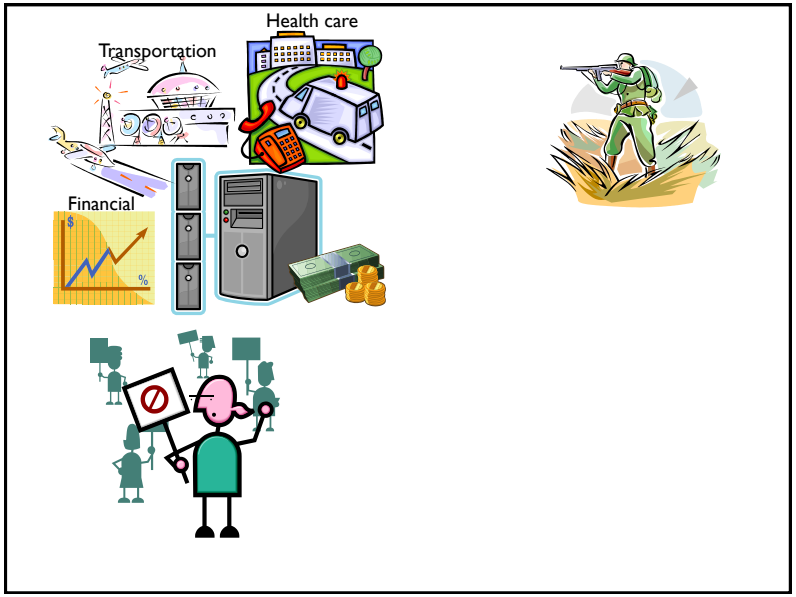
Outline

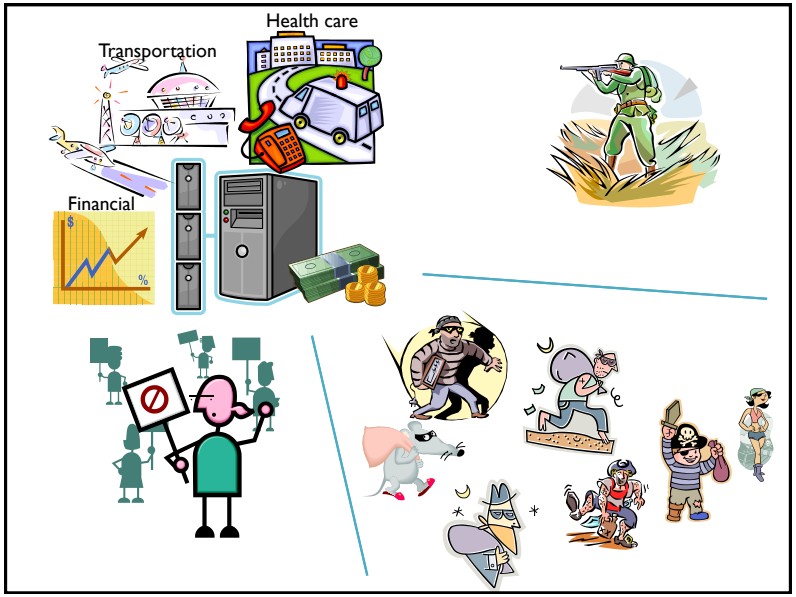
- Status today
- Monitoring traffic
- Research Activities
  - Reasoning with alerts from several sensors
  - Monitoring backbone traffic
- European network: SysSec




Health care
Transportation
Financial

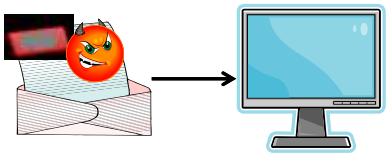

Health care
Transportation
Financial

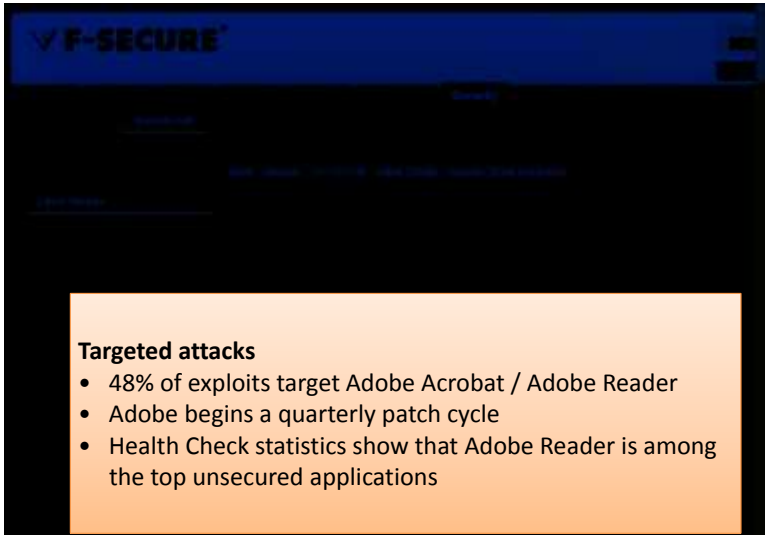

Health care
Transportation
Financial


Health care
Transportation
Financial

Malicious Code

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





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

Dangerous People (!!!)

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

The New York Times

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.

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

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.

Topics

nikko hypponen, paul ducklin, accidents and disasters, air disasters, computer security, computer technology, science and technology, spyware and adware, technology,

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 JK 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 Ducklin, 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, Ducklin 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 travelers 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.

WIRED

THREAT LEVEL

PRIVACY, CRIME AND SECURITY ONLINE

Hacker Disables More Than 100 Cars Remotely

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.

"We initially dismissed 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

Technology

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

Join the conversation

Top Technology articles

Latest Comment

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 technology network", the spokesman said.

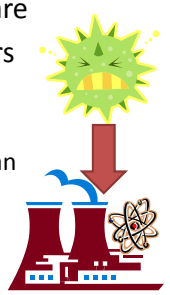

Europe

QUALITYHUNTERS

127

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.

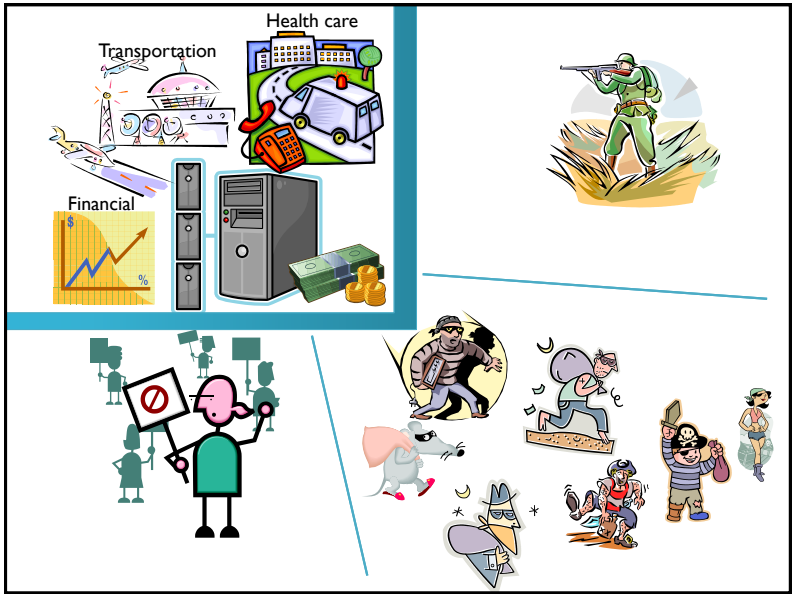
now blueprint to create malware targeting PLCs

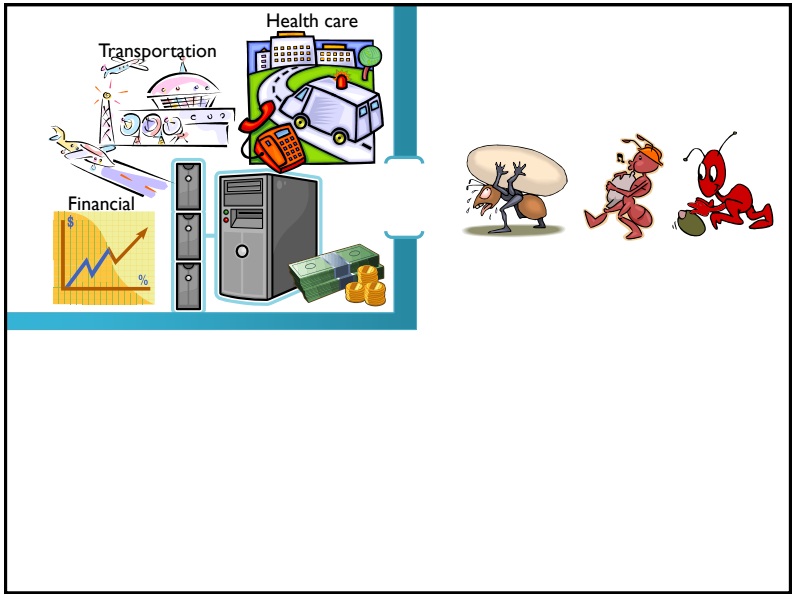
- Compare this with the *Loveletter* virus (2000)
  - 2003/11 there existed 82 different variants of Loveletter.
  - It is claimed that more than 5,000 attacks are carried out every day.

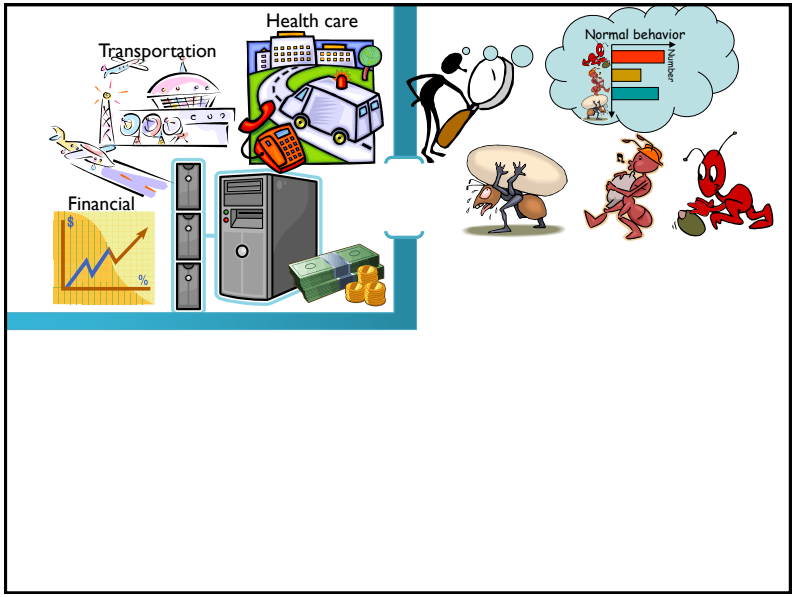
Status today

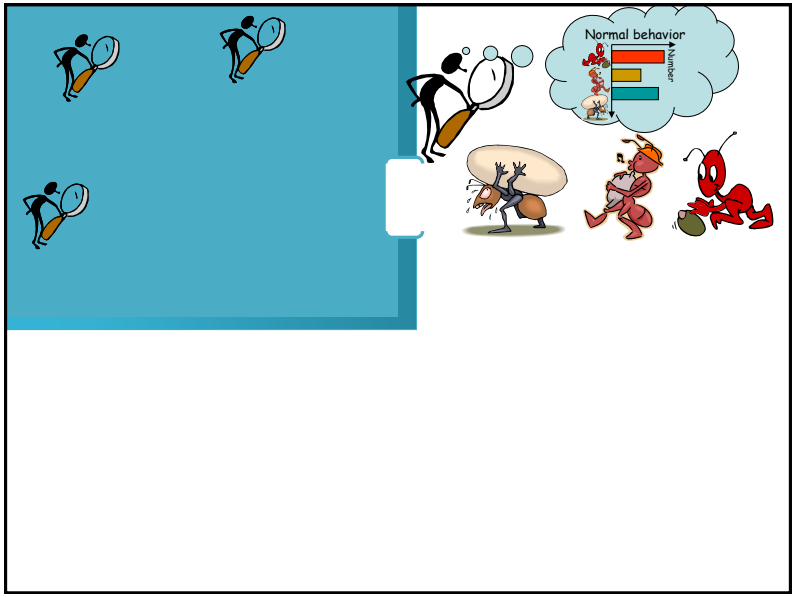
Monitoring traffic*: *Intrusion Detection Systems

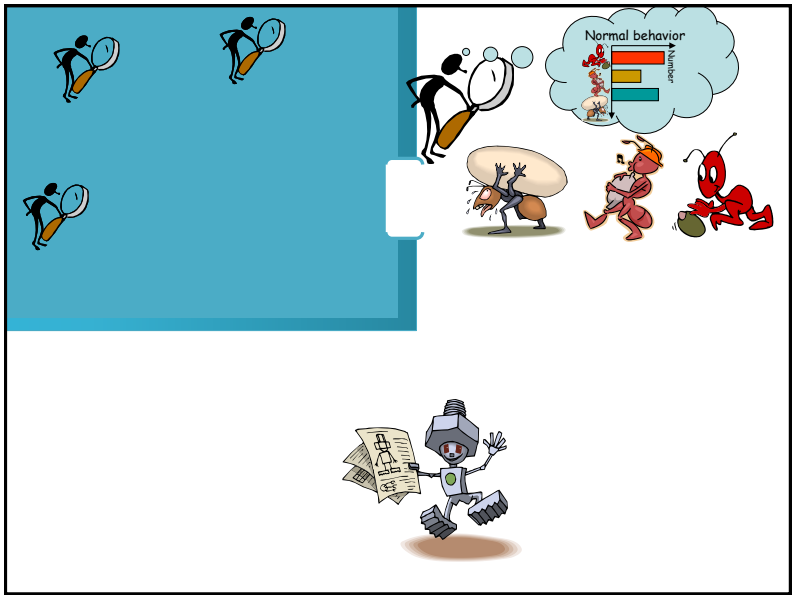
Research Activities

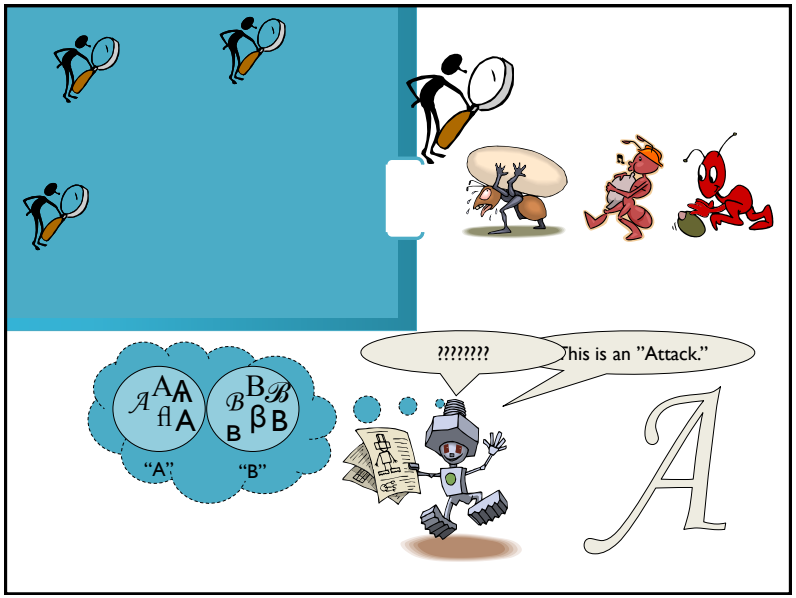

Health care
Transportation
Financial


Health care
Transportation
Financial


Health care
Transportation
Financial
Normal behavior
Number


Normal behavior
Number


Normal behavior
Number

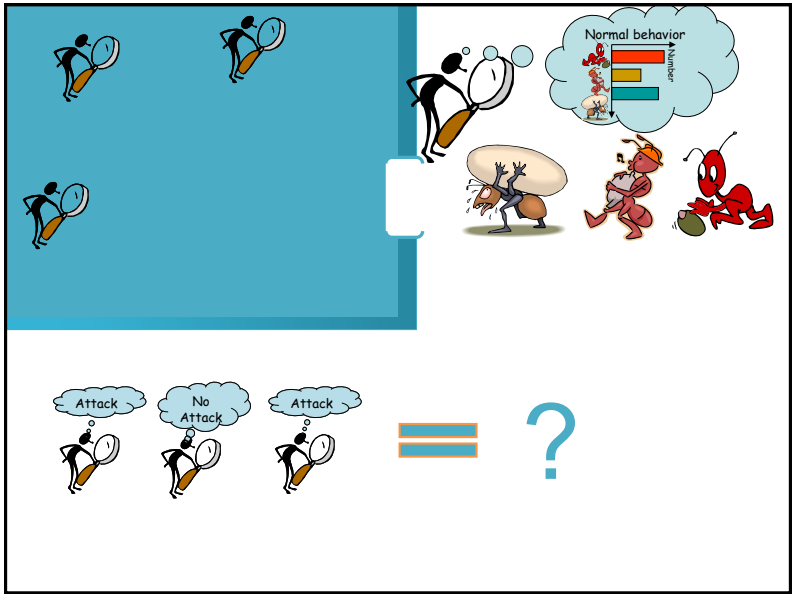

????????
This is an "Attack."
"A"
"B"

Status today

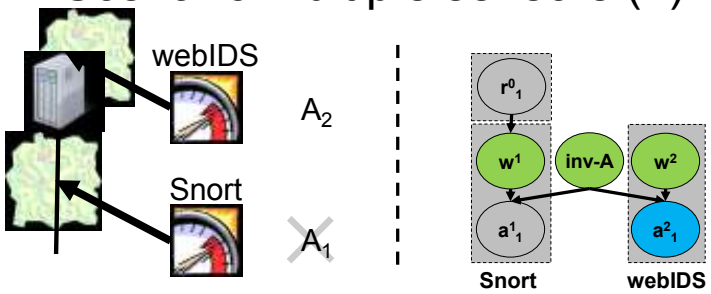
Monitoring traffic

Research Activities:

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

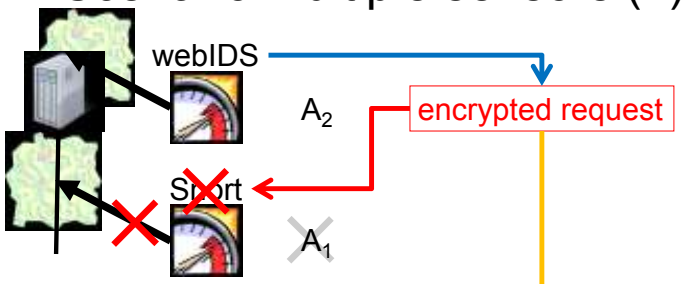


Scenario multiple sensors (1)



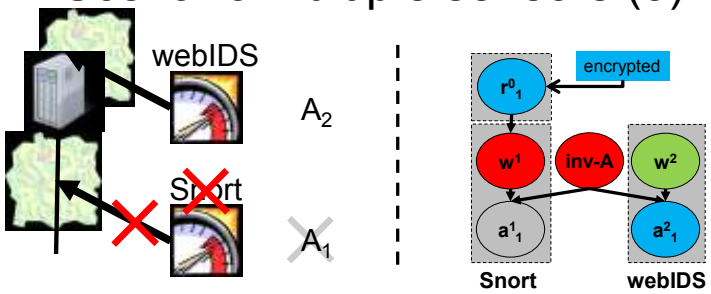
- Normal phf access (no attack)
  - P(inv-A | …) = 0.20 = ***don't investigate***

Scenario multiple sensors (2)



- Normal phf access (no attack)
  - P(inv-A | …) = 0.20 = ***don't investigate***

Scenario multiple sensors (3)

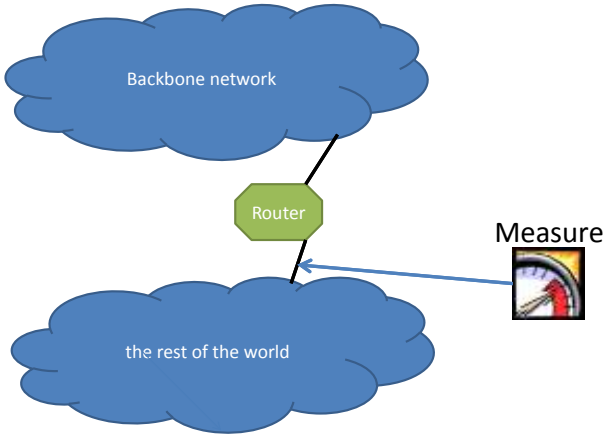


- Normal phf access (no attack)
  - P(inv-A | …) = 0.20 = ***don't investigate***
- ***Snort sensor defunct, this may be an attack!***
  - P(inv-A | …) = 0.54 = ***investigate***
  - P(w^1 | …) = 0.01 = ***sensor broken***

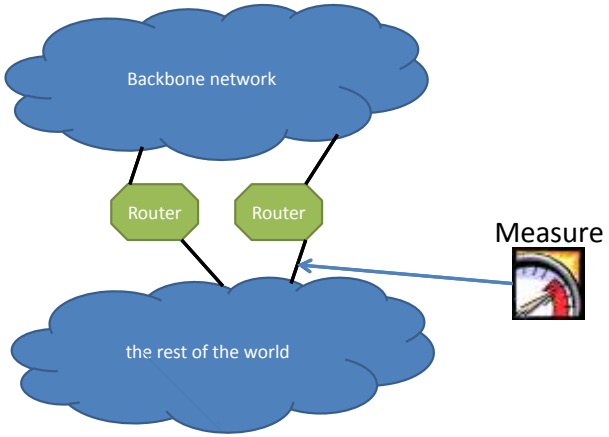
Analysis of malicious backbone traffic

- 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!)

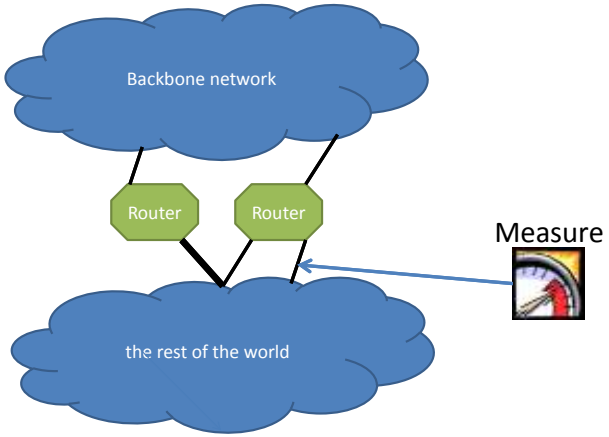
Measurement Setup (simplified)



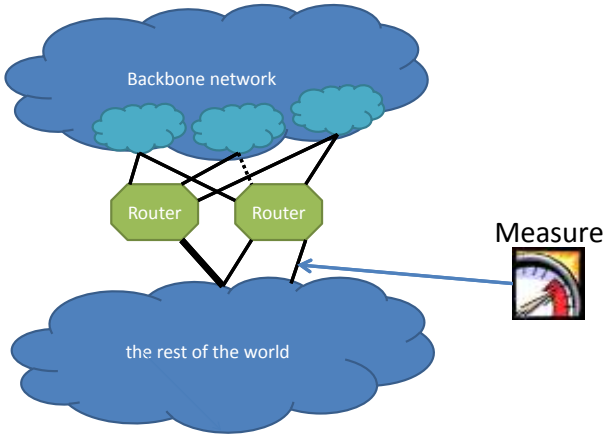
Measurement Setup (simplified)



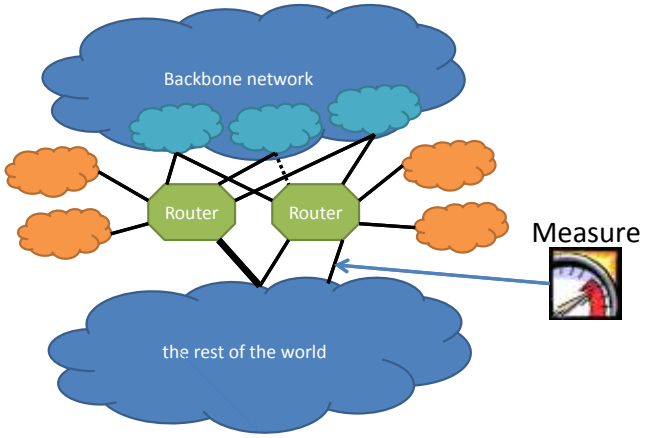
Measurement Setup (simplified)



Measurement Setup (simplified)

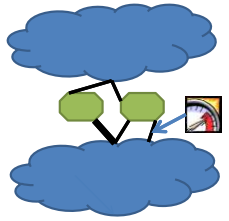


Measurement Setup (simplified)



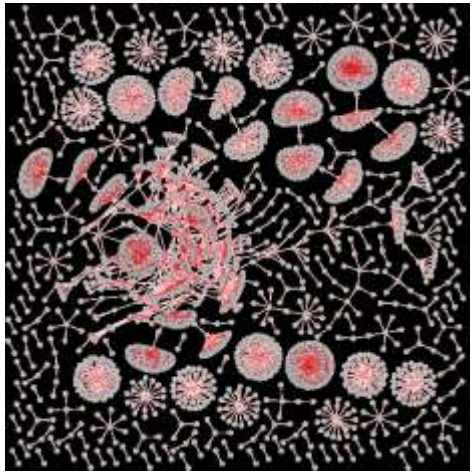
Statistics

- 23,600 ***inside hosts*** initiating communication with 18,780,894 on the outside.

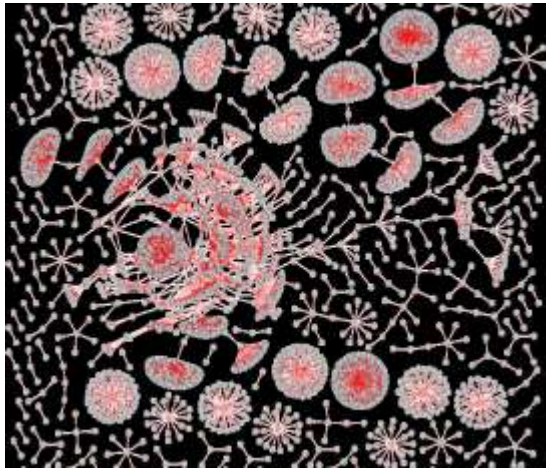


- 24,587,096 ***outside hosts*** trying to reach (scan) 970,149 inside hosts.

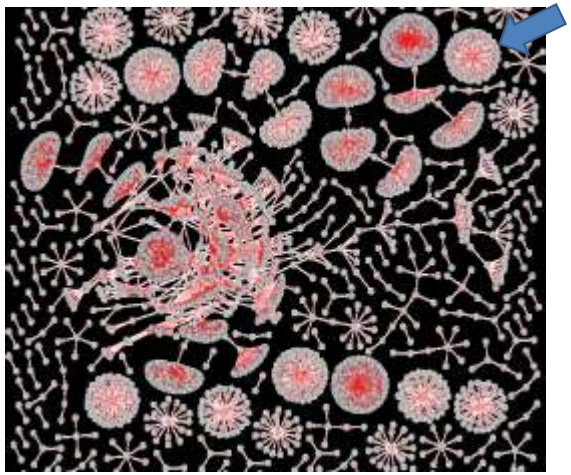
Analysis of backbone data



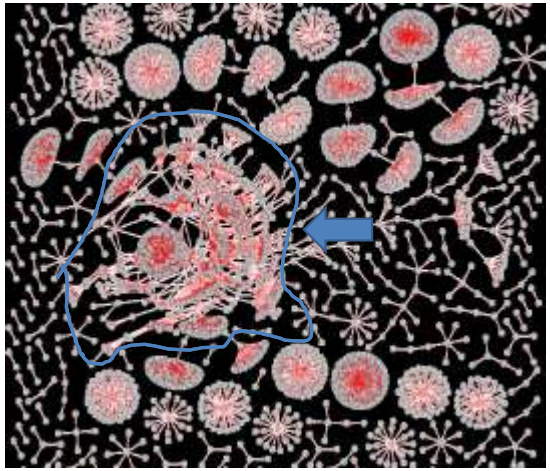
Analysis of backbone data



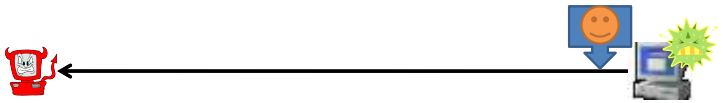
Analysis of backbone data



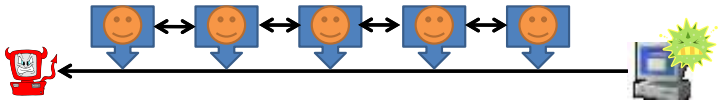
Analysis of backbone data



Timing Behavior of Malicious Hosts

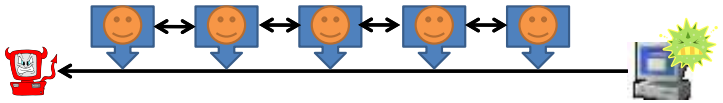


Timing Behavior of Malicious Hosts



Timing Behavior of Malicious Hosts

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

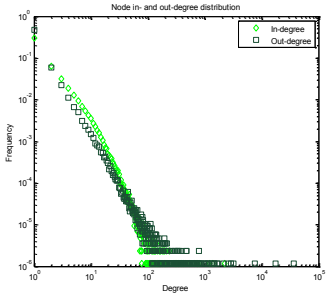


Timing Behavior of Malicious Hosts

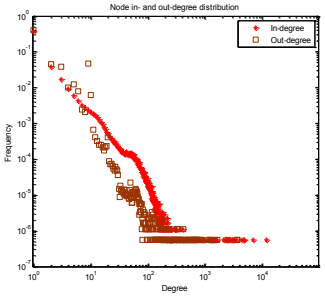
Exponential backoff: 111s, 222s, 333s, 666s, 1332s, 2664s

Identifying SPAM from data traffic

Legitimate email (Ham)



Unsolicited email (Spam)



syssec

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 Uniivesriteit (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/*