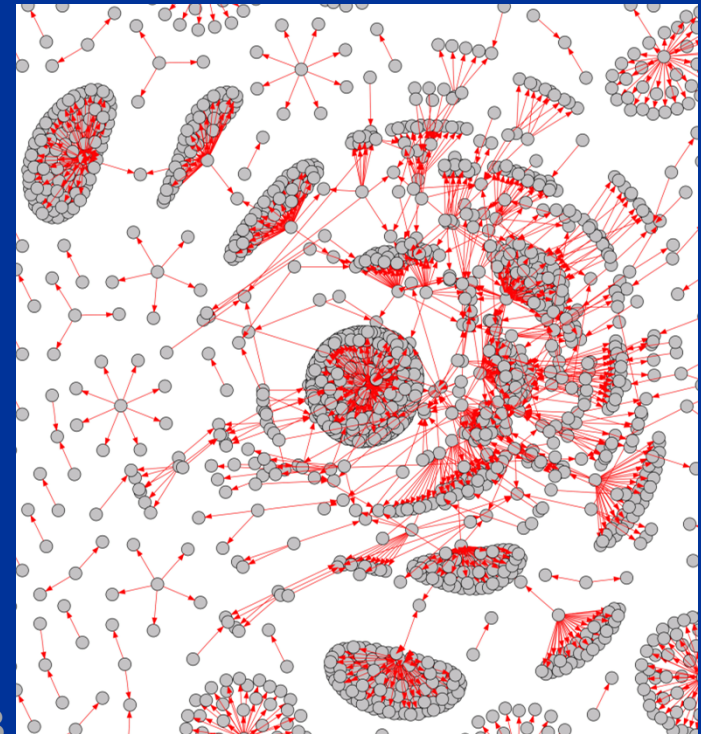


# Mitigating Cyber Attacks

Magnus Almgren

Göteborg, 2010-11-17



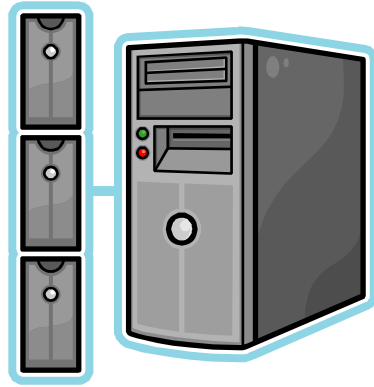
# 15—20 years ago ...

- 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 ?



# Outline

- Status today
  - News clips (if you do not believe in me ...)
- Monitoring traffic
  - Intrusion Detection Systems
- Research Activities
  - Reasoning with alerts from several sensors
  - Monitoring backbone traffic
- European network: SysSec





Health care



Transportation

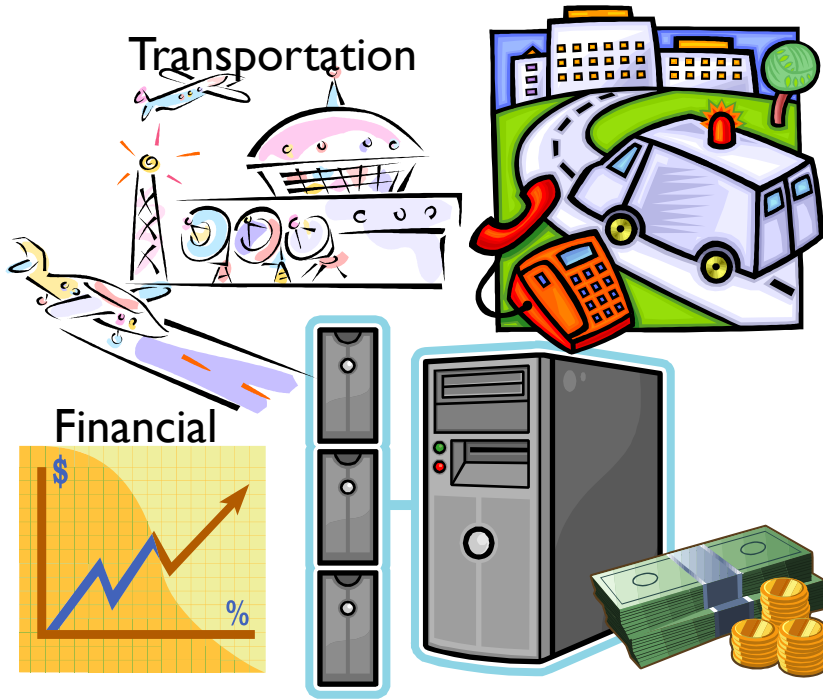


Financial



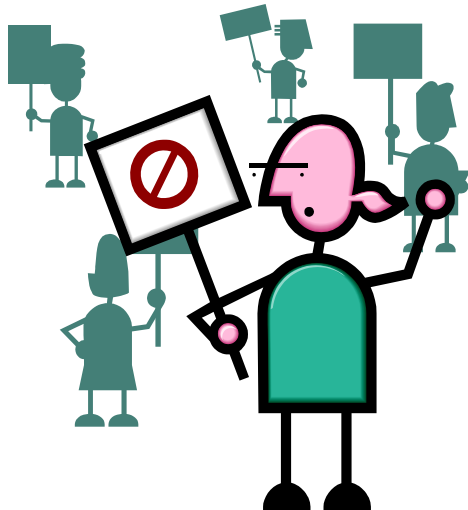
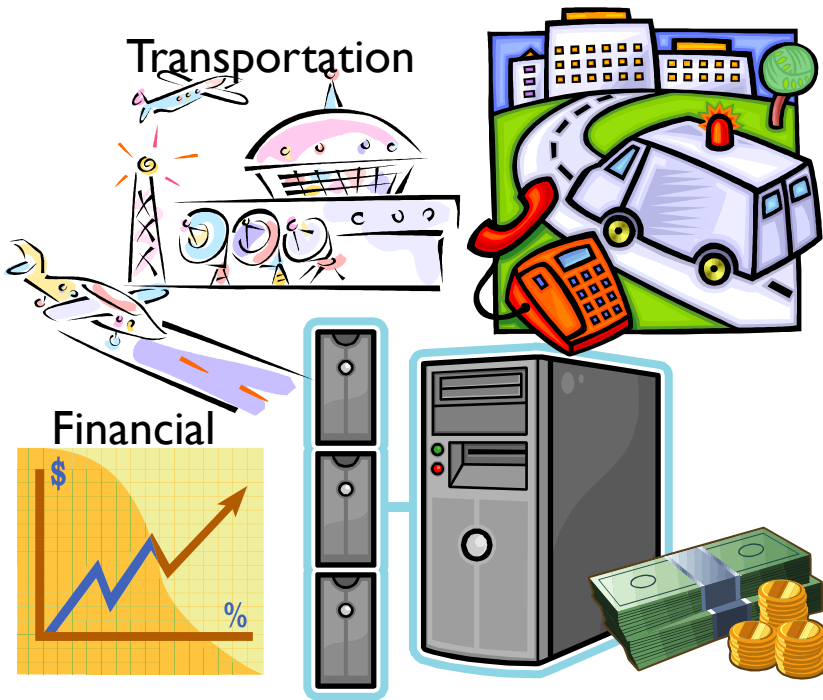
Health care

Transportation



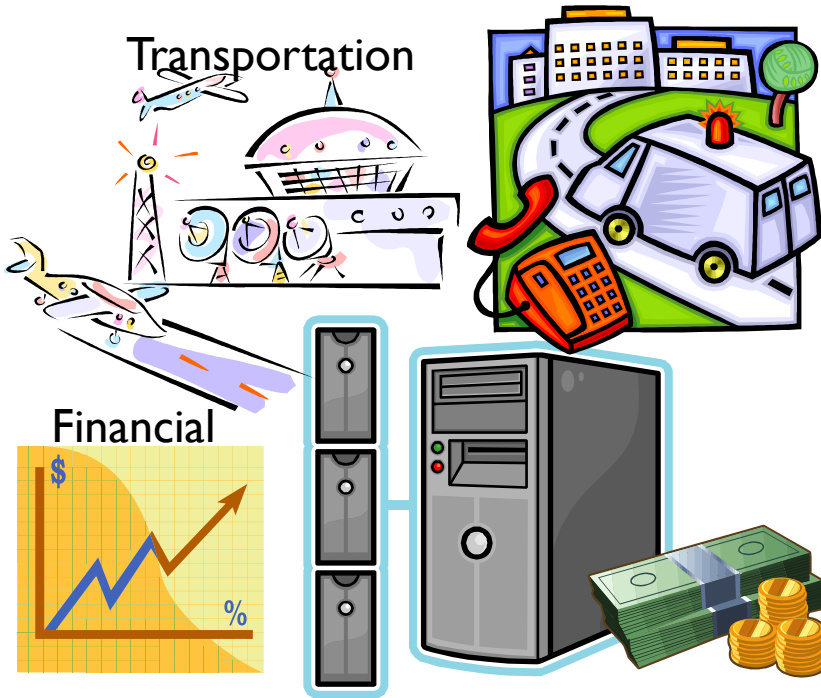
Health care

Transportation



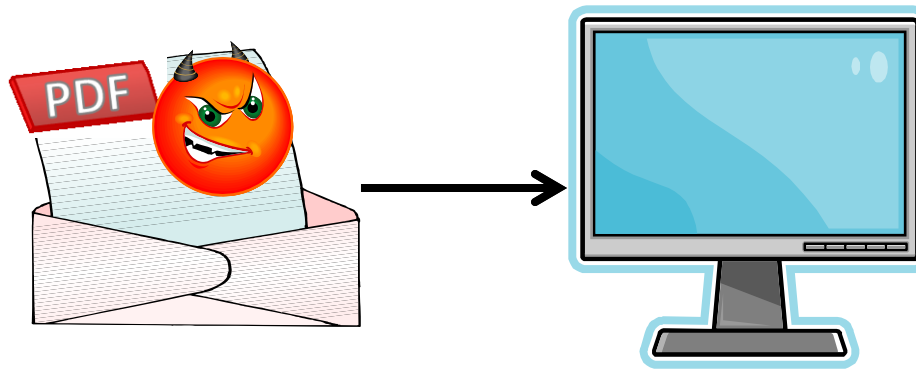
Health care

Transportation



# Malicious Code

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



## Security Lab

### Latest Threats

[Home](#) » [Security](#) » [Security Lab](#) » [Latest Threats](#) » [Security Threat Summaries](#) »

[2009 Q2](#) | [2009 Q1](#)

[2008 Q4](#) | [2008 Q3](#) | [2008 Q2](#) | [2008 Q1](#) | [2007 H2](#) | [2007 H1](#)

[2006 H2](#) | [2006 H1](#) | [2005 H2](#) | [2005 H1](#) | [2004](#) | [2003](#) | [2002](#)

## 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

# Dangerous People (!!!)



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



**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 that appears next to any article. Visit [www.nytreprints.com](http://www.nytreprints.com) for samples and additional information. [Order a reprint of this article now.](#)

PRINTER-FRIENDLY FORMAT  
SPONSORED BY



April 19, 2010

# 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.

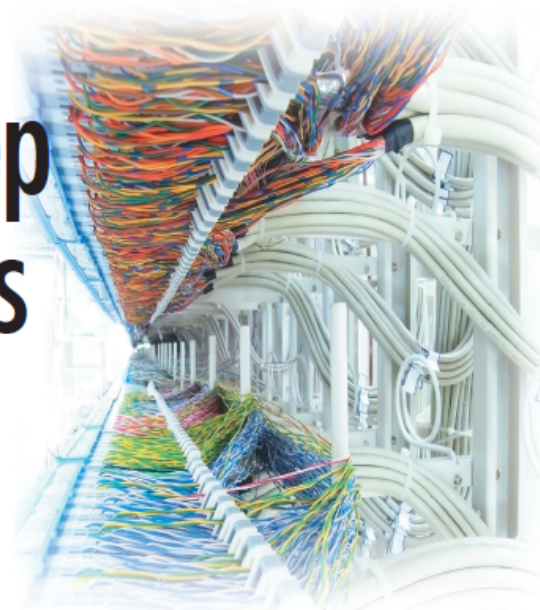
The program, code named Gaia for the Greek goddess of the earth, was attacked in a lightning raid taking less than two days last December, the person said. Described publicly only once at a technical conference four years ago, the software is intended to enable users and employees to sign in with their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



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.**

**I**mplantable medical devices—such as insulin pumps, cardiac pacemakers, and cardiac defibrillators—have become increasingly popular since being introduced about 50 years ago. In the US alone, 2.6 million people

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

All this convenience may come with unanticipated risks: the possibility that hackers could break into IMDs' communications 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.

"Hacking a medical device—espe-

# Malware link to air crash inconclusive

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

6 retweet

f Like

## 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

[mikko hypponen](#), [paul ducklin](#), [accidents and disasters](#), [air disasters](#), [computer security](#), [computer technology](#), [science and technology](#), [spyware and adware](#), [technology](#), [transportation](#)

**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.

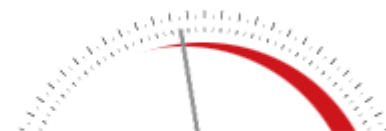
Paul Ducklin, Sophos' head of technology for the Asia-Pacific region, told ZDNet Asia in an e-mail interview, this is possibly the first case of malware being mentioned in relation to a plane crash. However, to what extent the infection contributed to the crash is "not yet clear" as more details of the 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 tie malware and, by association, cyberwarfare into the area of civilian aviation sounds as though it is worth worrying about," he said.

# THREAT LEVEL


PRIVACY, CRIME AND SECURITY ONLINE



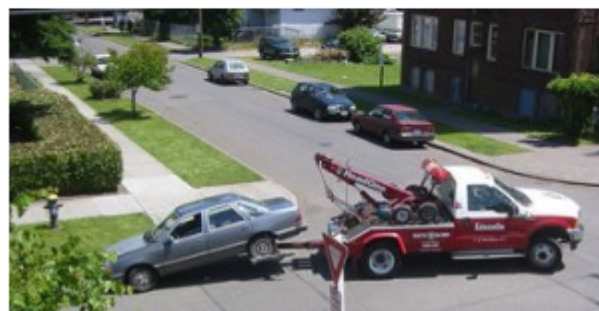
[PREVIOUS POST](#)

[NEXT POST](#)

## 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.

"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 install a small black box under vehicle dashboards that responds to commands issued through a central

## Technology

News Biz-Tech Security Enterprise Sci-Tech Blogs Digital Life Compare & Save

You are here: Home » Technology » Security » Article

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

Asher Moses  
October 1, 2009

Comments 21

### Join the conversation

You're the only person reading this now. [Tell your friends](#)

21 comments

[Comment on Twitter](#)

[Read tweets](#)

### Top Technology articles

1. US admires Australian botnet plan
2. Social networking sites a boon for criminals intent on fraud
3. WikiLeaks fears downgraded
4. iPad becomes big target for small rivals
5. Pentagon gets set for WikiLeaks Iraq fallout

+ [More Technology articles](#)

### Latest Comment

*"An update for  
"Realist" totally*

### Ads by Google

[Trojan Remover Download](#) [www.pctools.com](http://www.pctools.com)

Free Trojan Scan. Winner of the Best Anti-Spyware. Rated 5 Stars.

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.





FOLLOW THE

QUALITYHUNTERS

4 People/61 Days/Travelling the World/In Search of Quality



FOLLOW NO

## Estonia Computers Blitzed, Possibly by the Russians

By STEVEN LEE MYERS

Published: May 19, 2007

MOSCOW, May 18 — The computer attacks, apparently originating in [Russia](#), first hit the Web site of [Estonia](#)'s prime minister on April 27, the day the country was mired in protest and violence. The president's site went down, too, and soon so did those of several departments in a wired country that touts its paperless government and likes to call itself E-stonia.

Then the attacks, coming in waves, began to strike newspapers and television stations, then schools and finally banks, raising fears that what was initially a nuisance could have economic consequences.

The attacks have peaked and tapered off since then, but they have not ended, prompting officials there to declare Estonia the first country to fall victim to a virtual war.

"If you have a missile attack against, let's say, an airport, it is an act of war," a spokesman for the Estonian Defense Ministry, Madis Mikko, said Friday in a telephone interview. "If



TWITTER



SIGN IN TO E-MAIL OR SAVE THIS



PRINT



REPRINTS



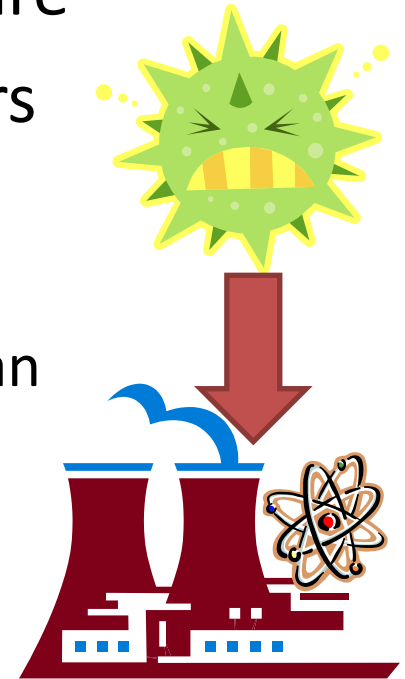
SHARE



127  
HOURS  
NOVEMBER 5

# New Era 2010: Stuxnet

- Advanced Malware
  - target specifically **P**rogrammable **L**ogic **C**ontrollers:  
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)



# 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.

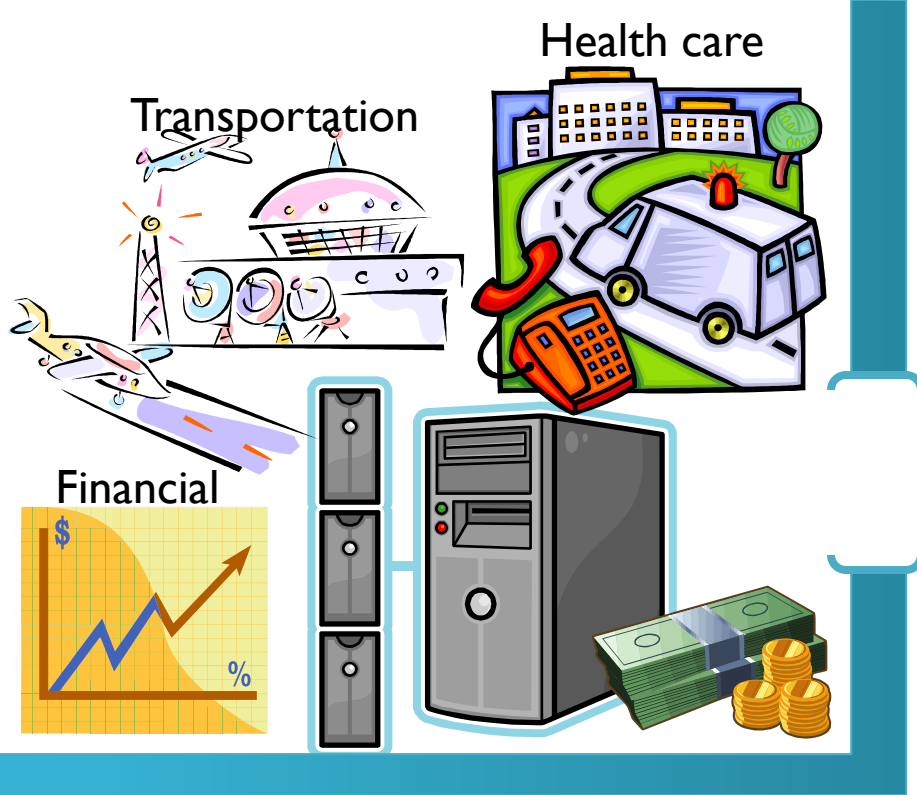
Status today

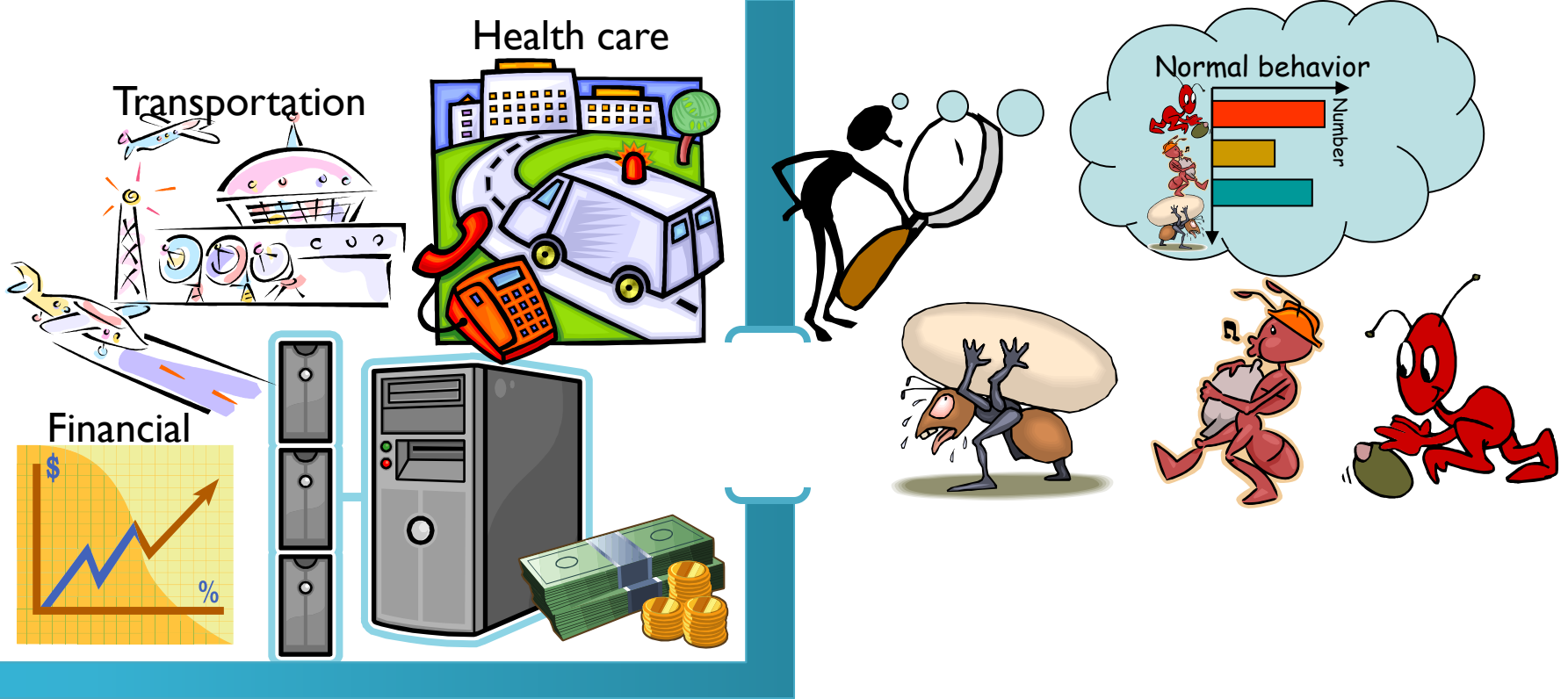
***Monitoring traffic: Intrusion Detection Systems***

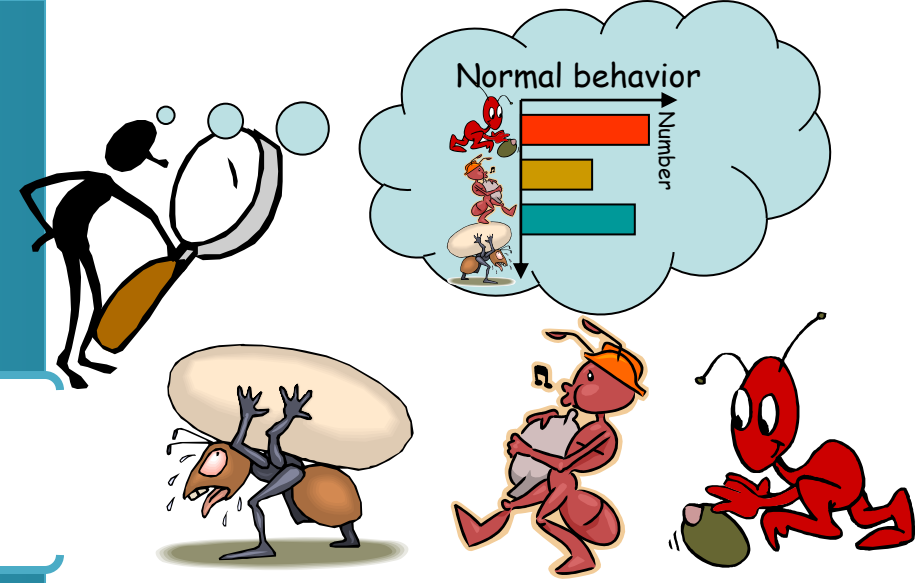
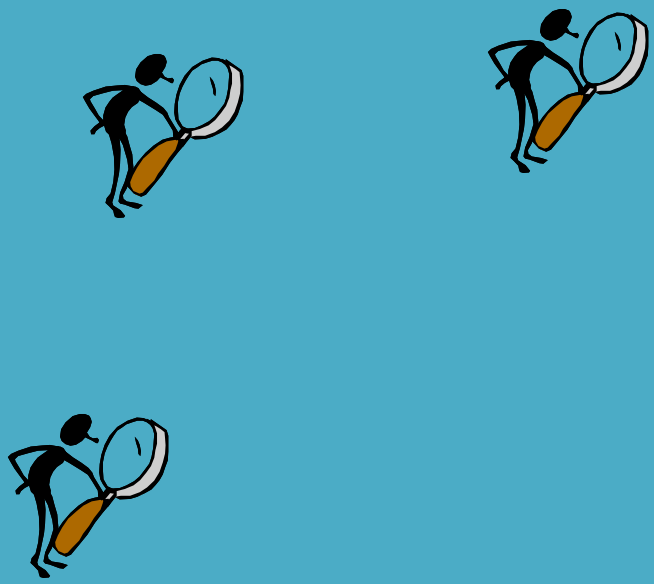
Research Activities

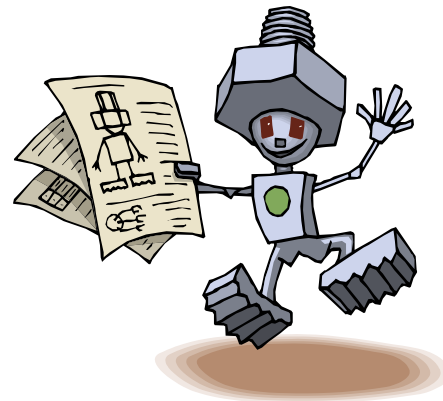
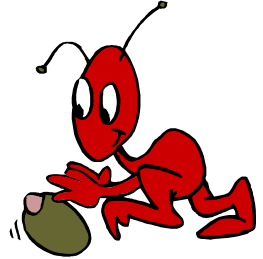
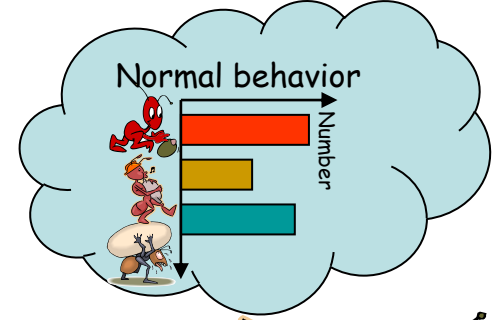
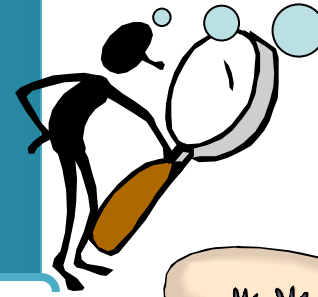
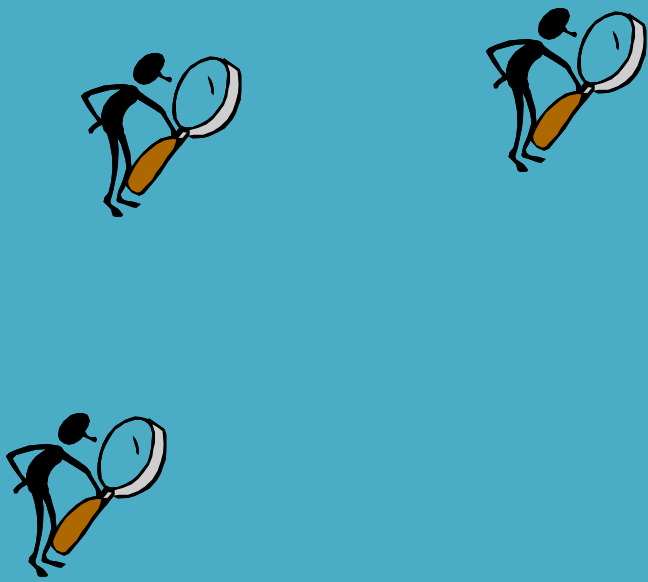


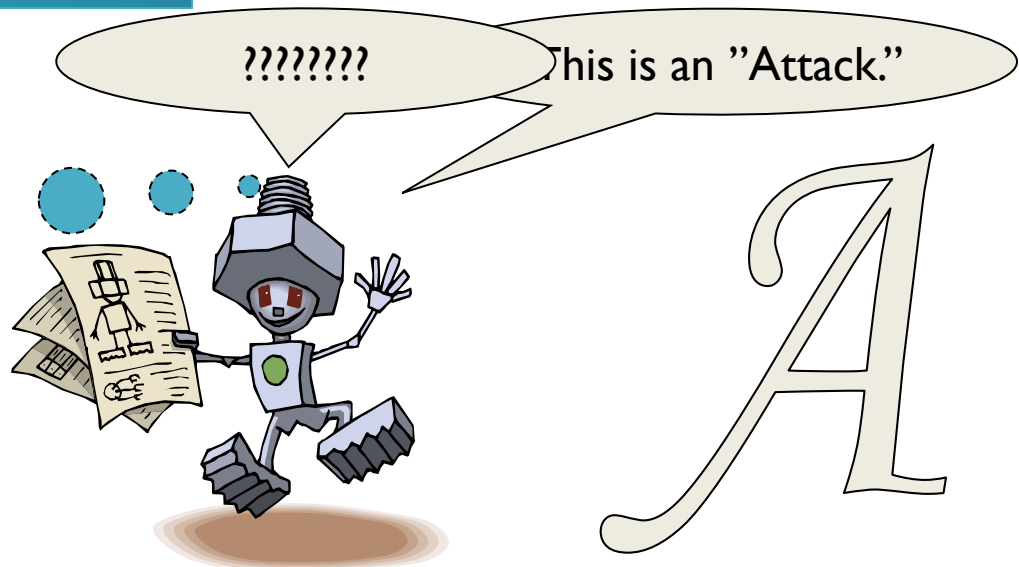
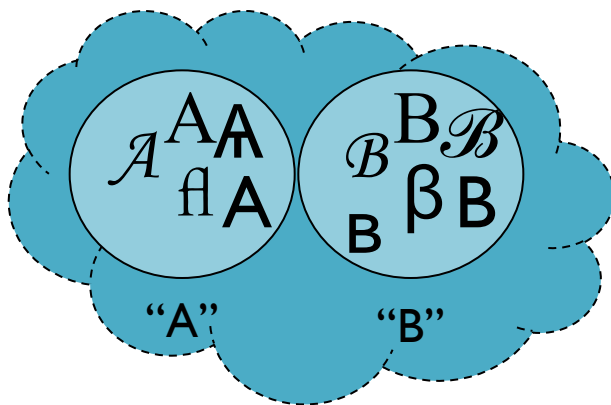
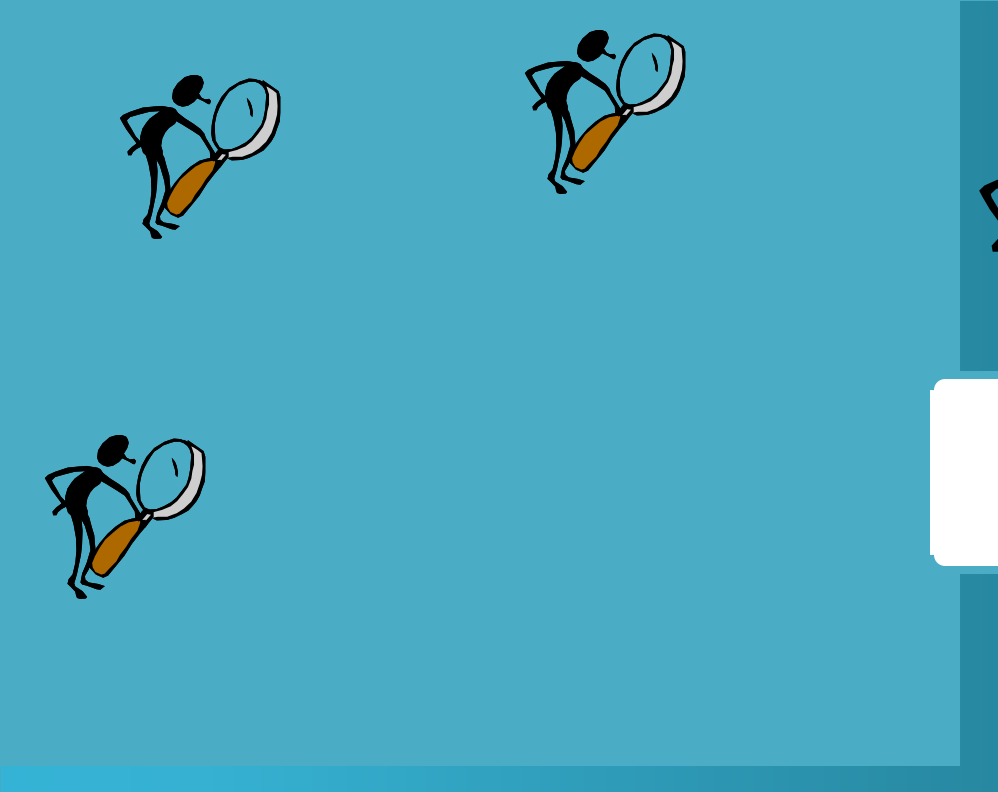












A

## Snorby Dashboard



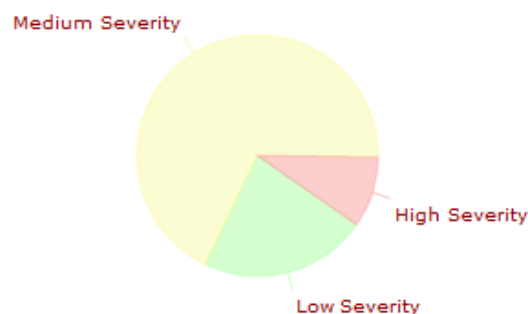
## Severity Statistics

High Severity	22 Events
Medium Severity	158 Events
Low Severity	52 Events

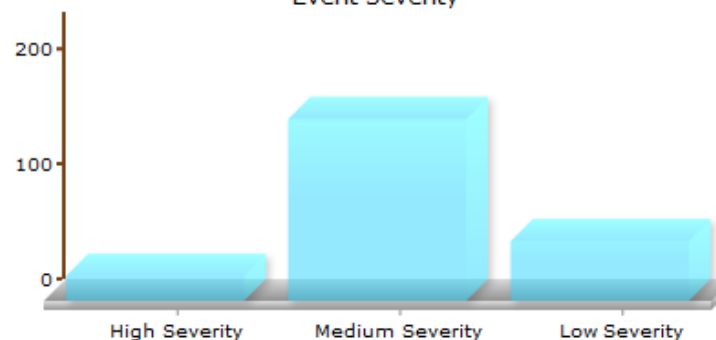
## Event Statistics

Total Event Count:	232 Events
Unique Events Types	74 Unique Event Types
Unique Addresses	8 Unique Addresses

Event Severity



Event Severity



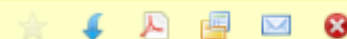
## Sensor Information:

Sensor	Hostname	Interface	Encoding	Last Event	Event Percentage
1	129.16.192.122	en1	hex	110	8.62%
2	10.0.1.5	en1	hex	215	91.38%

## Event Category Information:

Event Category	Event Count For Category	Event Percentage
web-application-attack	22 Events	9.48%
Unclassified	50 Events	21.55%
misc-attack	34 Events	14.66%
bad-unknown	7 Events	3.02%
attempted-recon	65 Events	28.02%
web-application-activity	52 Events	22.41%
misc-activity	2 Events	0.86%

## WEB-CGI faqmanager.cgi arbitrary file access attempt



Relevance info:

EMA-5: 39.0

EMA-10: 39.0

EMA-20: 39.0

Payload:

Show Ascii - Show Ascii Hex

```
00000000: 47 45 54 20 2f 63 67 69 2d 62 69 6e 2f 66 61 71 6d 61 6e 61 GET /cgi-bin/faqmana
00000014: 67 65 72 2e 63 67 69 3f 74 6f 63 3d 2f 65 74 63 2f 70 61 73 ger.cgi?to c=/etc/pas
00000028: 73 77 64 25 30 30 20 48 54 54 50 2f 31 2e 31 0d 0a 43 6f 6e swd%00 HTTP/1.1. Con
0000003C: 6e 65 63 74 69 6f 6e 3a 20 4b 65 65 70 2d 41 6c 69 76 65 0d nection: Keep-Alive.
00000050: 0a 48 6f 73 74 3a 20 31 30 2e 30 2e 31 2e 35 0d 0a 50 72 61 .Host: 10.0.1.5. Pra
00000064: 67 6d 61 3a 20 6e 6f 2d 63 61 63 68 65 0d 0a 55 73 65 72 2d gma: no-cache. User-
00000078: 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 34 2e 30 20 28 Agent: Mozilla/4.0 (
0000008C: 63 6f 6d 70 61 74 69 62 6c 65 3b 20 4d 53 49 45 20 38 2e 30 compatible; MSIE 8.0
000000A0: 3b 20 57 69 6e 64 6f 77 73 20 4e 54 20 35 2e 31 3b 20 54 72 ; Windows NT 5.1; Tr
000000B4: 69 64 65 6e 74 2f 34 2e 30 29 0d 0a 41 63 63 65 70 74 3a 20 ident/4.0) ..Accept:
000000C8: 69 6d 61 67 65 2f 67 69 66 2c 20 69 6d 61 67 65 2f 78 2d 78 image/gif, image/x-x
000000DC: 62 69 74 6d 61 70 2c 20 69 6d 61 67 65 2f 6a 70 65 67 2c 20 bitmap, image/jpeg,
000000F0: 69 6d 61 67 65 2f 70 6a 70 65 67 2c 20 69 6d 61 67 65 2f 70 image/png, image/p
0000104: 6e 67 2c 20 2a 2f 2a 0d 0a 41 63 63 65 70 74 2d 4c 61 6e 67 ng, */*. Accept-Lang
0000118: 75 61 67 65 3a 20 65 6e 0d 0a 41 63 63 65 70 74 2d 43 68 61 uage: en.. Accept-Cha
000012C: 72 73 65 74 3a 20 69 73 6f 2d 38 38 35 39 2d 31 2c 2a 2c 75 rset: iso-8859-1,*;u
0000140: 74 66 2d 38 0d 0a 0d 0a tf-8....
```

S. Port	D. Port	Seq #	Ack	Offset	Reset	Flags	Window	Checksum	Urgent Pointer
2811	80	4148171872	1273569274	5	0	24	16425	23195	0

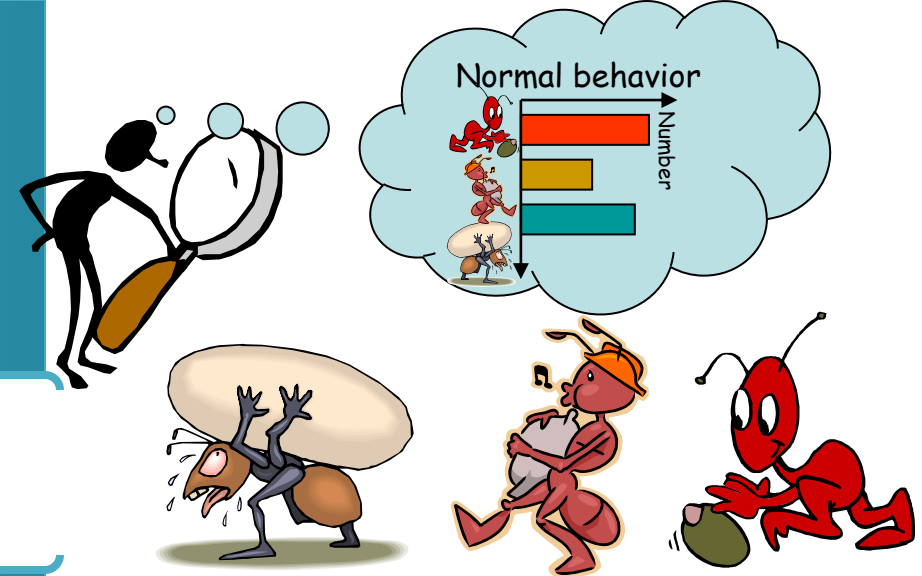
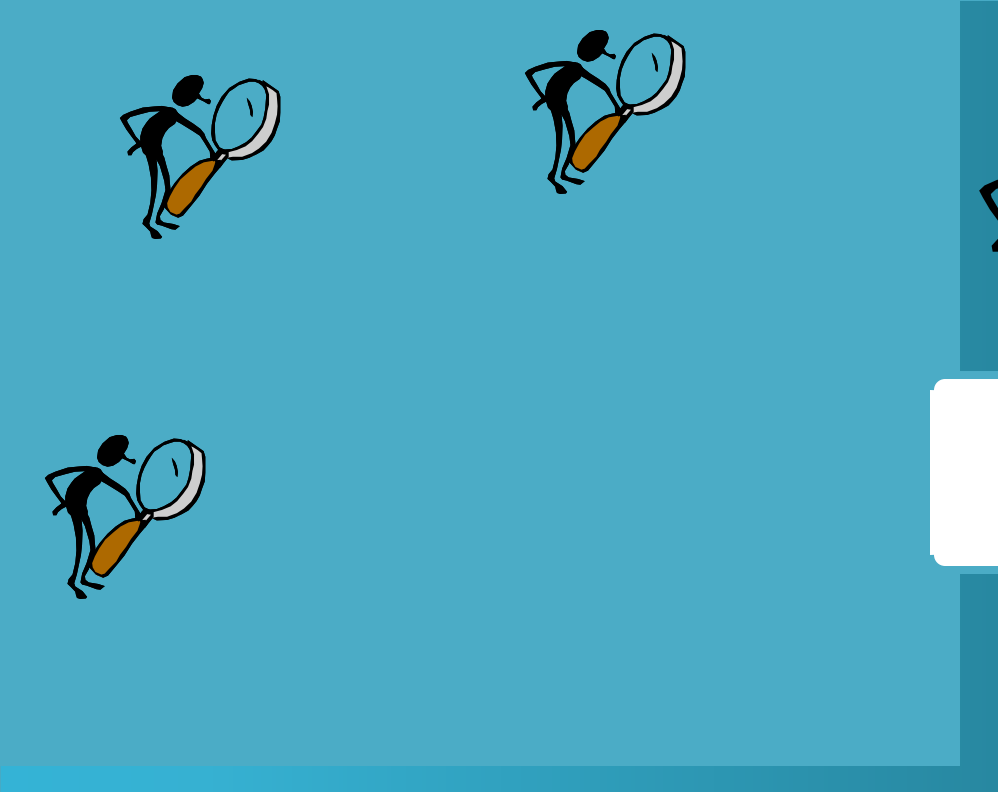


Status today

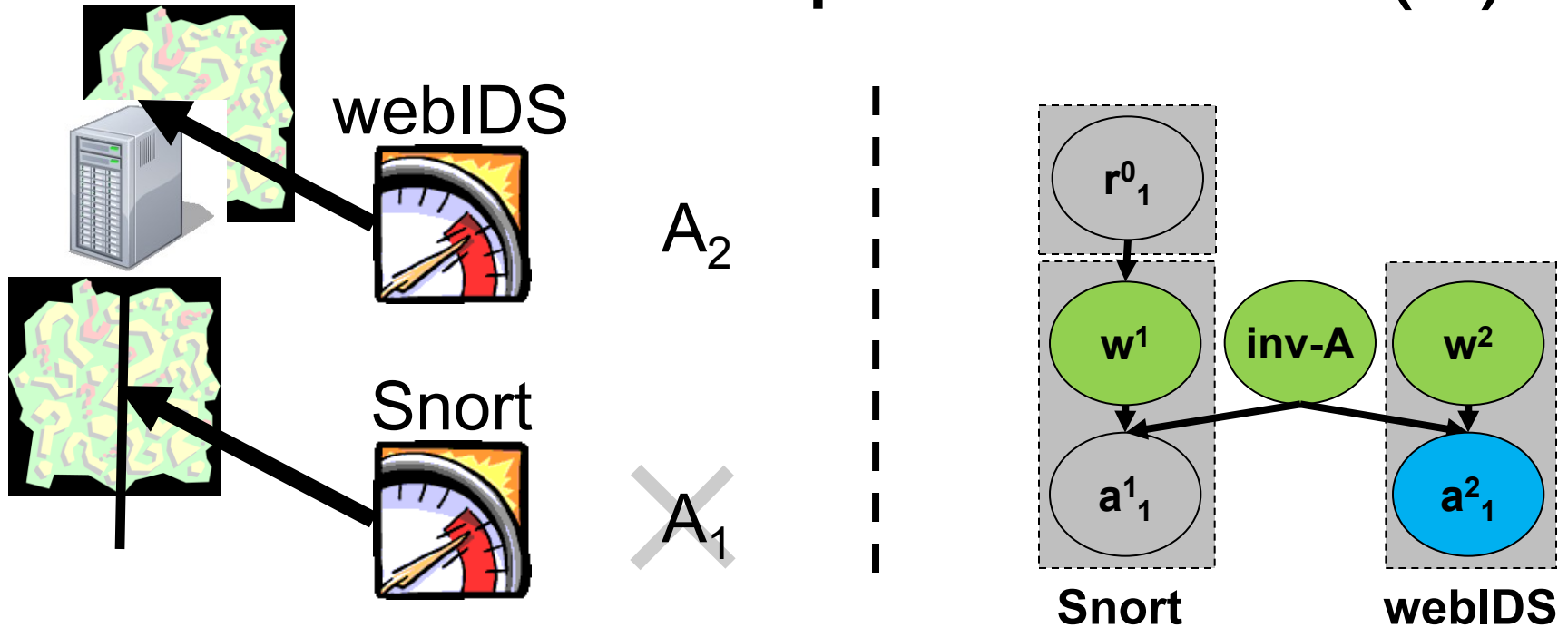
Monitoring traffic

***Research Activities:***

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

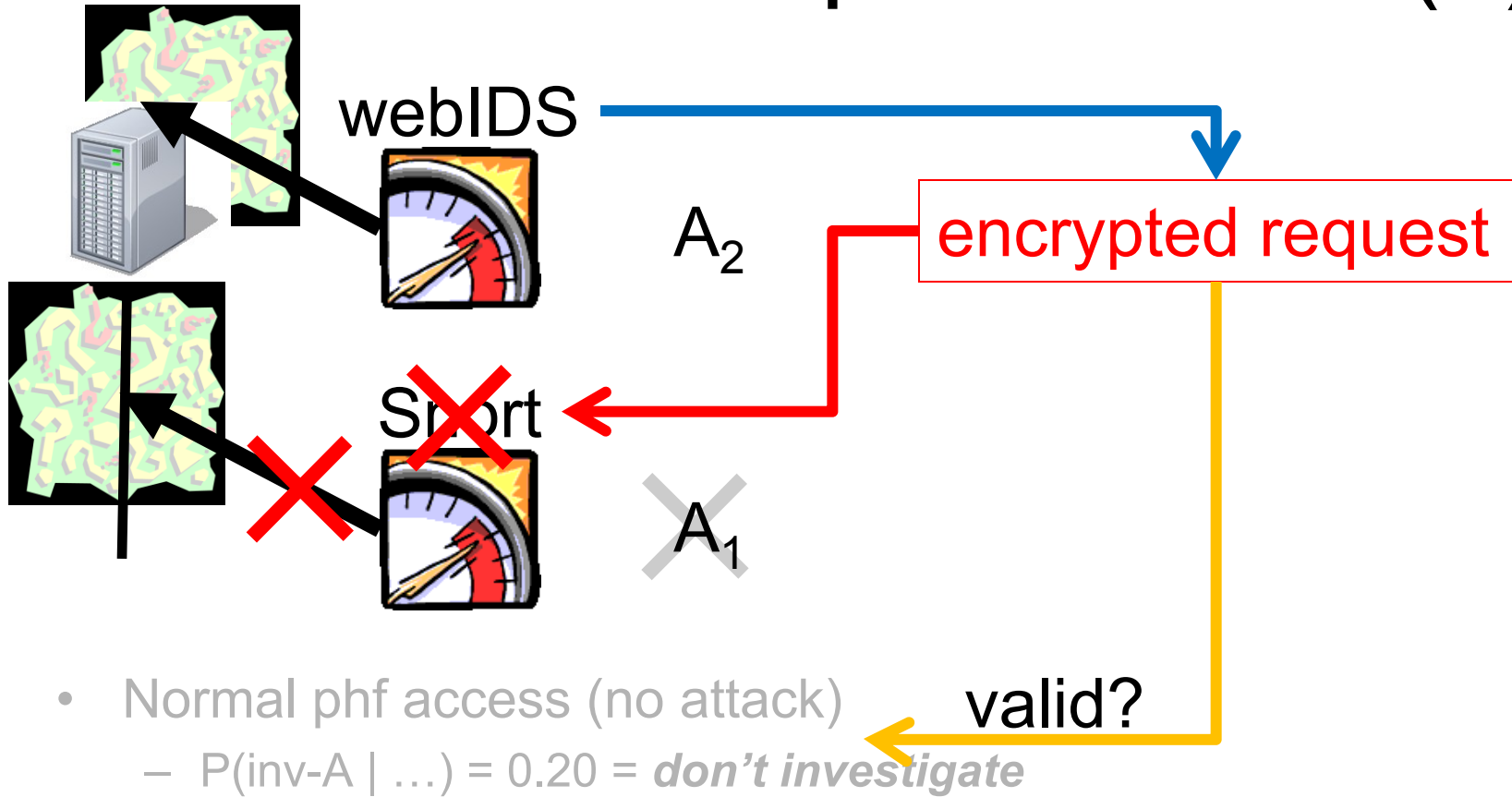


# Scenario multiple sensors (1)

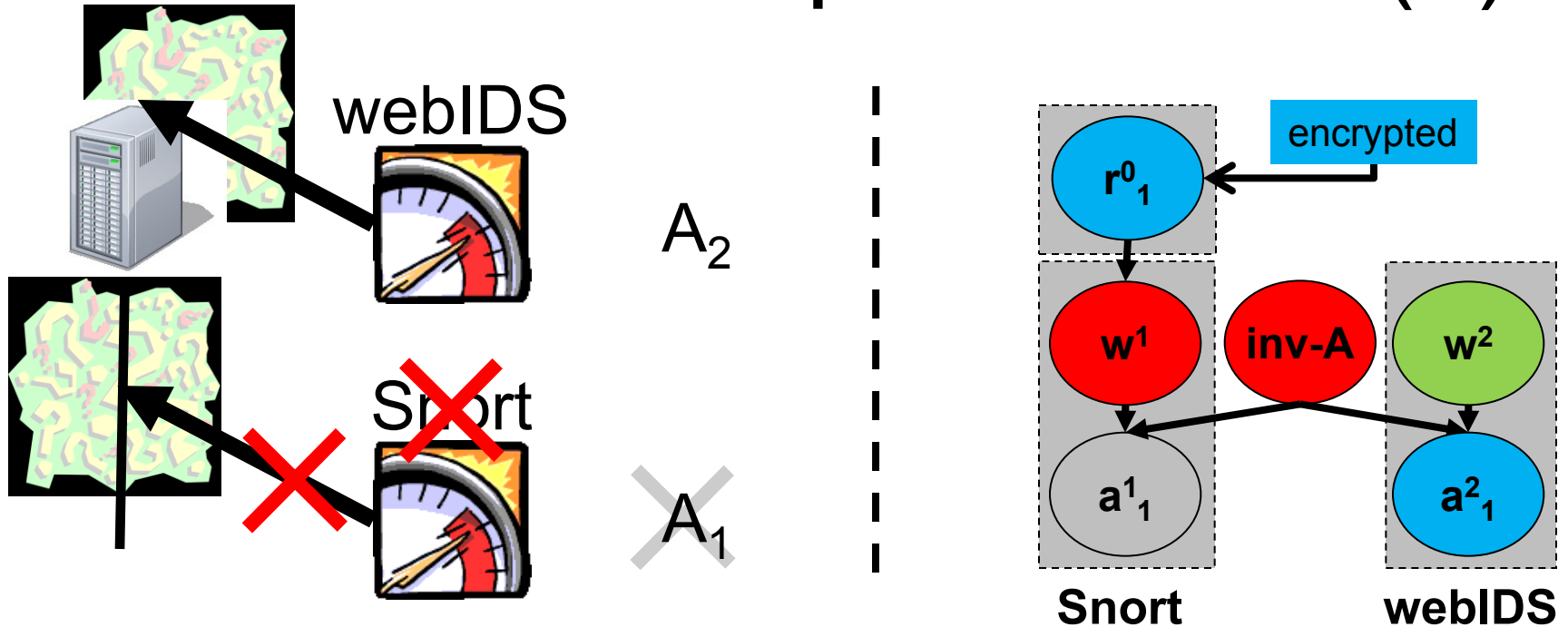


- Normal phf access (no attack)
  - $P(inv-A \mid \dots) = 0.20 = \textit{don't investigate}$

# Scenario multiple sensors (2)



# Scenario multiple sensors (3)



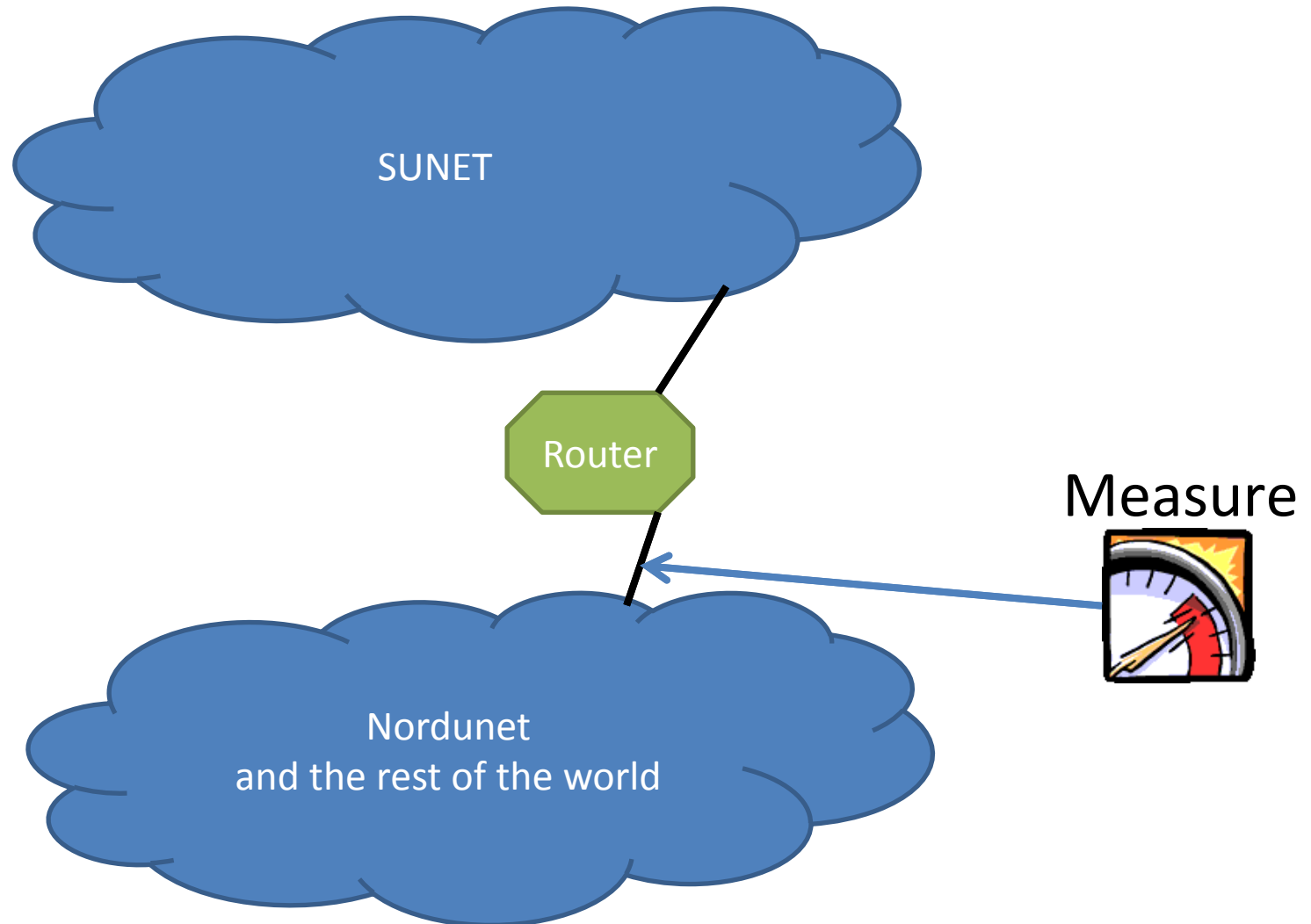
- Normal phf access (no attack)
  - $P(\text{inv-A} \mid \dots) = 0.20 = \text{don't investigate}$
- **Snort sensor defunct, this may be an attack!**
  - $P(\text{inv-A} \mid \dots) = 0.54 = \text{investigate}$
  - $P(w^1 \mid \dots) = 0.01 = \text{sensor broken}$

# Analysis of malicious backbone traffic

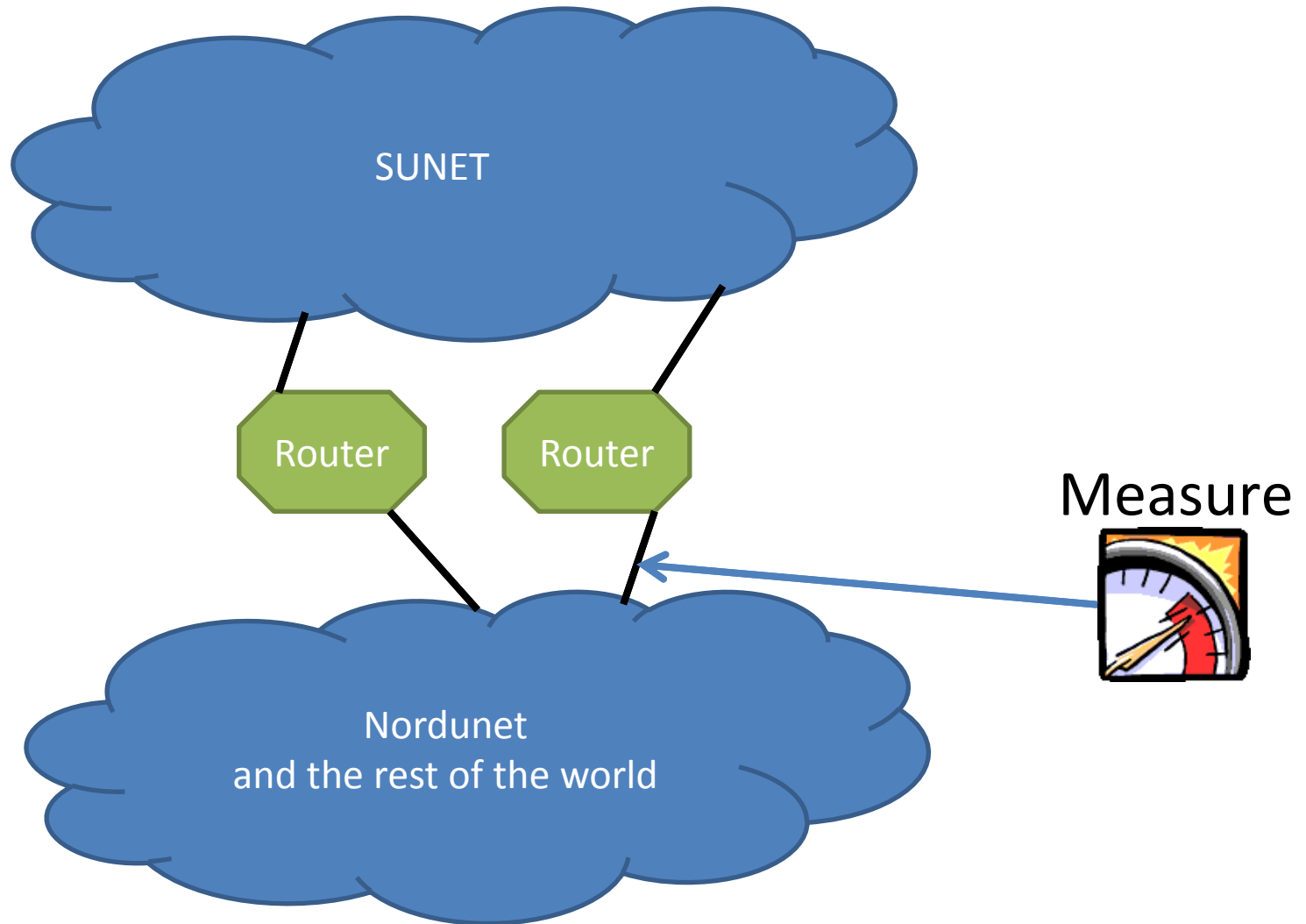
- Looking for attacks on a backbone network
  - 10 Gbps (=fast!)
  - Problems:
    - speed of network link
    - amount of data
    - routing
    - user privacy – anonymize data(!)



# Measurement Setup (simplified)

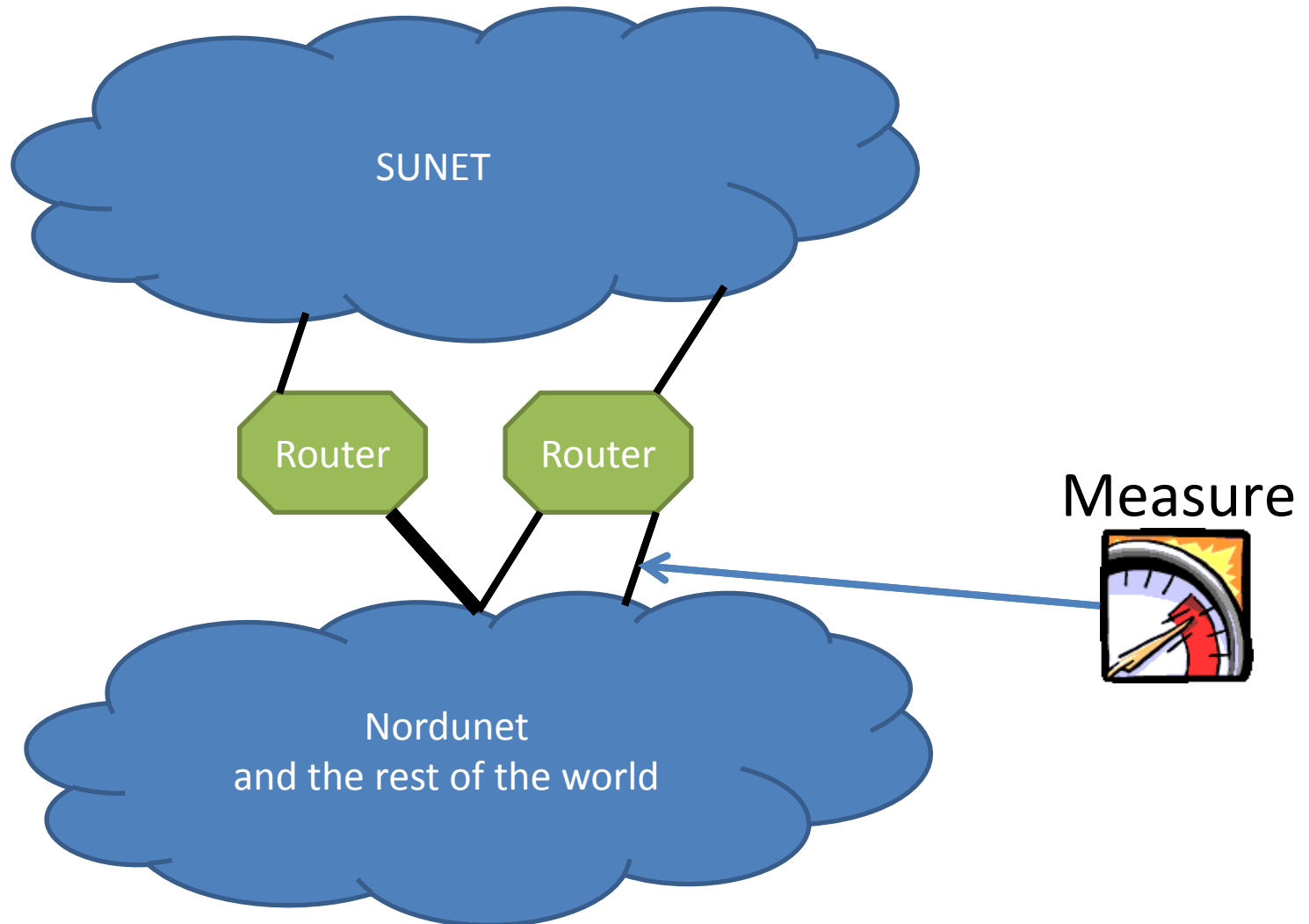


# Measurement Setup (simplified)

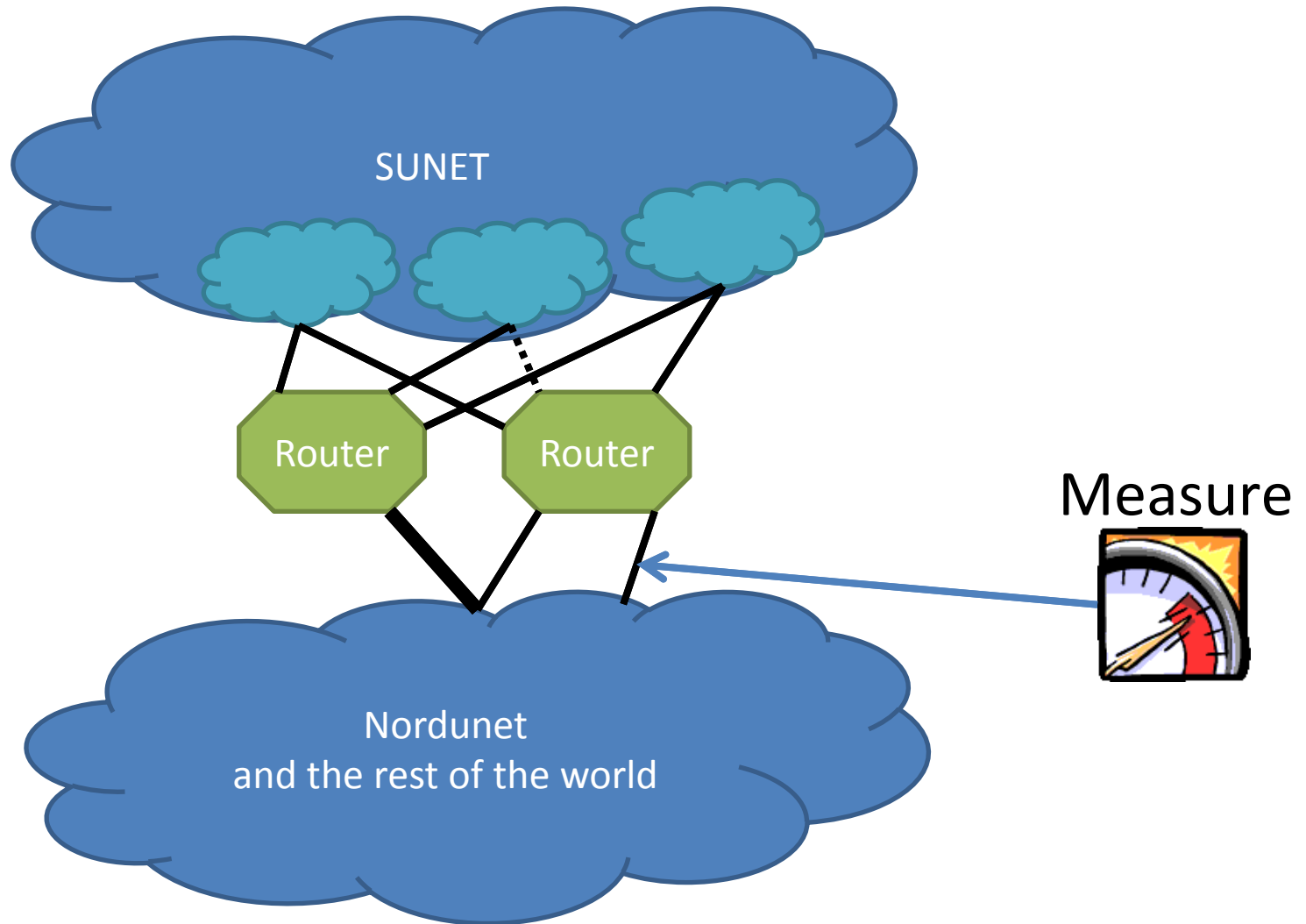




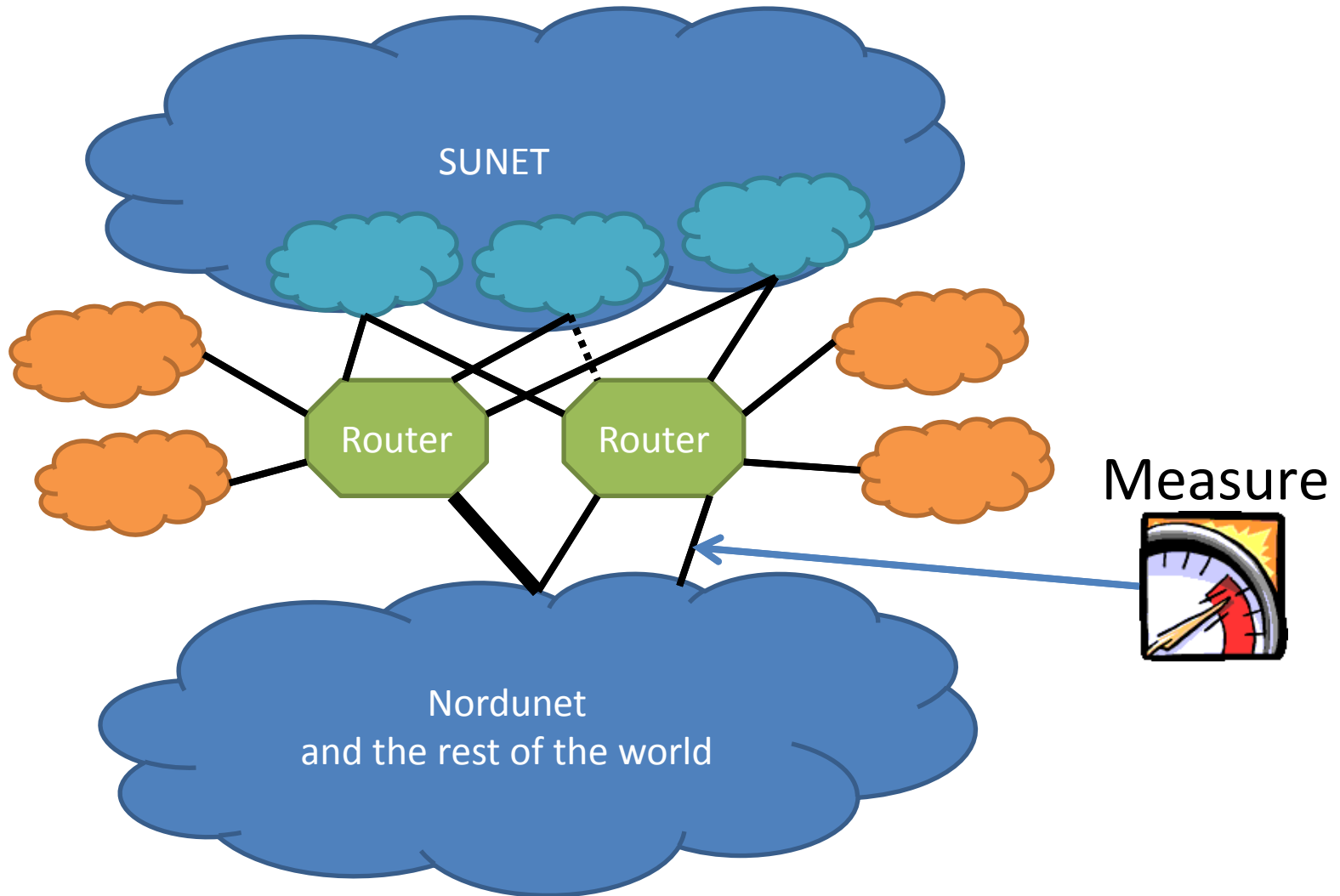
# Measurement Setup (simplified)



# Measurement Setup (simplified)

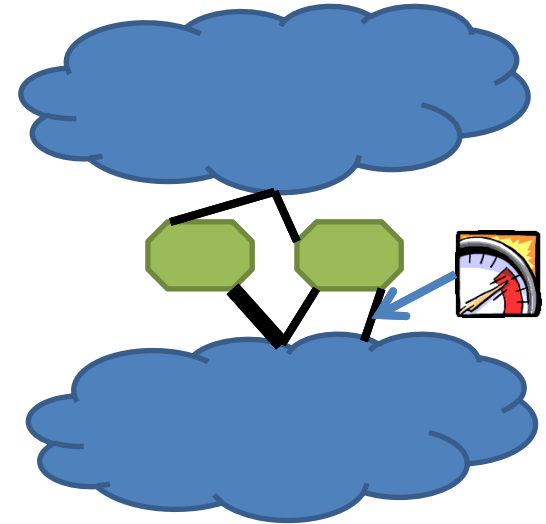


# Measurement Setup (simplified)



# 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.



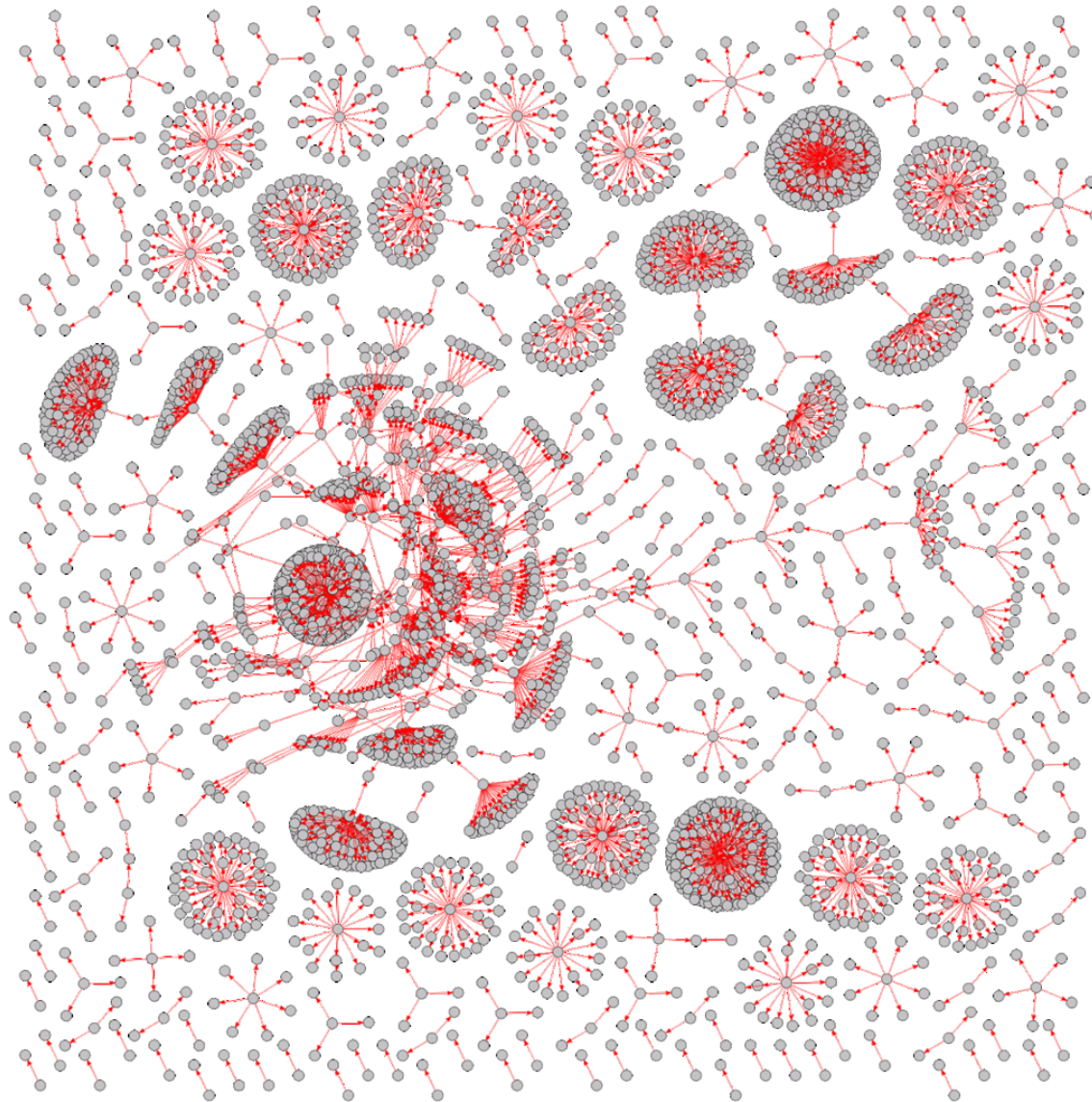
# Flow Output from CoralReef

- Unidirectional flows: 5-tuple

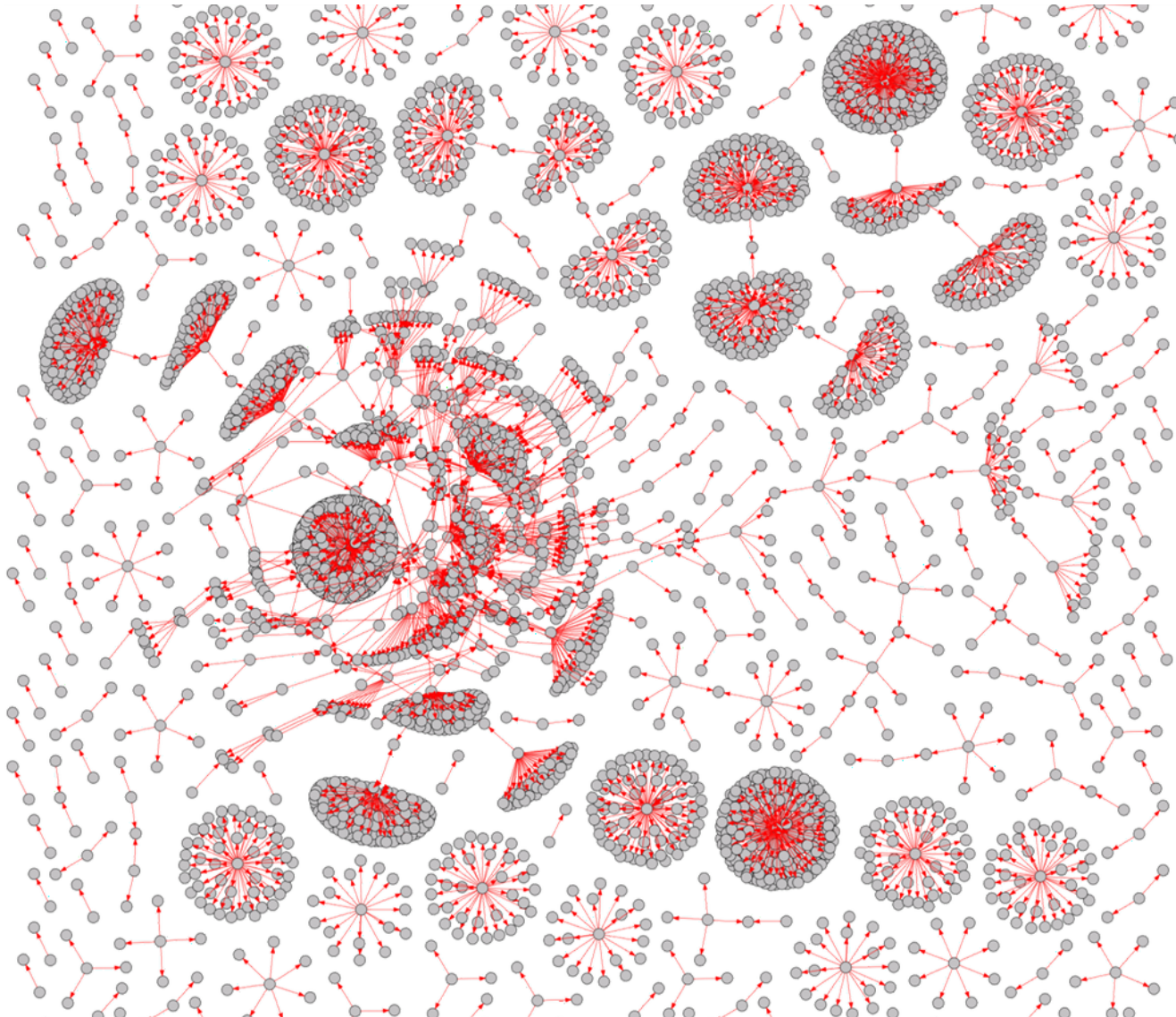
<u>srcIP</u>	<u>destIP</u>	<u>proto</u>	ok	<u>sport</u>	<u>dport</u>	pkts	bytes	flows	firstTS	lastTS
src <sup>1</sup>	dst <sup>1</sup>	6	1	445	3995	3	120	1	t <sub>0</sub> <sup>1</sup>	t <sub>n</sub> <sup>1</sup>
src <sup>2</sup>	dst <sup>2</sup>	1	1	3	1	1	56	1	t <sub>0</sub> <sup>2</sup>	t <sub>n</sub> <sup>2</sup>

- Data collected over a 6-week period (spring)
- IP addresses anonymized

# Analysis of backbone data

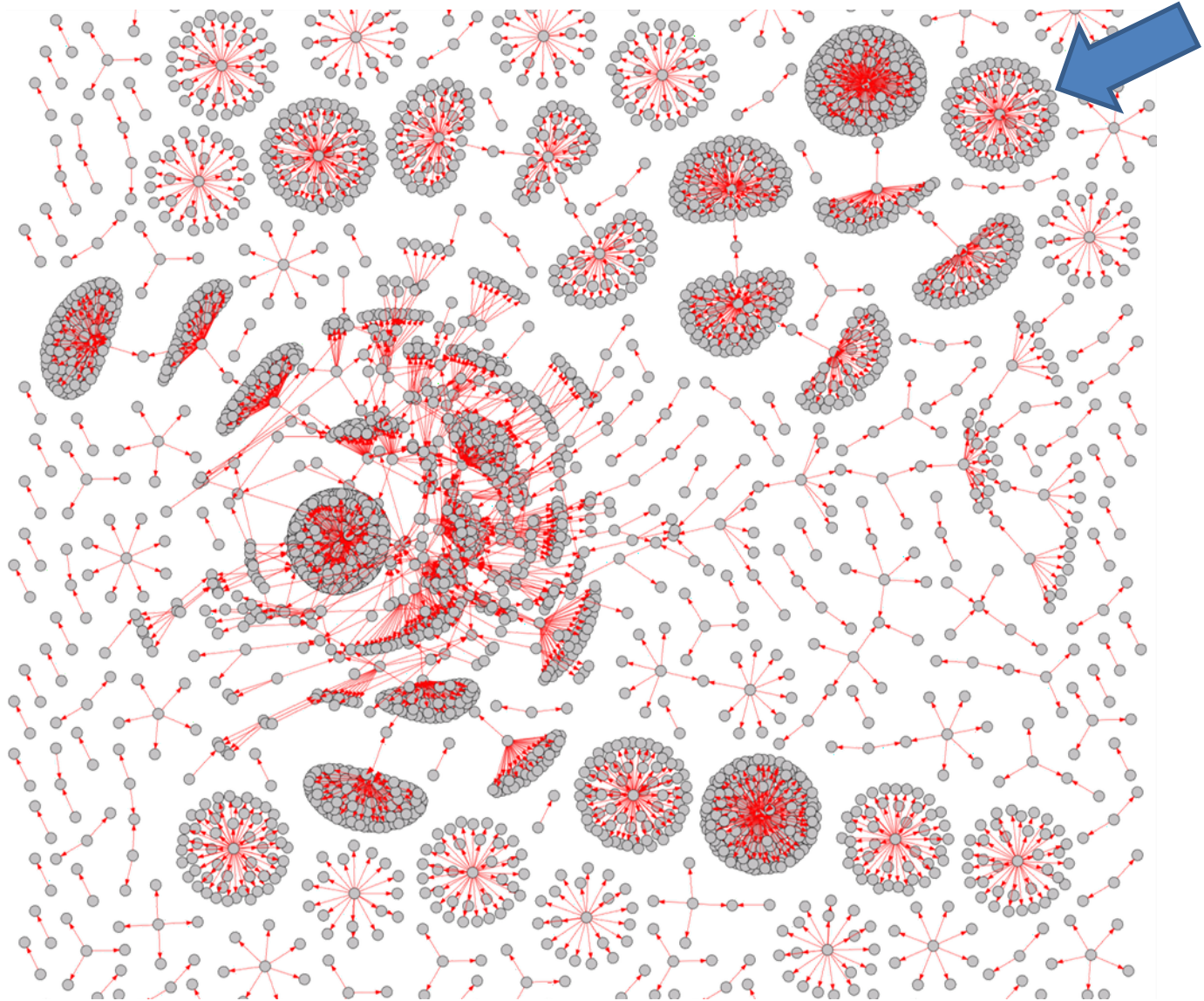


# Analysis of backbone data



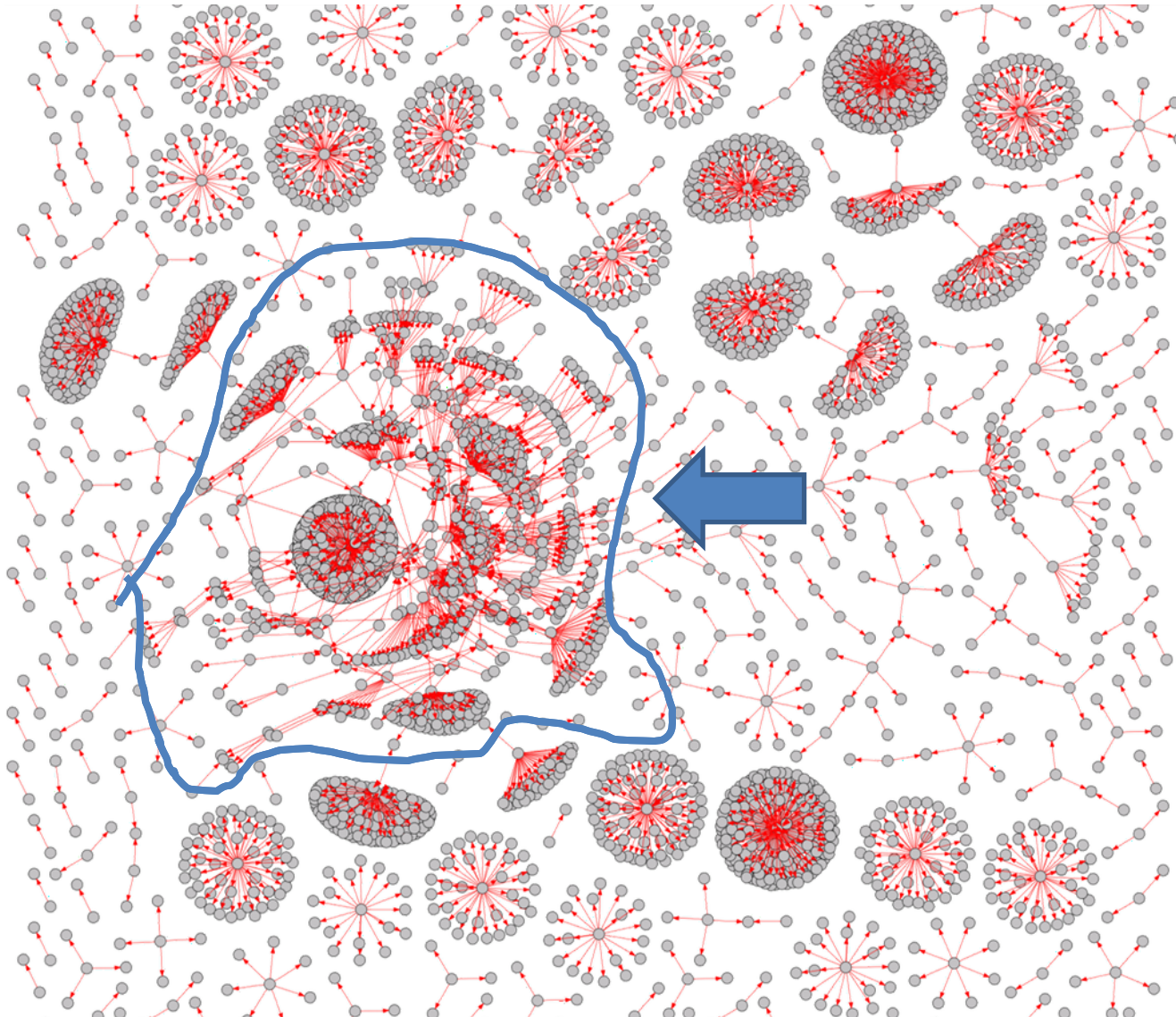


# Analysis of backbone data



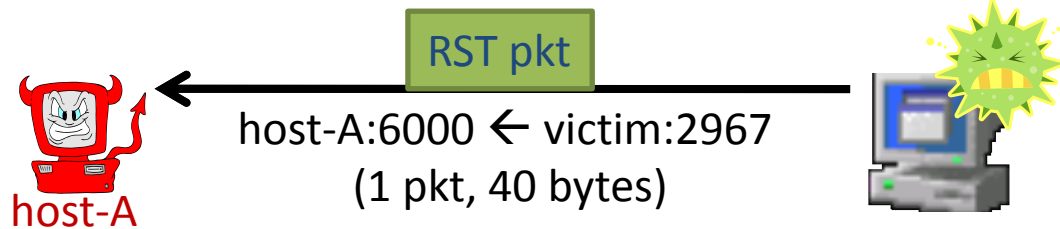


# Analysis of backbone data



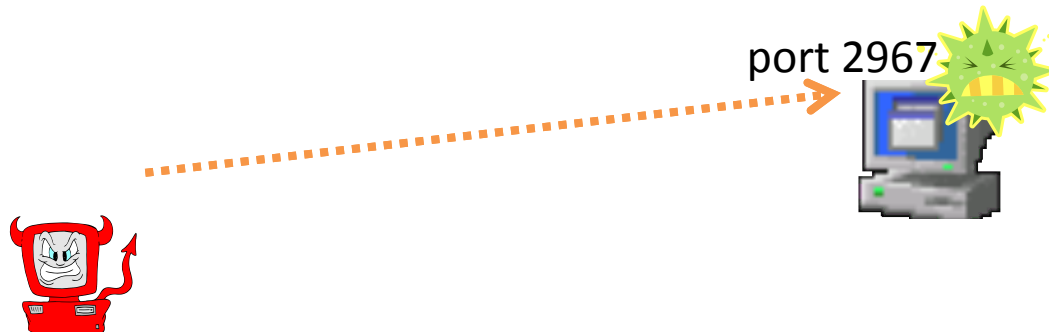


# Host-A: The Scanner



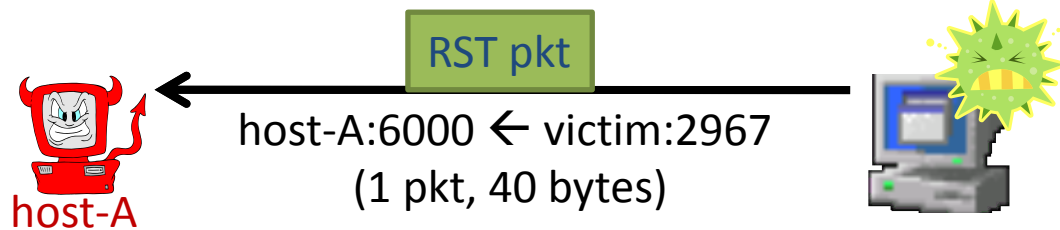
---

April 1: 2967 probed



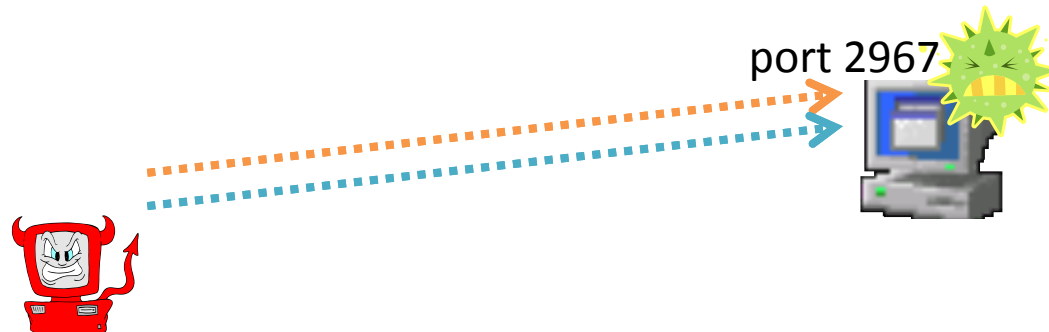


# Host-A: The Scanner



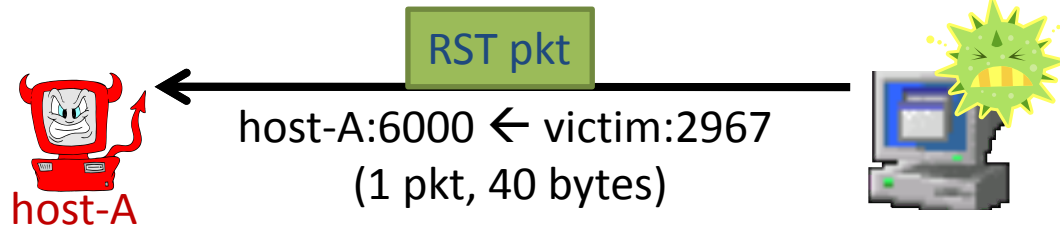
April 1: 2967 probed

April 8: 2967 probed





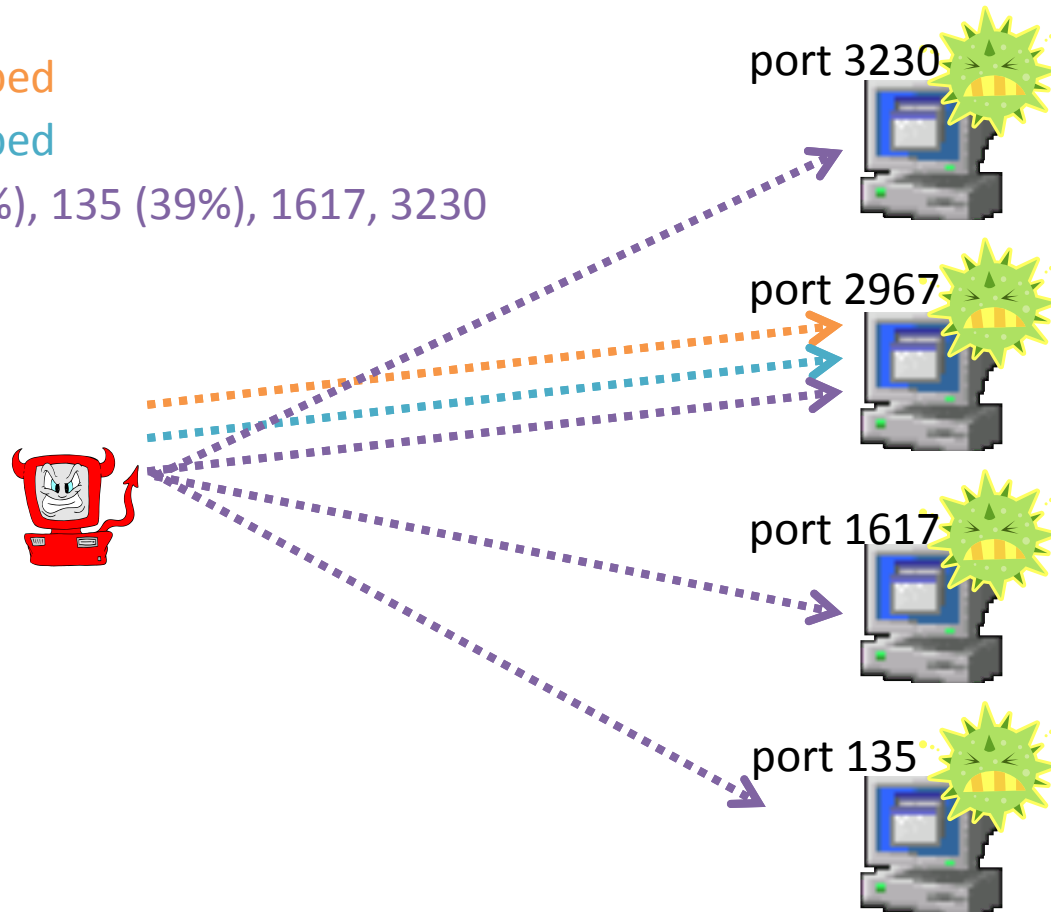
# Host-A: The Scanner



April 1: 2967 probed

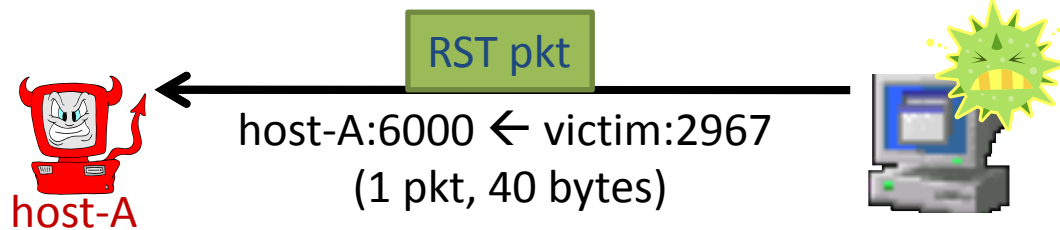
April 8: 2967 probed

April 15: 2967 (51%), 135 (39%), 1617, 3230





# Host-A: The Scanner

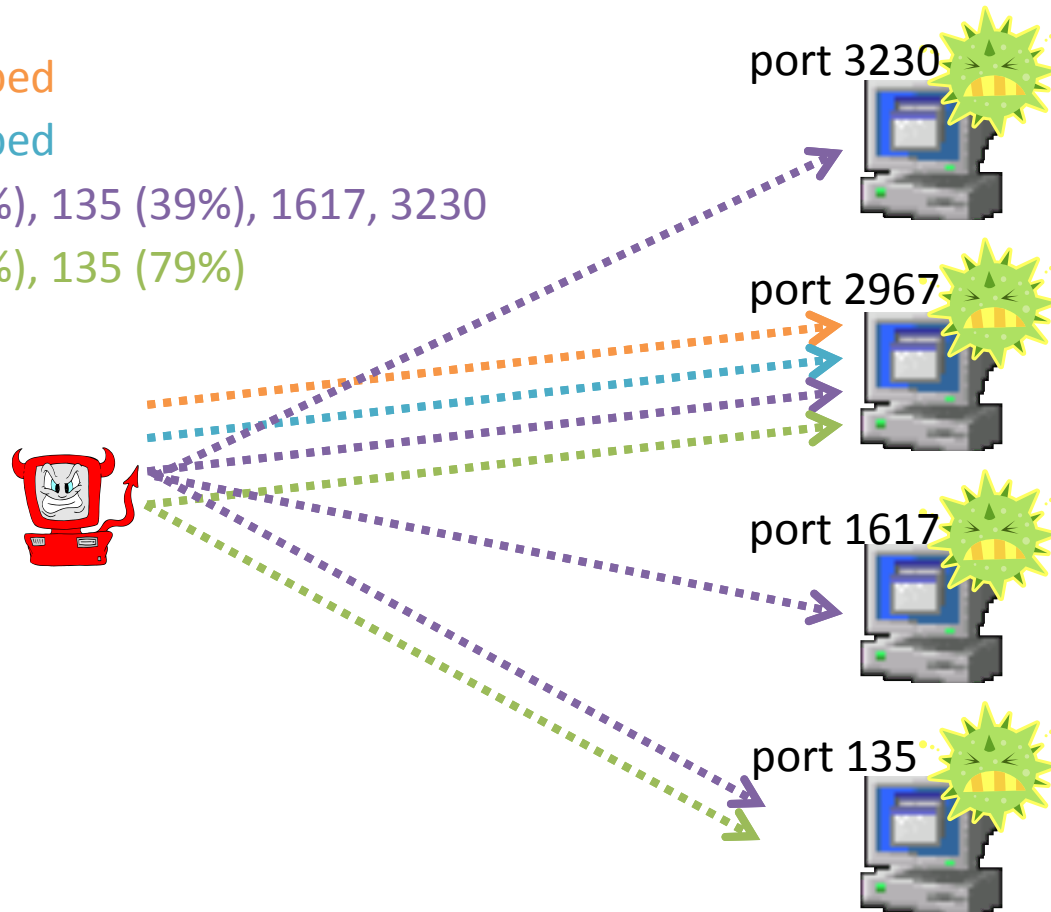


April 1: 2967 probed

April 8: 2967 probed

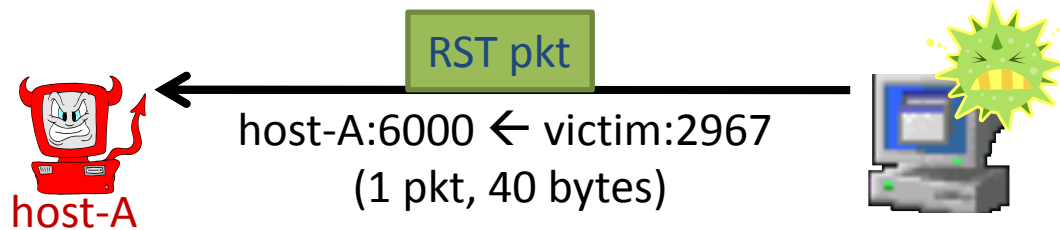
April 15: 2967 (51%), 135 (39%), 1617, 3230

April 22: 2967 (21%), 135 (79%)





# Host-A: The Scanner



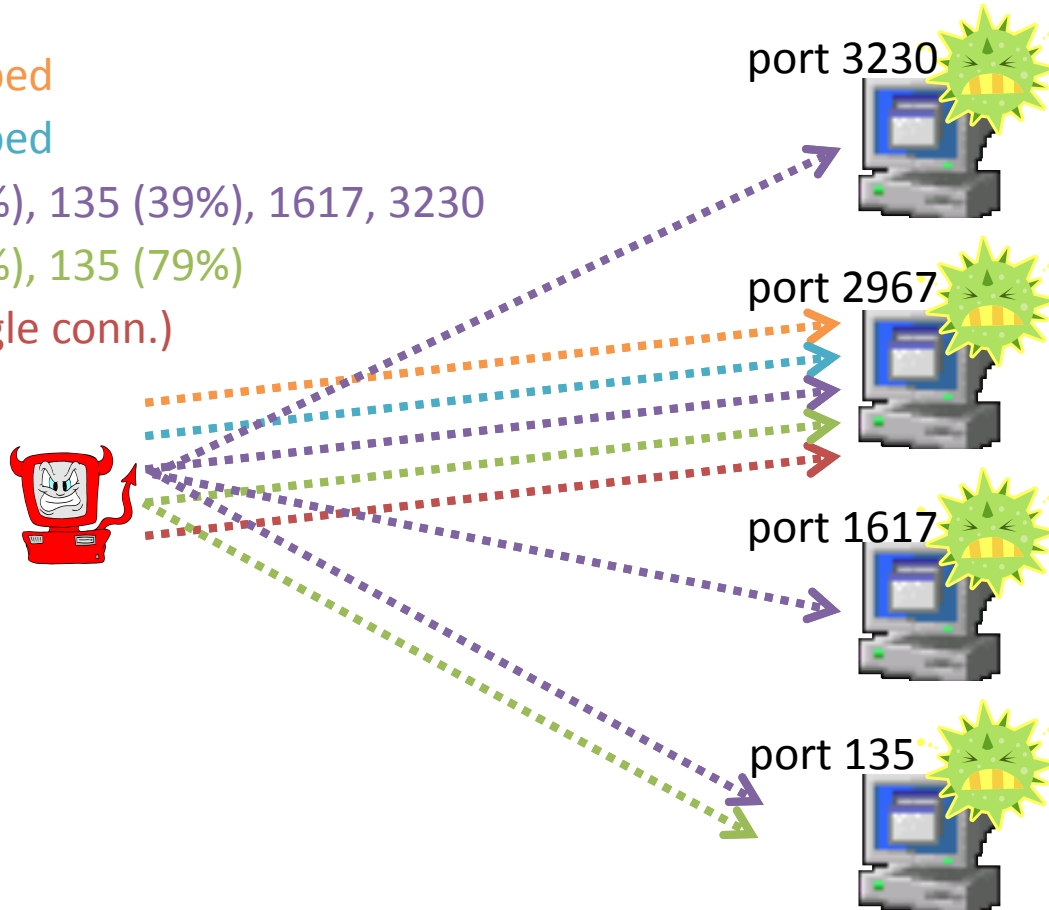
April 1: 2967 probed

April 8: 2967 probed

April 15: 2967 (51%), 135 (39%), 1617, 3230

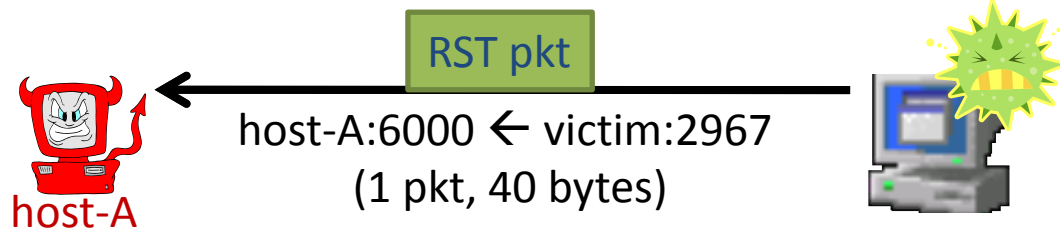
April 22: 2967 (21%), 135 (79%)

April 29: 2967 (single conn.)





# Host-A: The Scanner



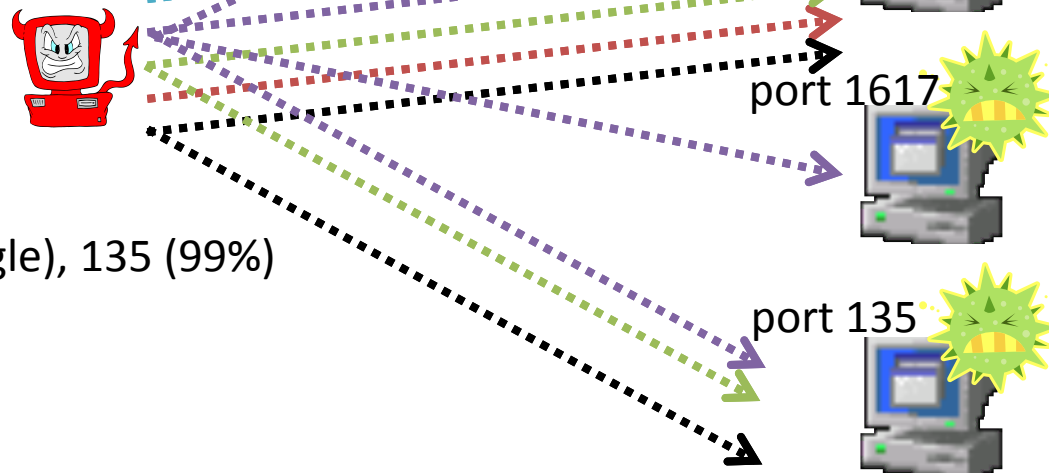
April 1: 2967 probed

April 8: 2967 probed

April 15: 2967 (51%), 135 (39%), 1617, 3230

April 22: 2967 (21%), 135 (79%)

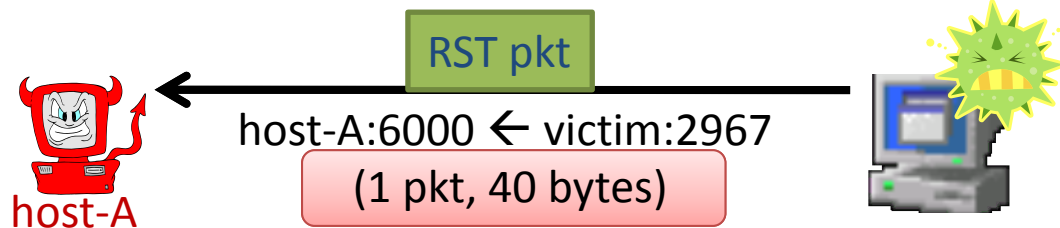
April 29: 2967 (single conn.)



May 5: 2967 (single), 135 (99%)



# Host-A: The Scanner



April 1: 2967 probed

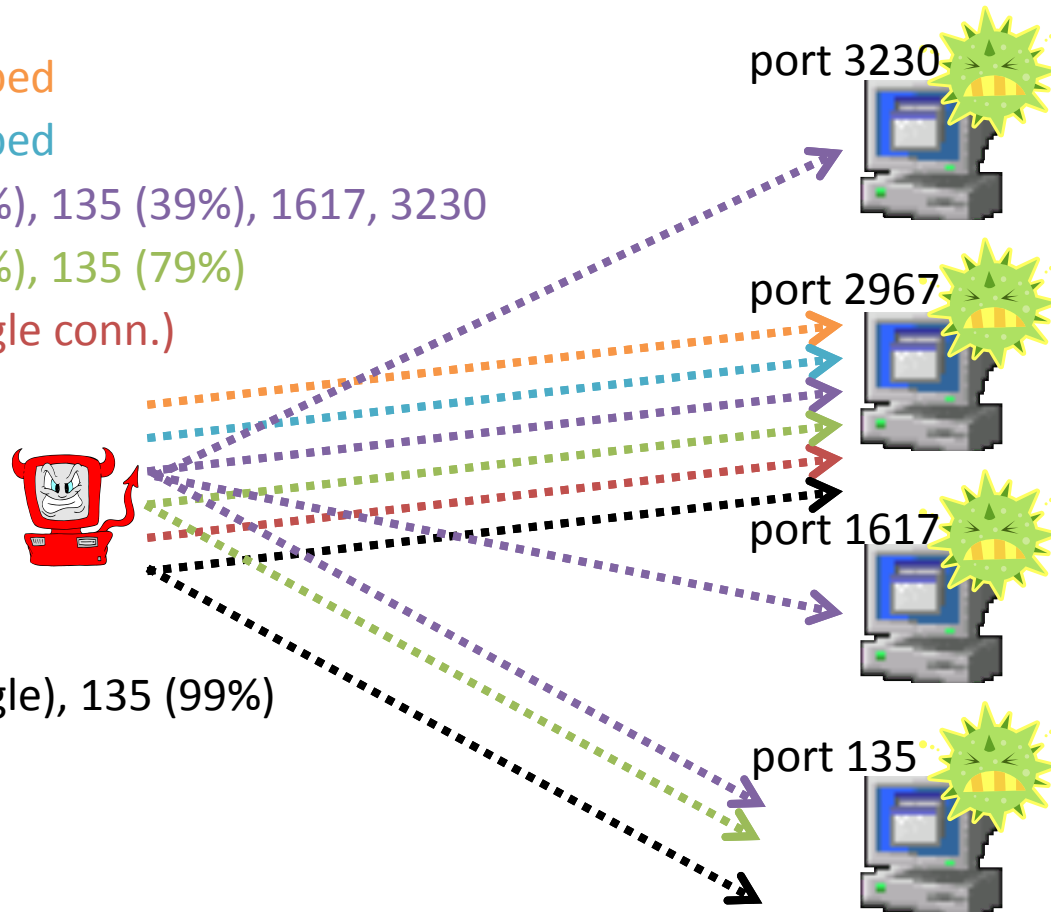
April 8: 2967 probed

April 15: 2967 (51%), 135 (39%), 1617, 3230

April 22: 2967 (21%), 135 (79%)

April 29: 2967 (single conn.)

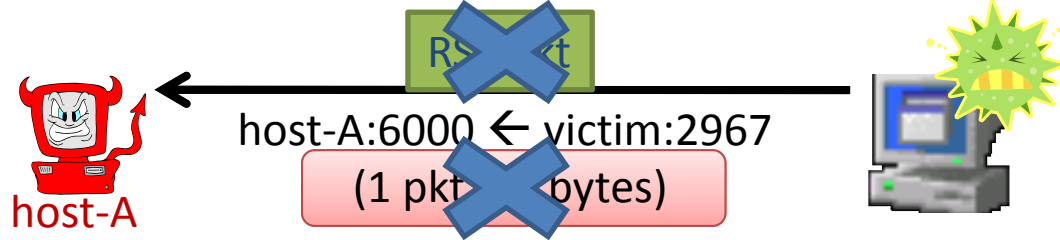
May 5: 2967 (single), 135 (99%)







# Host-A: The Scanner



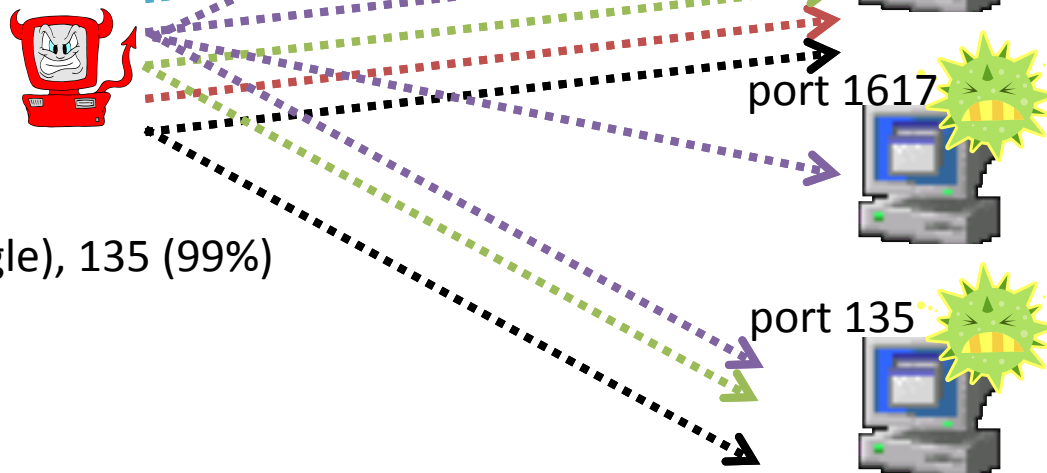
April 1: 2967 probed

April 8: 2967 probed

April 15: 2967 (51%), 135 (39%), 1617, 3230

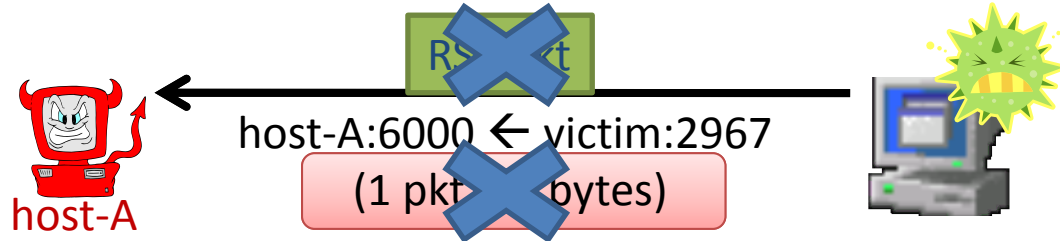
April 22: 2967 (21%), 135 (79%)

April 29: 2967 (single conn.)

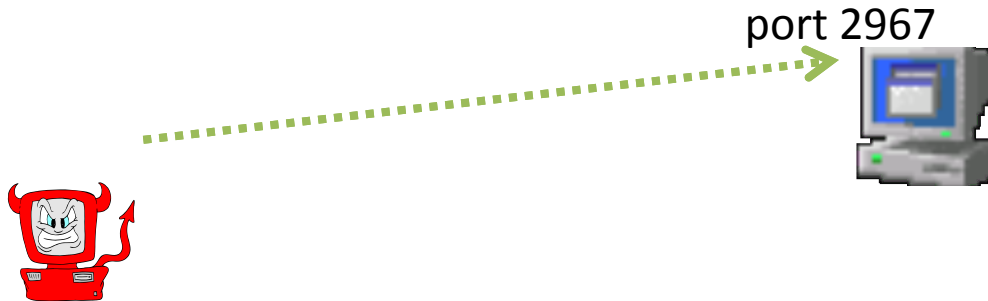


May 5: 2967 (single), 135 (99%)

# Host-A: The Scanner

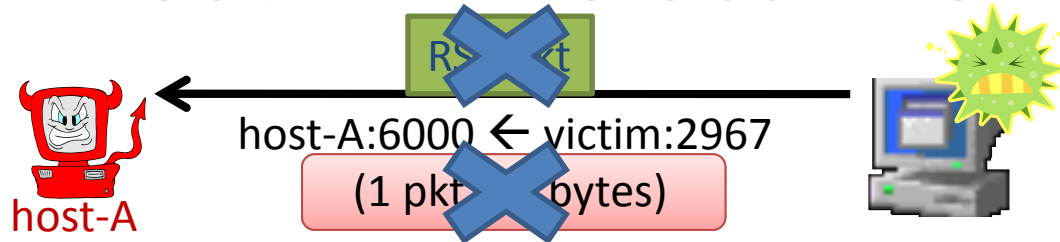


*April 22:*

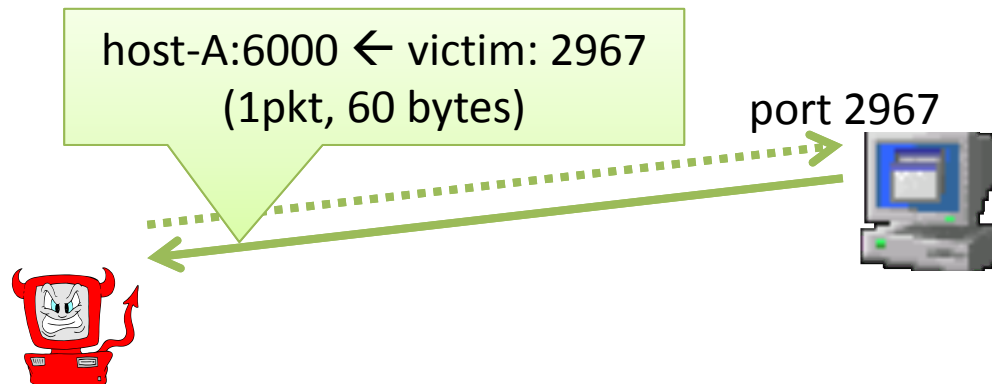




# Host-A: The Scanner

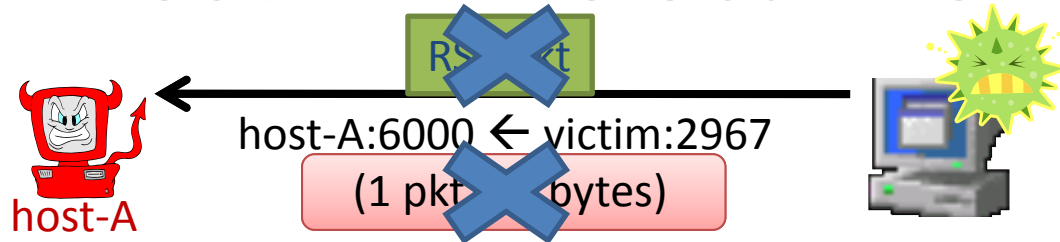


*April 22:*

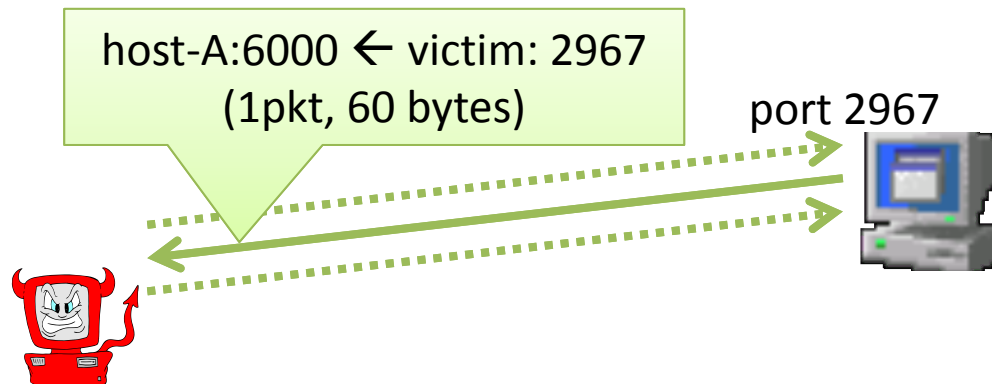




# Host-A: The Scanner

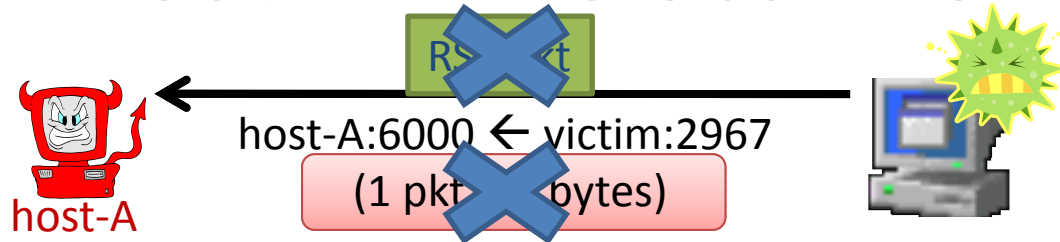


*April 22:*

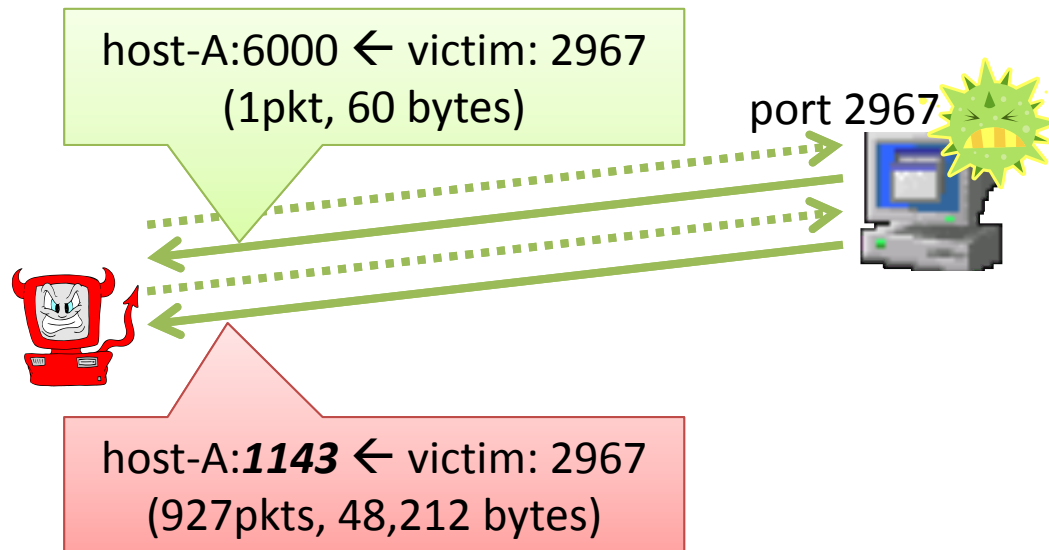




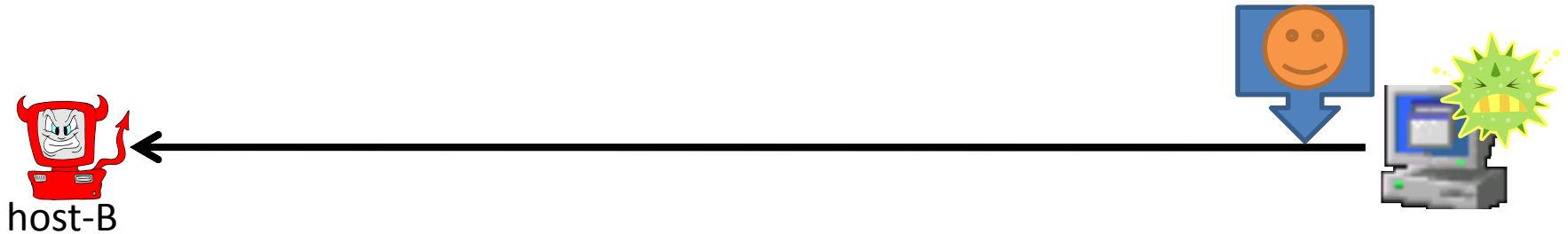
# Host-A: The Scanner



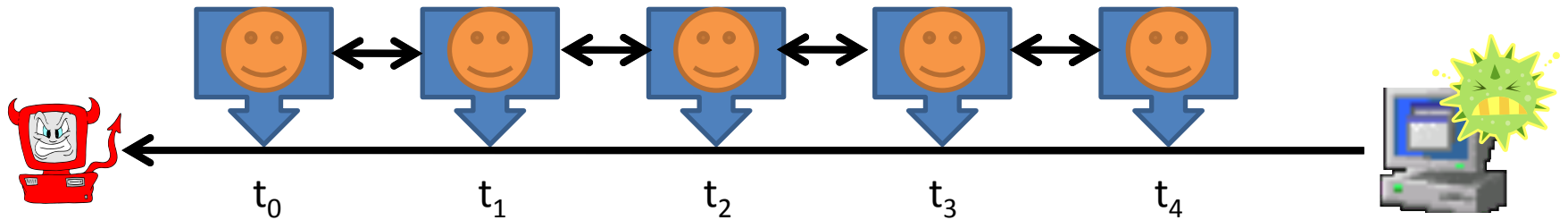
*April 22:*



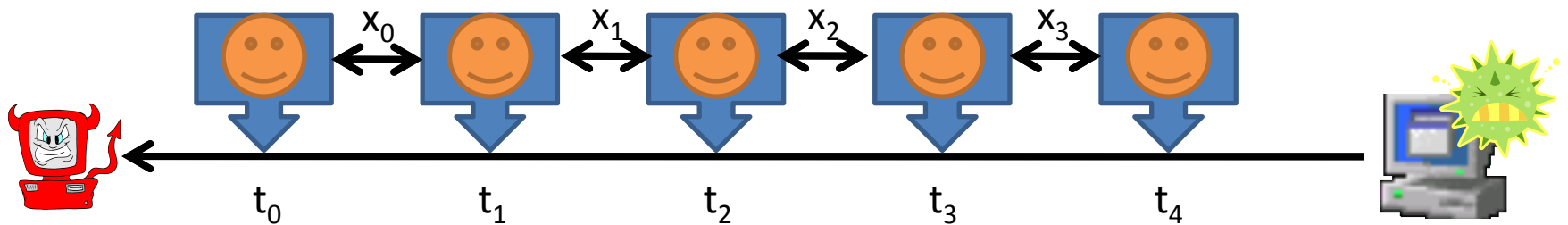
# Timing Behavior of Malicious Hosts







# Timing Behavior of Malicious Hosts



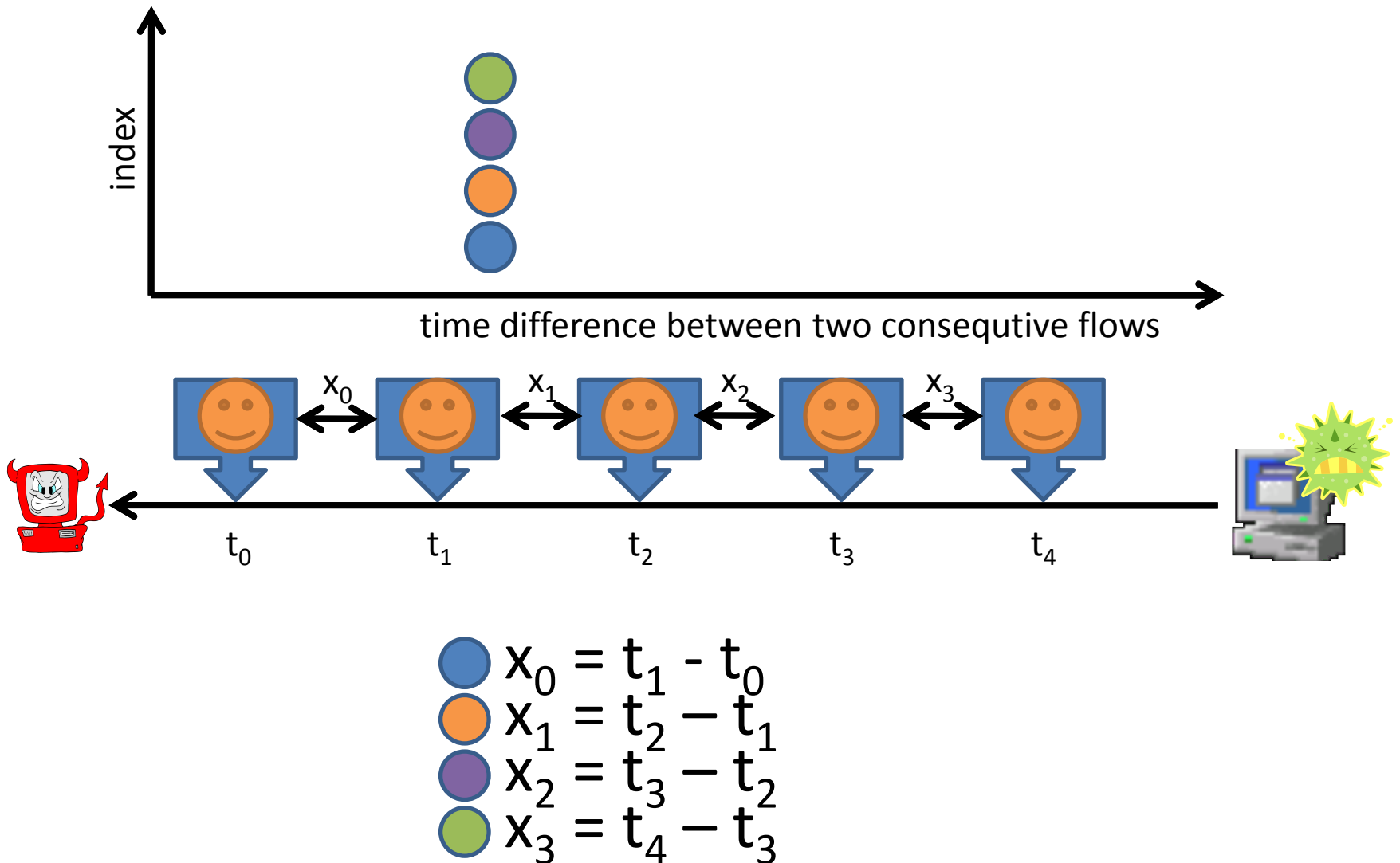
# Timing Behavior of Malicious Hosts



-   $x_0 = t_1 - t_0$
-   $x_1 = t_2 - t_1$
-   $x_2 = t_3 - t_2$
-   $x_3 = t_4 - t_3$

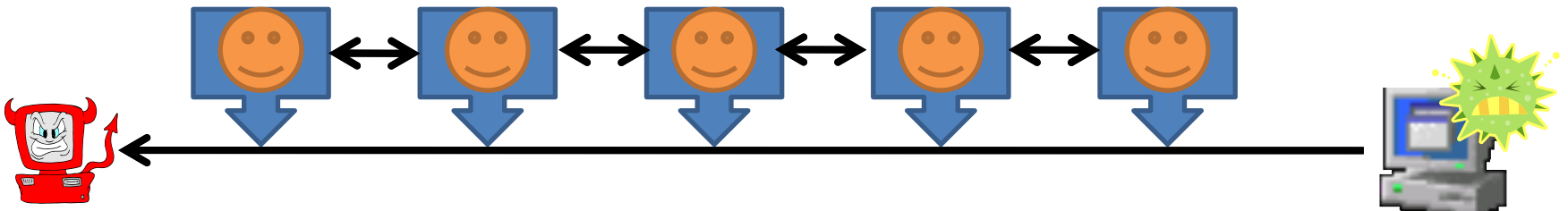


# Timing Behavior of Malicious Hosts



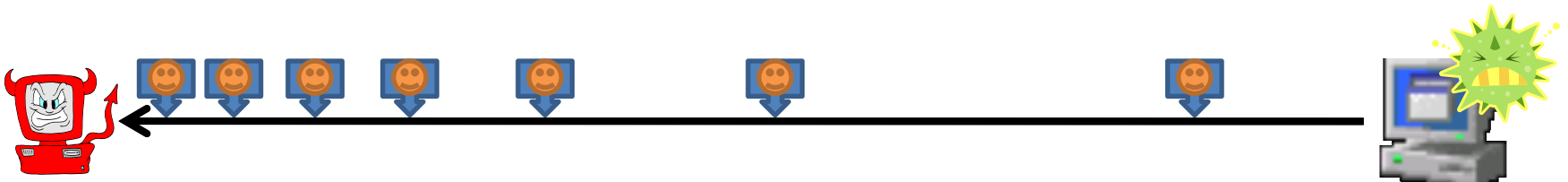
# Timing Behavior of Malicious Hosts

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



# Timing Behavior of Malicious Hosts

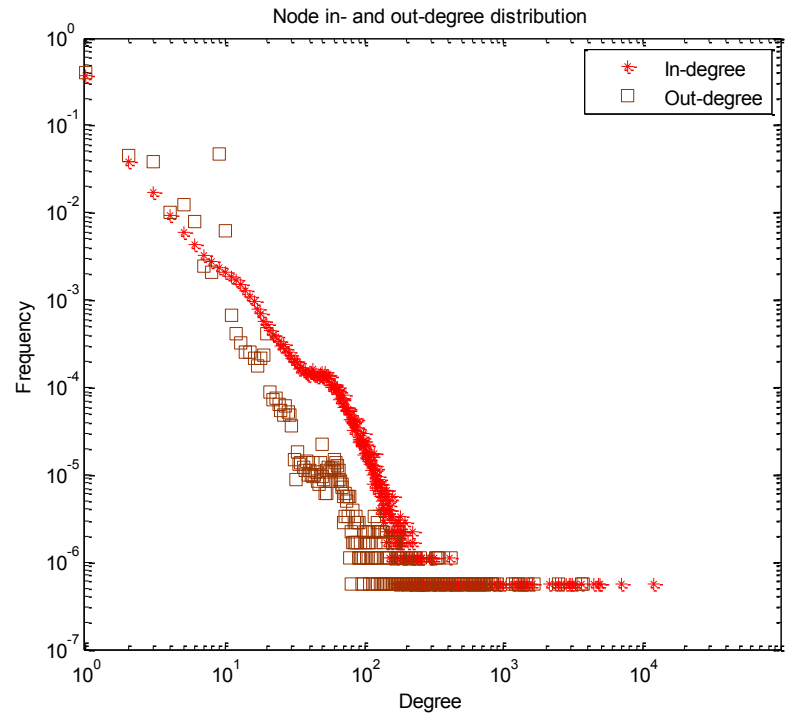
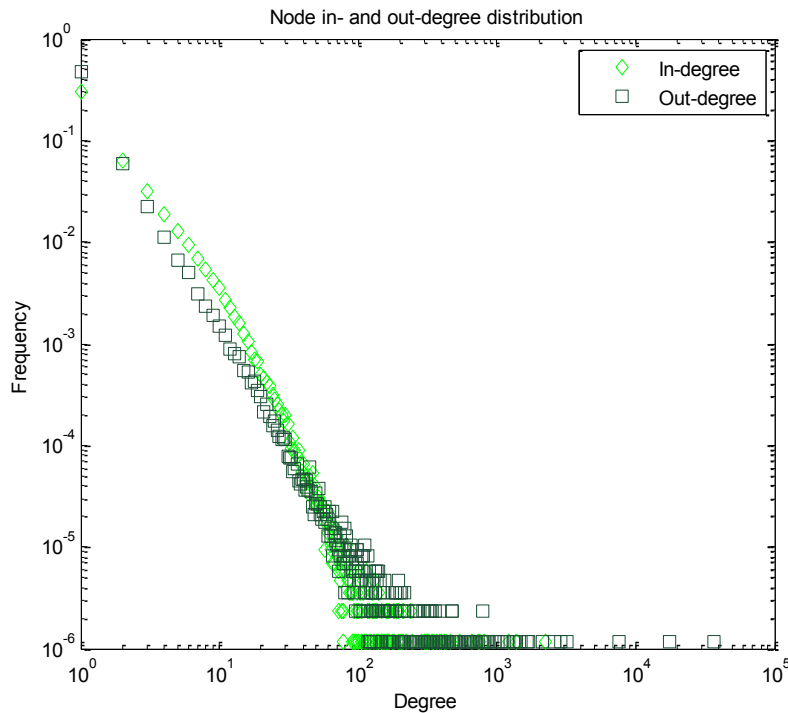
Exponential backoff: 111s, 222s, 333s, 666s, 1332s, 2664s



# 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

# 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/>*