Network Security @ ICS MU

Jan Vykopal

vykopal@ics.muni.cz

May 10, 2012
FI MU, Brno

Part I

Introduction

Present Computer Security

Present Essentials and Best Practices

- host-based: firewall, antivirus, automated patching, NAC[1]
- network-based: firewall, antispam filter, IDS[2], UTM[3]

Network Security Monitoring

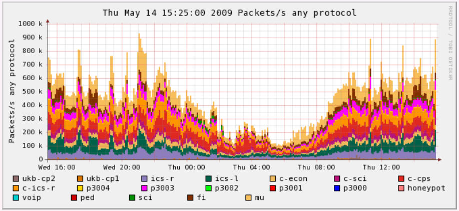
- **Necessary complement to host-based approach.**
- NBA[4] is a **key approach** in large and high-speed networks.
- Traffic acquisition and storage is almost done, **security analysis is a challenging task**.

[1] Network Access Control, [2] Intrusion Detection System
[3] Unified Threat Management, [4] Network Behavior Analysis

Flow Based Monitoring

- Provides information about who communicates with whom, for how long, which protocol, how much data and so on.
- Based on CISCO NetFlow v5/v9 technology and IETF IPFIX.
- Enables you to watch your network traffic in real-time.
- GEANT2 Security Toolset = FlowMon probe + NfSen.

```
Duration Proto        Src IP Addr:Port          Dst IP Addr:Port   Flags
   2.096 TCP               56956  ->          108.7.1.50:80     .AP.S.
   0.094 TCP     108.7.1.         ->    59.173.182.61:49442     .AP.S.
   0.368 TCP     108.7.1.50       ->    59.173.182.61:49440     .AP.S.
   0.737 TCP                      ->    59.173.182.61:49434     .AP.S.
   0.379 TCP     108.7.1.50:      ->    59.173.182.61:49438     .AP.S.
   0.296 TCP                                108.7.1.50:80       .AP.S.
   0.575 TCP   59.173.182.61:4                108.7.1.50:80       .AP.S.
   0.574 TCP   59.173.182.61:                 108.7.1.50:80       .AP.S.
   0.451 TCP                                  108.7.1.50:80       .AP...
   1.281 TCP   59.173.182.61                  108.7.1.50:80       .AP.SF
   1.280 TCP                           3.233.173:41667     .AP.SF
   5.886 TCP   9.173.182.61         ->          .248.129:1687      .AP...
   6.051 TCP          13.233    687   ->                 50:80      .AP...
   2.800 TCP          108.7.1.50:80   ->    210.                :56607     .AP.S.
   2.980 TCP     210.56.6.116:56607   ->          108.7.              .AP.S.
   1.693 TCP          108.7.1.50:80   ->    157.242.141.18
   1.778 TCP          108.7.1.50:80   ->    157.242.141.183:132
   0.604 TCP   157.242.141.183:1325   ->          108.7.1.50:80
   1.990 TCP   157.242.141.183:1324   ->          108.7.1.50:80      .AP.S.
```



Detailed network view with NetFlow data.

NetFlow Applications in Time

Originally

Accounting

NetFlow Applications in Time

Originally

Accounting

Then

Incident handling
Network forensics

NetFlow Applications in Time

Originally

Accounting

Then

Incident handling
Network forensics

Now

Intrusion detection
Network protection

Part II

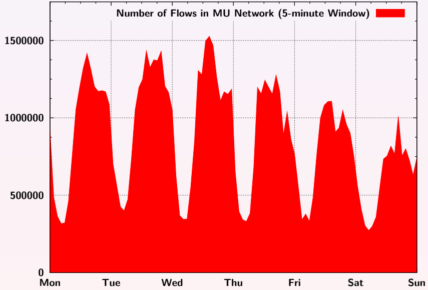
NetFlow Monitoring at MU

Masaryk University, Brno, Czech Republic

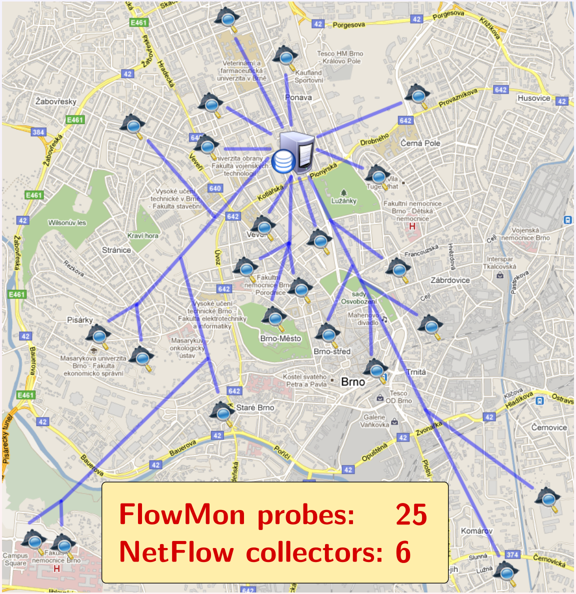
- 9 faculties: 200 departments and institutes
- 48,000 students and employees
- **15,000 networked hosts**
- 2x 10 gigabit uplinks to CESNET (NREN)

Interval	Flows	Packets	Bytes
Second	5 k	150 k	132 M
Minute	300 k	9 M	8 G
Hour	15 M	522 M	448 G
Day	285 M	9.4 G	8 T
Week	1.6 G	57 G	50 T

Average traffic volume at the edge links in peak hours.



FlowMon Probes at Masaryk University Campus


Žabovřesky
Ponava
Husovice
Černá Pole
Lužánky
Wilsonův les
Kraví hora
Stránice
Zábrdovice
Pisárky
Brno-Město
Brno-střed
Brno
Trnitá
Staré Brno
Černovice
Komárov
Veterinární a farmaceutická univerzita v Brně
Vysoké učení technické v Brně - Fakulta stavební
Vysoké učení technické Brno - Fakulta elektrotechniky a informatiky
Masarykova univerzita Brno - Fakulta ekonomicko správní
Masarykův onkologický ústav
Fakultní nemocnice Brno - Dětská nemocnice
Fakultní nemocnice Brno
Kostel svatého Petra a Pavla
Tesco HM Brno Královo Pole
Campus Square

FlowMon probes: 25
NetFlow collectors: 6

NetFlow Monitoring at Masaryk University

1/10 GE

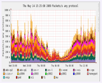
FlowMon probe

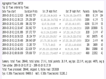
FlowMon probe

FlowMon probe

NetFlow data acquisition

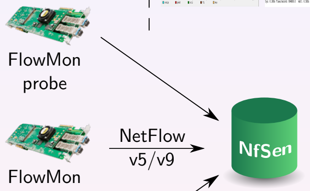
NetFlow Monitoring at Masaryk University





```
Aggregated flows 246720
Top 10 flows ordered by flows:
Date flow start          Duration Proto   Src IP Addr:Port       Dst IP Addr:Port   Packets  Bytes Flows
2009-03-20 02:11:12.533  364.932 TCP    [illegible] -> [illegible]    8699    8.1 M   184
2009-03-20 02:12:30.215  379.256 UDP    [illegible] -> [illegible]   19286    4.1 M    72
2009-03-20 02:11:51.690  388.352 TCP    [illegible] -> [illegible]   41096   53.3 M    55
2009-03-20 02:12:18.467  282.902 TCP    [illegible] -> [illegible]   18089  1035699    51
2009-03-20 02:12:01.806  307.372 TCP    [illegible] -> [illegible]    2638    2.0 M    47
2009-03-20 02:16:56.525   26.194 TCP    [illegible] -> [illegible]     343   288875    45
2009-03-20 02:12:30.480  286.948 UDP    [illegible] -> [illegible]   18234    2.4 M    44
2009-03-20 02:15:42.053   13.280 TCP    [illegible] -> [illegible]     186    18089    43
2009-03-20 02:13:45.343  213.639 TCP    [illegible] -> [illegible]    3864   253888    43
2009-03-20 02:08:00.690  579.690 TCP    [illegible] -> [illegible]    4900   215262    41

Summary: total flows: 298440, total bytes: 17.0 G, total packets: 26.9 M, avg bps: 221.9 M, avg pps: 44876, avg b
Time window: 2009-03-20 02:07:32 - 2009-03-20 02:17:39
Total flows processed: 298440, skipped: 0, Bytes read: 15519100
Sys: 0.380s flows/second: 984880.0   Wall: 0.580s flows/second: 511301.2
```



1/10 GE

FlowMon probe

FlowMon probe

FlowMon probe

NetFlow v5/v9

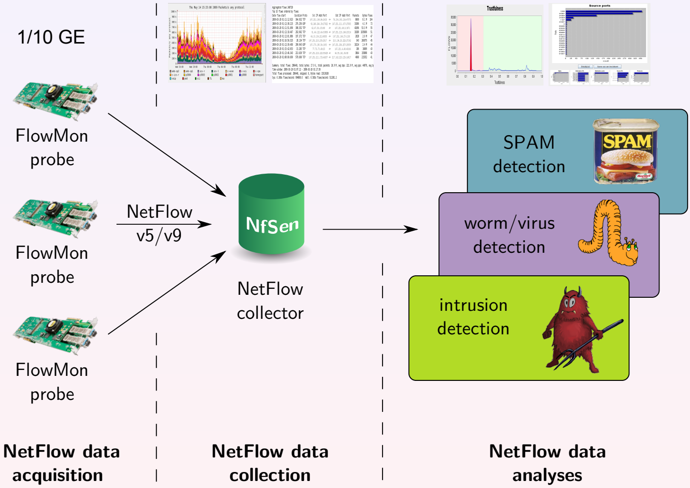
NfSen

NetFlow collector

NetFlow data acquisition

NetFlow data collection

NetFlow Monitoring at Masaryk University



1/10 GE

FlowMon probe

FlowMon probe

FlowMon probe

NetFlow v5/v9

NfSen

NetFlow collector

SPAM detection

worm/virus detection

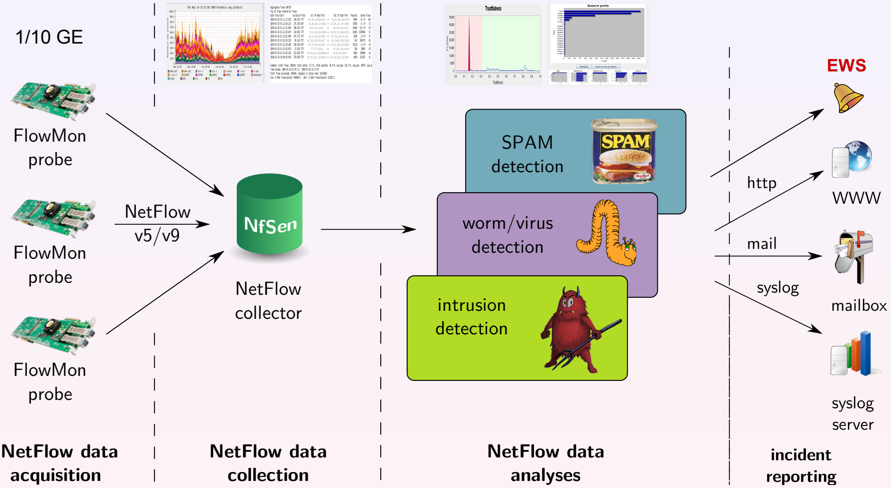
intrusion detection

NetFlow data acquisition

NetFlow data collection

NetFlow data analyses

NetFlow Monitoring at Masaryk University



1/10 GE

FlowMon probe

FlowMon probe

FlowMon probe

NetFlow v5/v9

NfSen

NetFlow collector

SPAM detection

worm/virus detection

intrusion detection

http

mail

syslog

EWS

WWW

mailbox

syslog server

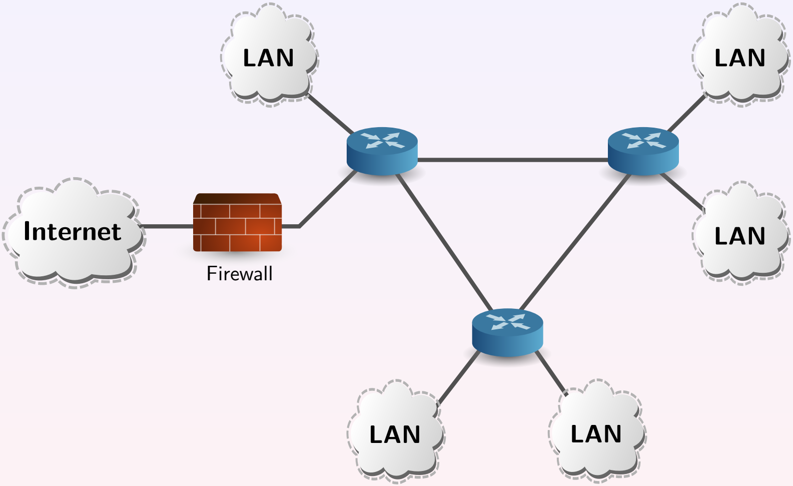
NetFlow data acquisition

NetFlow data collection

NetFlow data analyses

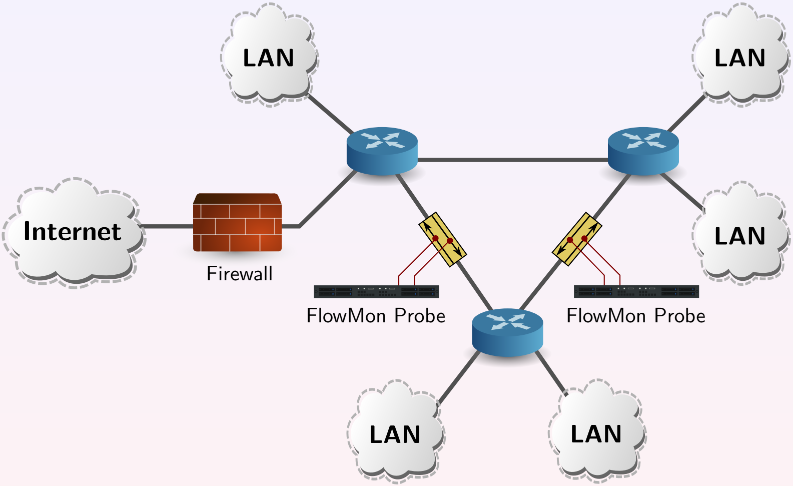
incident reporting

Flow-based Traffic Monitoring System



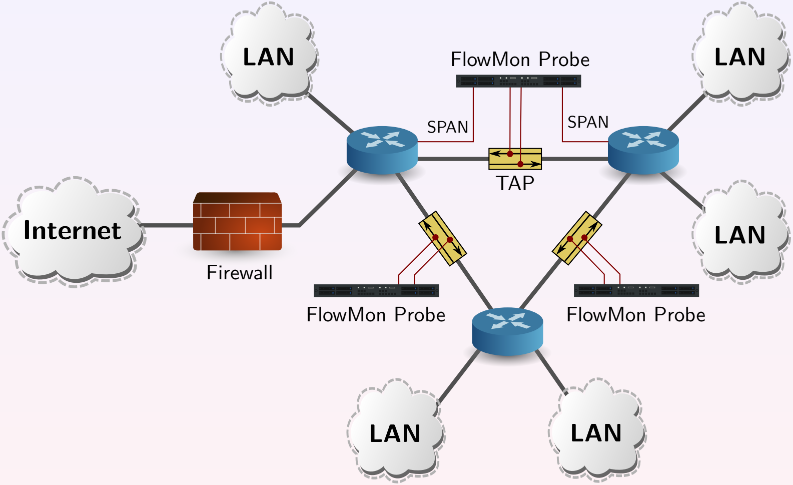
Network without any flow monitoring system.

Flow-based Traffic Monitoring System



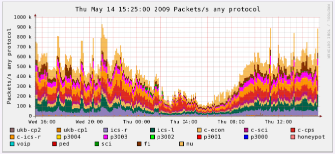
FlowMon probe connected to in-line TAP.

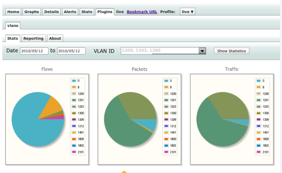
Flow-based Traffic Monitoring System



FlowMon observes data from TAP and SPAN ports.

NfSen/NFDUMP Collector Toolset Architecture

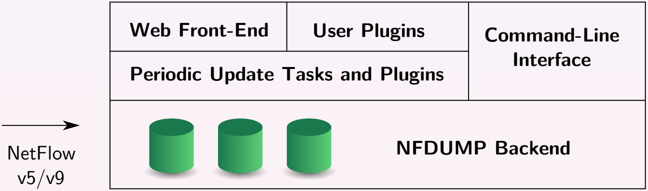




Date 2010/05/12 to 2010/05/12

VLAN ID 1200, 1203, 1300

```
Duration Proto      Src IP Addr:Port          Dst IP Addr:Port   Flags
   2.096 TCP     [illegible]:56956 ->        108.7.1.50:80      .AP.S.
   0.094 TCP     108.7.1.[illegible] ->   59.173.182.61:49442   .AP.S.
   0.368 TCP     108.7.1.50[illegible] -> 59.173.182.61:49440   .AP.S.
   0.737 TCP     [illegible]          ->  59.173.182.61:49434   .AP.S.
   0.379 TCP     108.7.1.50:[illegible] -> 59.173.182.61:49438  .AP.S.
   0.296 TCP     [illegible]          ->        108.7.1.50:80   .AP.S.
   0.575 TCP     59.173.182.61:4[illegible] ->  108.7.1.50:80   .AP.S.
   0.574 TCP     59.173.182.61:4[illegible] ->  108.7.1.50:80   .AP.S.
   0.451 TCP     [illegible]          ->        108.7.1.50:80   .AP...
   1.281 TCP     59.173.182.61:[illegible] ->   108.7.1.50:80   .AP.SF
   1.280 TCP     [illegible]          -> [illegible].233.173:41667 .AP.SF
   5.886 TCP     [illegible]9.173.182.61[illegible] -> [illegible].129:1687 .AP...
   6.051 TCP     [illegible]13.233[illegible]:1687 -> [illegible]:80 .AP...
   2.800 TCP       108.7.1.50:80       ->  210.[illegible]:56607 .AP.S.
   2.980 TCP     210.56.6.116:56607    ->  108.7.[illegible]     .AP.S.
   1.693 TCP       108.7.1.50:80       ->  157.242.141.1[illegible] [illegible]
   1.778 TCP       108.7.1.50:80       ->  157.242.141.183:132[illegible] [illegible]
   0.604 TCP     157.242.141.183:1325  ->        108.7.1.50:80   [illegible]
   1.990 TCP     157.242.141.183:1324  ->        108.7.1.50:80   .AP.S.
```



Web Front-End

User Plugins

Command-Line Interface

Periodic Update Tasks and Plugins

NetFlow v5/v9

NFDUMP Backend

- **NfSen – NetFlow Sensor** – http://nfsen.sf.net/
- **NFDUMP – NetFlow display** – http://nfdump.sf.net/

Methods for Data Analysis I

TCP SYN scanning detection

- Very simple, but effective general method.
- Reveals compromised hosts in our network.
- Very low false positive rate.

Honeypot monitoring

- Uses subnet allocated for high- and low-interaction honeypots.
- Eliminates false positives, mainly catches hosts from outside.
- Besides flow, passwords attempted by attackers are stored.

Methods for Data Analysis II

Brute force attack detection

- Online password guessing is ubiquituos, still a threat.
- Similar flows may be symptoms of this attack.
- Suitable even for encrypted services such as SSH.
- One attacker often aims to more targets $\Rightarrow$ easier detection.

Round trip time anomaly detection

- (D)DOSes overwhlem servers and increase response time.
- Abrupt increase of RTT may point to attack/misconfiguration.
- Number of incoming flows/packets is often correlated to RTT.

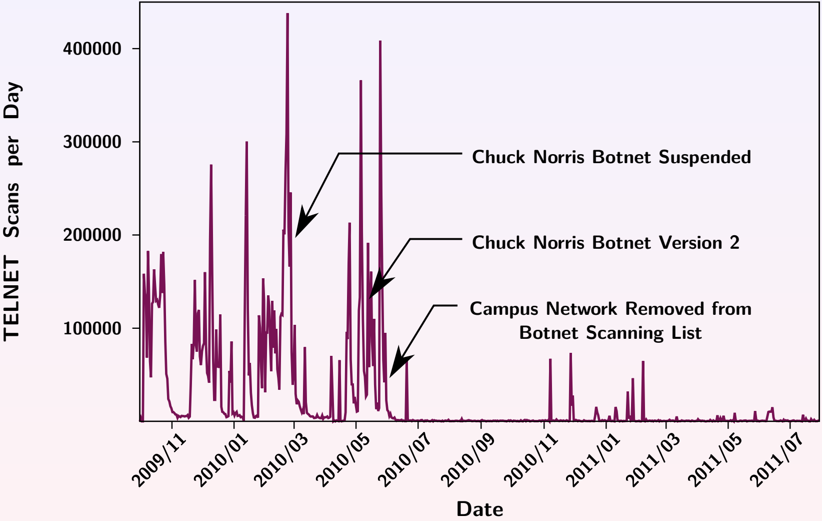
Chuck Norris Botnet in Nutshell

- **Linux malware** – IRC bots with central C&C servers.
- Attacks **poorly-configured** Linux **MIPSEL** devices.
- Vulnerable devices – **ADSL modems** and **routers**.

- Uses **TELNET brute force** attack as infection vector.
- Users are **not aware** about the malicious activities.
- **Missing** anti-malware **solution** to detect it.

Discovered at Masaryk University on 2 December 2009. The malware got the Chuck Norris moniker from a comment in its source code `[R]anger Killato : in nome di Chuck Norris !`

TELNET Malware Activities – 2009/11 - 2011/7



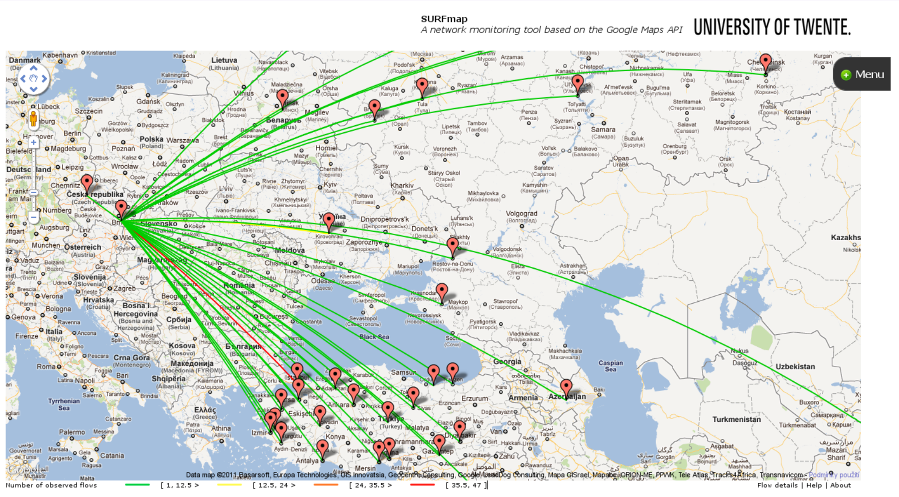
Chuck Norris Botnet Suspended

Chuck Norris Botnet Version 2

Campus Network Removed from Botnet Scanning List

Chuck Norris Will Never Die or Cyber War ?

TELNET scans against single host – 2011/10/20.



SURFmap
A network monitoring tool based on the Google Maps API

UNIVERSITY OF TWENTE.

Number of observed flows 🟩 [1, 12.5 > 🟨 [12.5, 24 > 🟧 [24, 35.5 > 🟥 [35.5, 47]

Menu
Black Sea
Caspian Sea
Türkiye (Turkey)
România (Romania)
Україна (Ukraine)
Беларусь (Belarus)
Polska (Poland)
Česká republika (Czech Republic)
Slovensko (Slovakia)
Magyarország (Hungary)
Moldova
България (Bulgaria)
Georgia
Armenia
Azerbaijan
Kazakhstan
Uzbekistan
Turkmenistan
Data map ©2011 Basarsoft, Europa Technologies, GIS Innovatsia, Geocentre Consulting, Google, LeadDog Consulting, Mapa GISrael, Mapabc, ORION-ME, PPWK, Tele Atlas, Tracks4Africa, Transnavicom - Podmínky použití
Flow details | Help | About

SURFmap – http://surfmap.sf.net

Part III

Flow-based Network Protection

Goals and Components

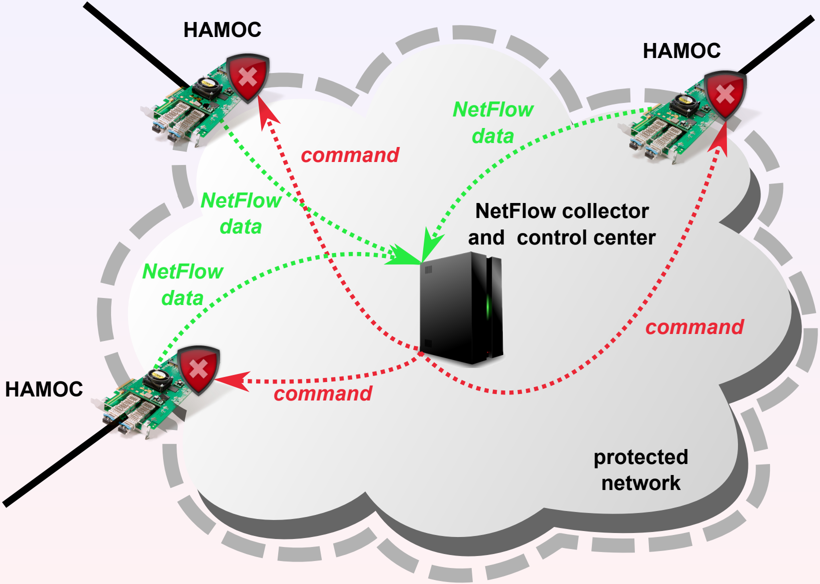
Goals of Network Protection

- Using **NetFlow data** to protect network.
- Defending perimeter against **attacks from outside**.
- **Automated** attack detection.
- Suitable for **high speed networks** (10 Gbps+).

System Parts

- Sensors (⇒ NetFlow data).
- Control center (⇒ commands).
- Active network components (⇒ blocking/filtering).
- HAMOC platform – both sensor and active component.

Architecture of Network Protection



Part IV

Integration with Early Warning Systems

Warden: Czech academic EWS

Client/server achitecture

- Security-related events are sent to the center.
- Clients (periodically) poll the center for new events.
- Events: port scanning, brute force attack, phishing, etc.
- Transport protocols: SOAP over HTTPS (+ SSL certificates)

Integration

- Control center also calls remote procedure to store a newly detected event.
- Events coming from center may trigger an action.
- Trustworthiness of participants is a key factor!

Part V

In Daily Operation

Computer Security Incident Response Team of MU

The **first university CSIRT** in the Visegrad Four listed and accredited in the **Trusted Introducer** public database.

Provided services:

- Incident handling and response (and its coordination).
- **Intrusion detection** based on NetFlow probes and honeypots.
- Network policy checks and network analysis (e. g., reverse DNS records, live IPs, accounting, . . .).
- User education, alerts&warning: security advisories and bulletins.

Constituency: tens of thousands of university students and staff.

Part VI

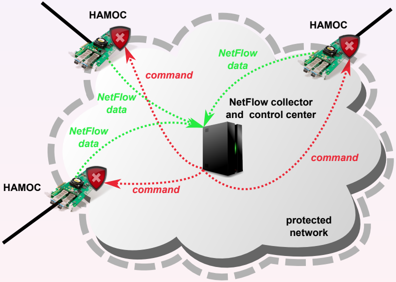
Conclusion

Conclusion

- Flow-based network protection is suitable for large networks.
- Online network monitoring contributes to the overall security.
- Early warning systems may profit from flow-based detection.
- Automated network protection based solely on the EWS may be dangerous.

Thank you for your attention!

Network Security @ ICS MU



Jan Vykopal

vykopal@ics.muni.cz

Project CYBER
http://www.muni.cz/ics/cyber

CSIRT-MU
http://www.muni.cz/csirt