Automatic Network Protection Scenarios Using NetFlow

Vojtěch Krmíček, Jan Vykopal

{krmicek|vykopal}@ics.muni.cz

FloCon 2012
January 9-12, Austin, Texas

Part I

Flow-based Network Protection

Goals and Components

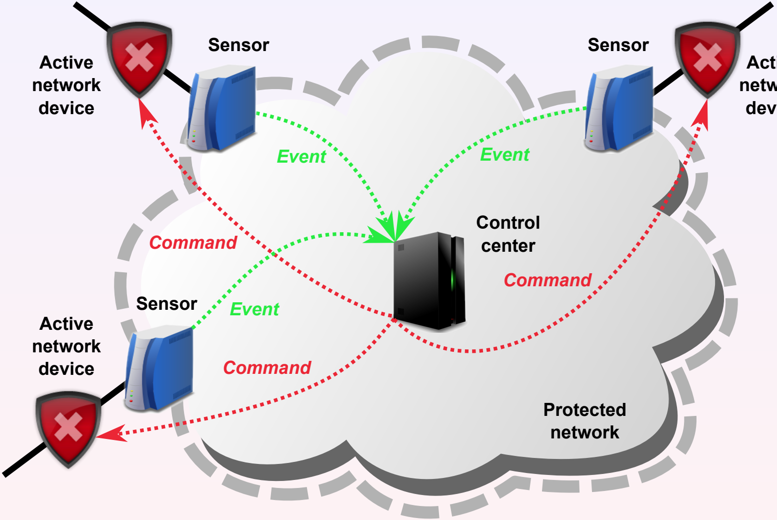
Goals of Network Protection

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

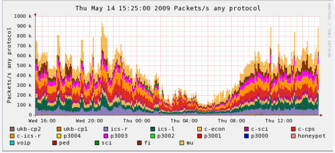
System Parts

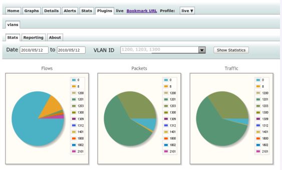
- Sensors (⇒ NetFlow data).
- Control center (⇒ commands).
- Active network components (⇒ blocking/filtering).
- HAMOC platform – both sensor and active component.

General Architecture of Network Protection

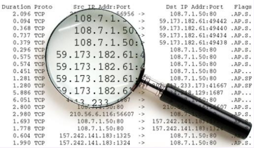


NfSen/NFDUMP Collector Toolset Architecture

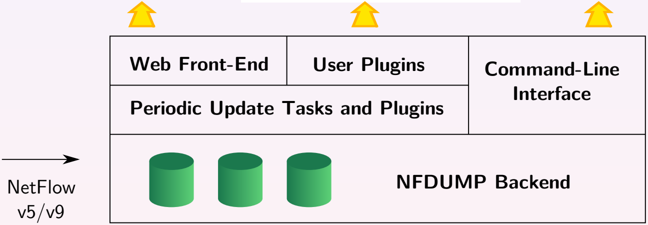




Date 2010/05/12 to 2010/05/12 VLAN ID 1200, 1203, 1300



```
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       108.7.1.50[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       59.173.182.61:[illegible] -> 108.7.1.50:80     .AP.S.
   0.575 TCP       59.173.182.61:[illegible] -> 108.7.1.50:80     .AP.S.
   0.574 TCP       59.173.182.61:[illegible] -> 108.7.1.50:80     .AP.S.
   0.451 TCP       59.173.182.61:[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       59.173.182.6[illegible] -> [illegible].248.129:1687 .AP...
   6.051 TCP       [illegible].233.[illegible]87 -> [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.
```



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

Methods for Data Analysis

TCP SYN scanning detection

- Simple, effective general method, low false positive rate.

Honeypot monitoring

- Uses subnet allocated for high- and low-interaction honeypots.
- Eliminates false positives, mainly catches hosts from outside.

Brute force attack detection

- Similar flows may be symptoms of this attack.
- Suitable even for encrypted services such as SSH.

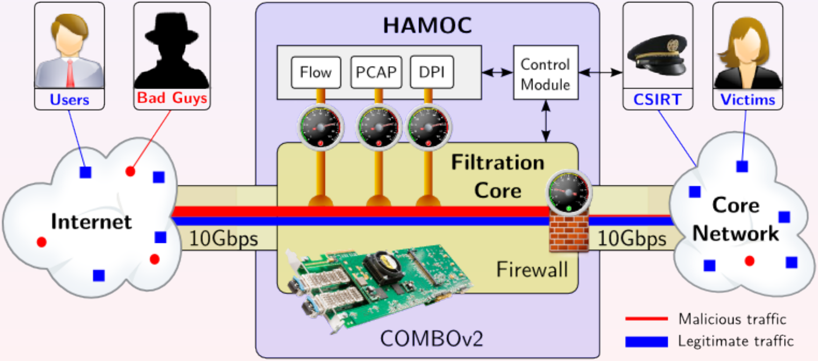
Round trip time anomaly detection

- (D)DOSes overwhelm servers and increase response time.
- Abrupt increase of RTT may point to attack/misconfiguration.

HAMOC Hardware Platform

Features

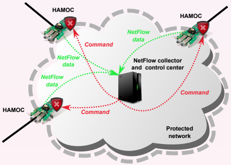
- Traffic distribution among multiple CPU cores.
- Network applications with hardware acceleration.
- Capable of concurrent monitoring/blocking/filtering/etc.
- Low-speed networks – SW alternative (NetFlow/iptables).

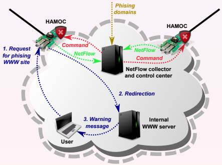


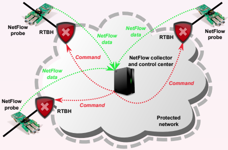
Network Protection – Deployment Scenarios

Scenarios

- NetFlow probes + control center + **RTBH**[1] filtering
- HAMOC as NetFlow probe and **firewall**
- HAMOC as **redirection to quarantine** (phishing)
- HAMOC as NetFlow probe and **active attack tool**
- HAMOC as NetFlow probe and **traffic limiter**





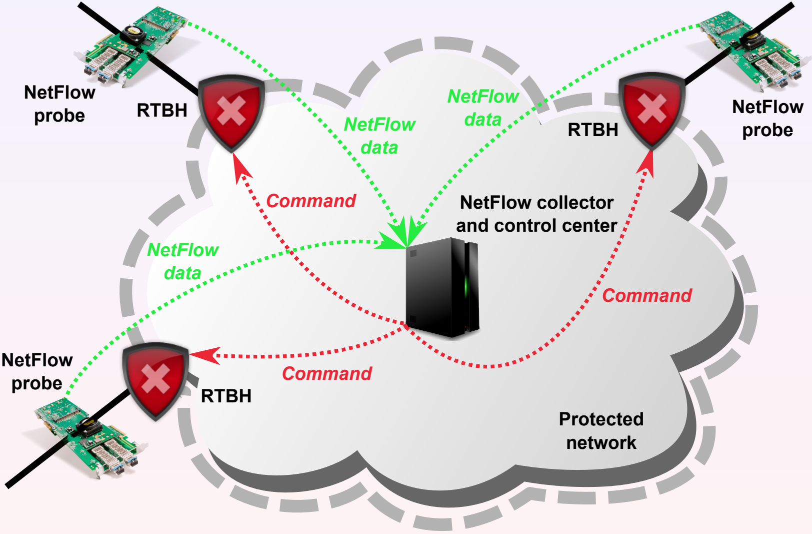


[1] Remote Triggered Black Hole

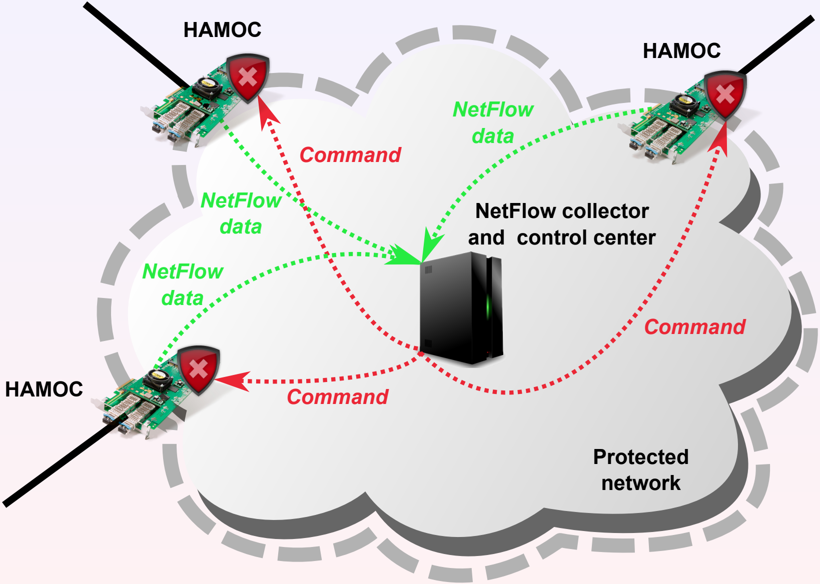
Part II

Network Protection Scenarios

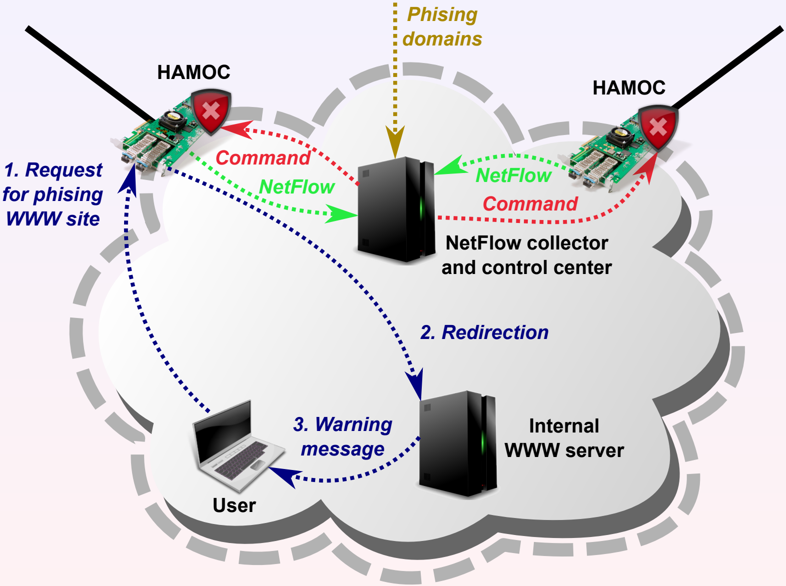
NetFlow Probes + Control Center + RTBH Filtering



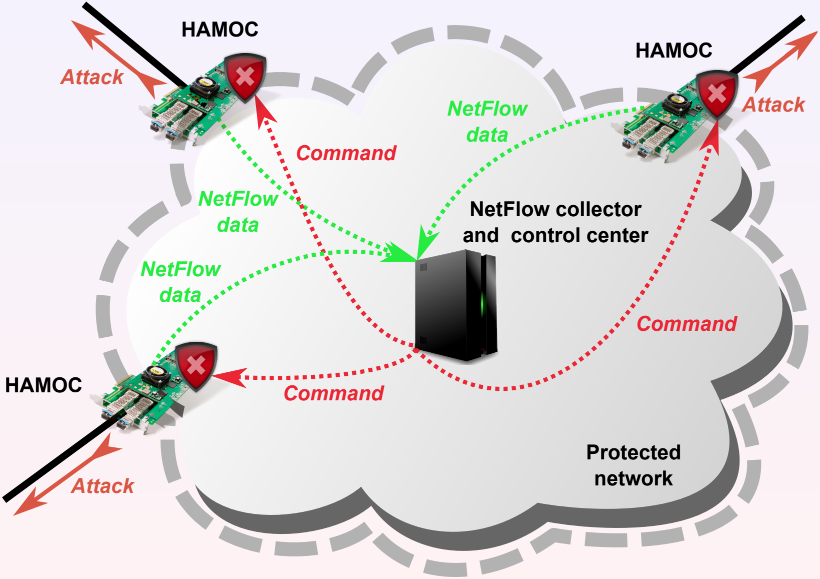
HAMOC as NetFlow Probe and Firewall



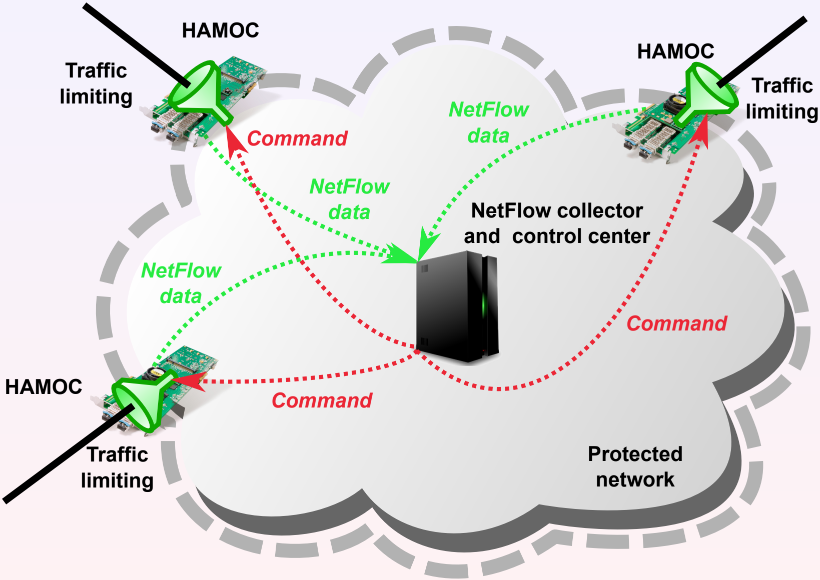
HAMOC as Redirection to Quarantine (Phishing)



HAMOC as NetFlow Probe and Active Attack Tool



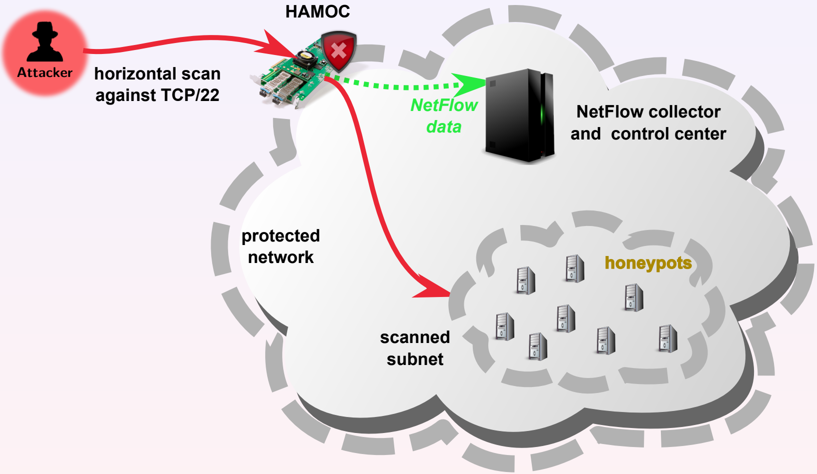
HAMOC as NetFlow Probe and Traffic Limiter



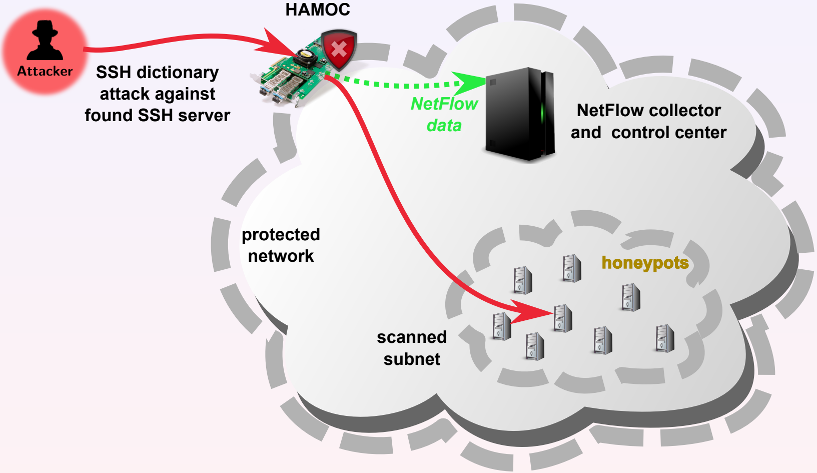
Part III

Network Protection Use Case: SSH Dictionary Attack and HAMOC Firewall

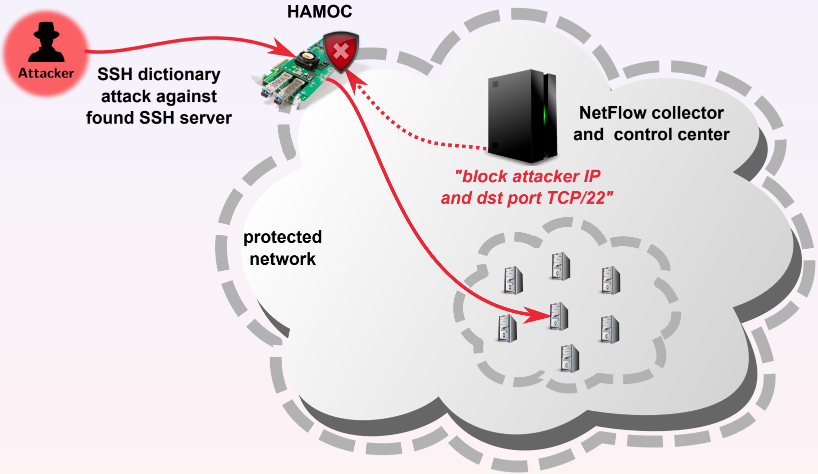
I. Attacker Performs SSH Horizontal Scan



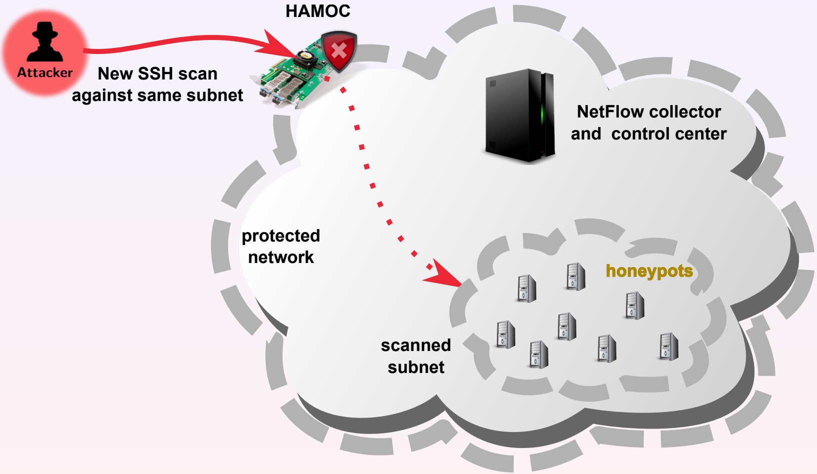
II. Attacker Starts SSH Dictionary Attack


HAMOC
Attacker
SSH dictionary attack against found SSH server
NetFlow data
NetFlow collector and control center
protected network
honeypots
scanned subnet

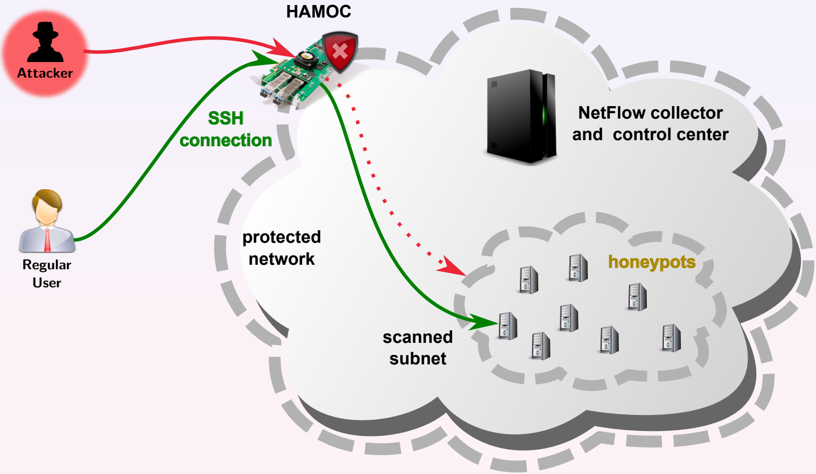
III. Center Detects Attack/Inserts Blocking Rule


HAMOC
Attacker
SSH dictionary attack against found SSH server
NetFlow collector and control center
"block attacker IP and dst port TCP/22"
protected network

IV. New SSH Attack, Blocked at the Border


HAMOC
Attacker
New SSH scan against same subnet
NetFlow collector and control center
protected network
honeypots
scanned subnet

V. Regular User Can Access Network, Attacker Not



Part IV

Conclusion

Conclusion

Role of IP Flow Monitoring in High Speed Networks

- Flow-based monitoring **suitable for large networks**.
- Observe and **automatically inspect 24x7** network data.
- Possible future deployment in **10Gbps/40Gbps/100Gbps networks**.

Automatic Network Protection

- Class of attacks can be detected **automatically**.
- Automatic network protection **supports operators**.
- Detect and block attacks **before hosts are infected**.
- Not usable in every situation – **limitations**.

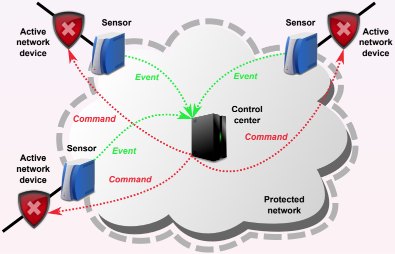
Thank you for your attention!

Automatic Network Protection Scenarios Using NetFlow

Vojtěch Krmíček et al.

{krmicek|vykopal}@ics.muni.cz

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



This material is based upon work supported by the
Czech Ministry of Defence under Contract No. OVMASUN200801.