
CCDCOE
NATO Cooperative Cyber Defence
Centre of Excellence
Tallinn, Estonia
CyCon
International Conference
on Cyber Conflict

CCDCOE
NATO Cooperative Cyber Defence Centre of Excellence
Tallinn, Estonia

CyCon
International Conference on Cyber Conflict
30 MAY - 2 JUNE 2017, TALLINN, ESTONIA

Early detection of internal cyber threats

Fabio Pierazzi
Postdoctoral Researcher
University of Modena and Reggio Emilia, Italy

Presentation of paper:
"Scalable architecture for online prioritization of cyber threats"
F. Pierazzi, G. Apruzzese, M. Colajanni, A. Guido, M. Marchetti

Defending enterprise networks

- **Perimetral network defenses** are commonly adopted to protect the border

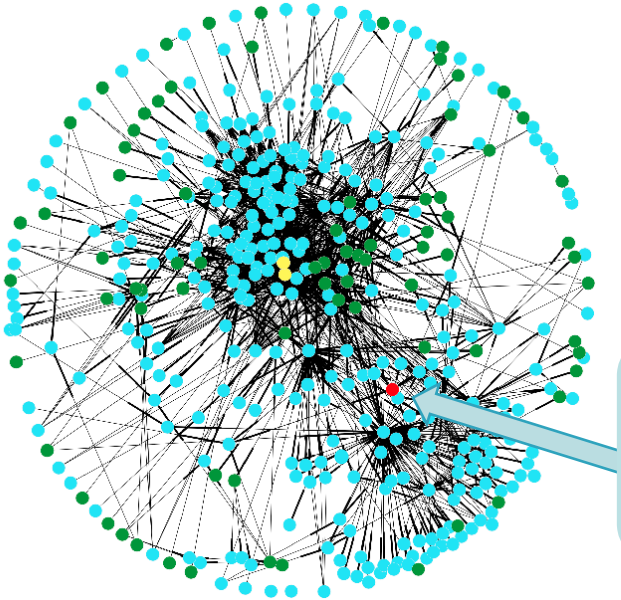
- Limited solutions exist for **defending the core** of a network, once the attacker gets in
  - Once a host is compromised, the attacker may perform Reconnaissance, data transfer to dropzone, Man in the Middle, Watering hole, Lateral movement, Pivorting, …

Some examples of cyber attacks to internal networks:

- Operation Aurora (2010--)
- Operation Night Dragon (2011--)
- BlackEnergy (2015)
- MEDJACK (2016)
- Archimedes (2017),…

Defending the network core

Graph of internal communications
(**real data** from department of large organization)



= department hosts

= DNS servers

= other departments

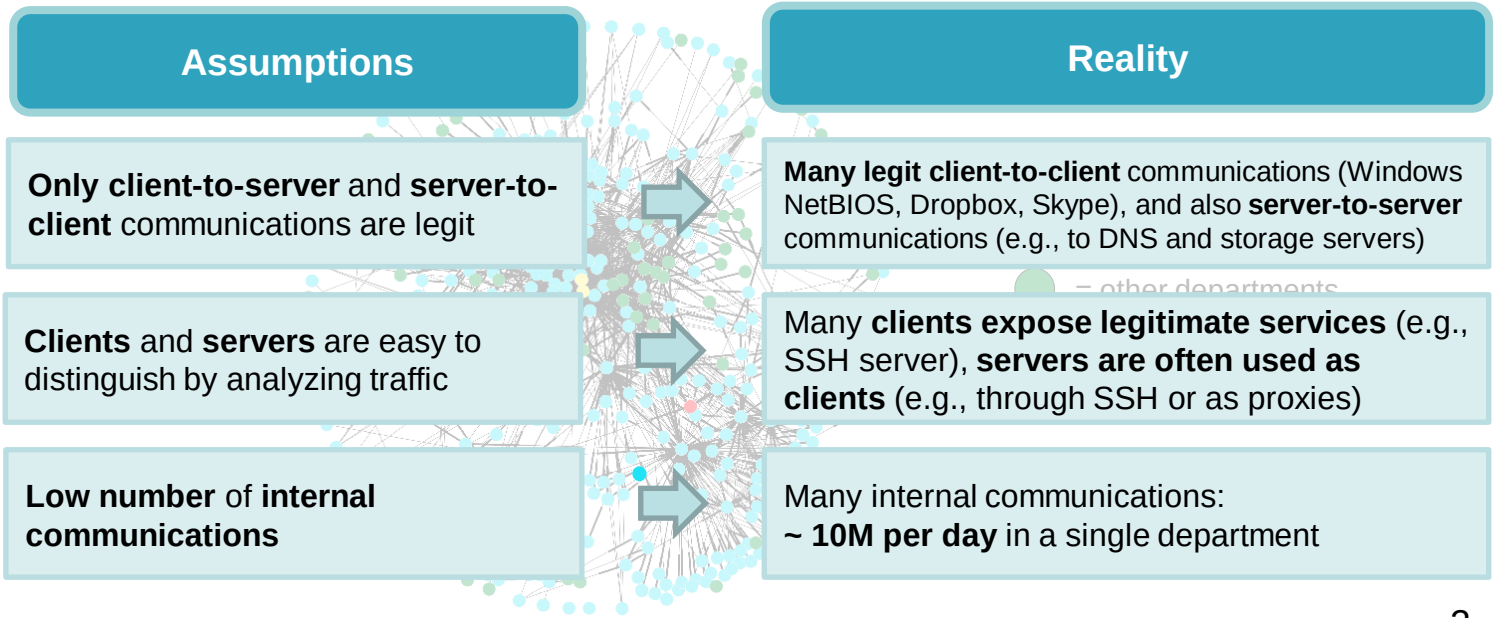
Final objective:
To identify the **one or few host** that are performing malicious activities

CCDCOE
NATO Cooperative Cyber Defence Centre of Excellence Tallinn, Estonia

CyCON
International Conference on Cyber Conflict
30 MAY - 2 JUNE 2017, TALLINN, ESTONIA

Defending the network core

Graph of internal communications
(real data from department of large organization)



Key aspects of proposal

A **Multi-layer analysis** vs. single-layer analysis

Consider **different layers** **(i.e., perspectives)** of network traffic (e.g., packets, bytes, DNS resolutions,…)

- To **correlate** different events
- To improve **accuracy**

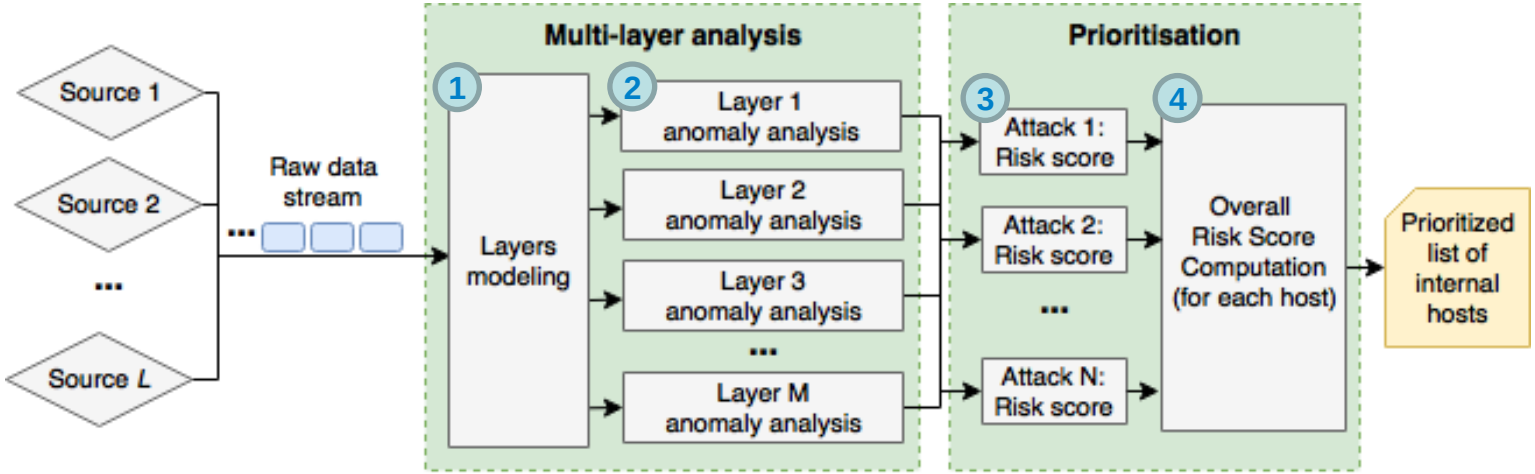
B **Prioritisation** vs. detection

Certain "detection" is almost **impossible**

Instead, we propose **prioritisation**

- **Risk score**: likelihood that a host is involved in one or more internal attacks
- **Security experts** can **investigate** the most suspicious hosts

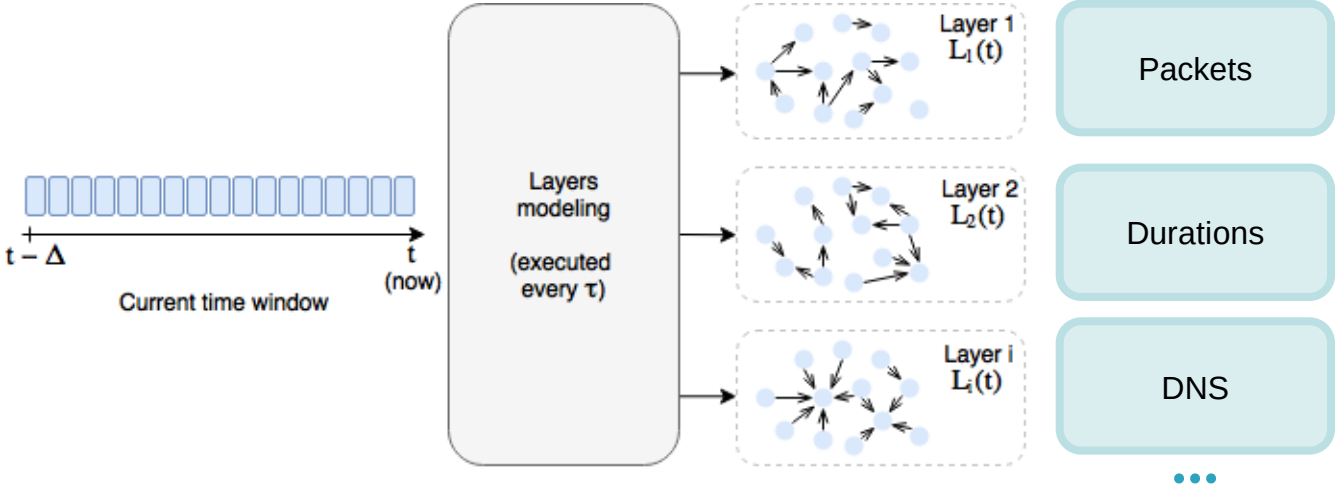
Overview


Source 1
Source 2
...
Source L
Raw data stream
Multi-layer analysis
1
Layers modeling
2
Layer 1 anomaly analysis
Layer 2 anomaly analysis
Layer 3 anomaly analysis
...
Layer M anomaly analysis
Prioritisation
3
Attack 1: Risk score
Attack 2: Risk score
...
Attack N: Risk score
4
Overall Risk Score Computation (for each host)
Prioritized list of internal hosts

Multi-layer analysis

Phase 1: Layers modelling

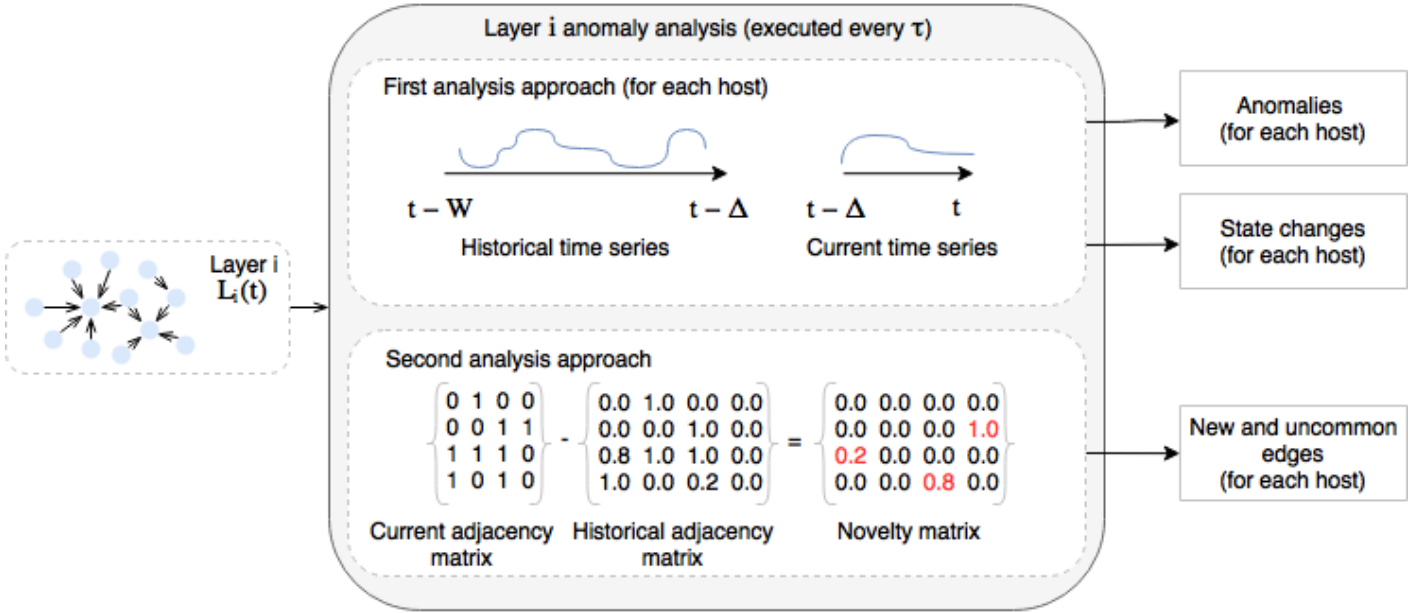
Layers: graphs of **different network metrics**
→ *Look at data from different perspectives*



Multi-layer analysis

Phase 2: Anomaly analysis

Performed **in parallel** **for each layer**



Prioritisation

Phase 3: Attacks risk scores

The **outputs** of the Multi-Layer analysis are **correlated** to provide a **risk score** for different types of **internal cyber attacks** (for each host)

R: Reconnaissance

DTD: Data Transfer to Dropzone

MITM: Man in the Middle through ARP spoofing

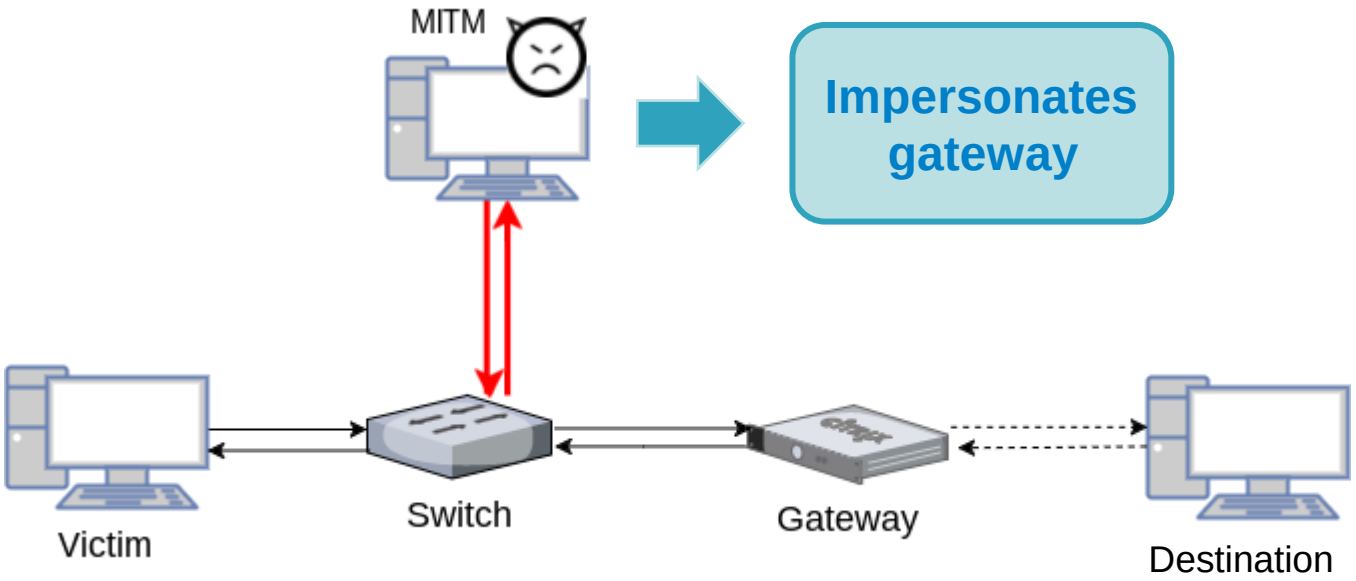
WH: Watering Hole through DNS spoofing

LM: Lateral Movement Through Pivoting

Prioritisation

Man in the Middle

- Attacker intercepts (possibly manipulates) all victim communication
- **ARP spoofing**: no evidence in IP communications from victim IP



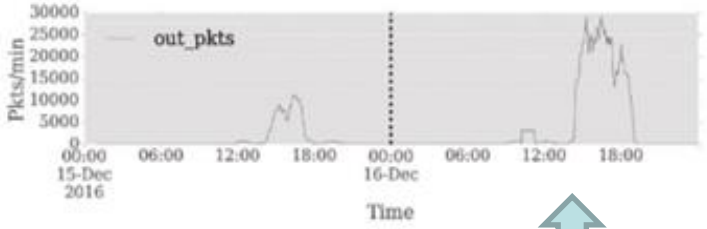
Prioritisation

Man in the Middle – Risk score

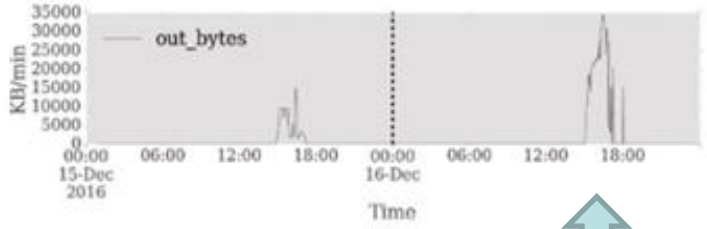
- **Number of contacted hosts** remains **stable**
- **New correspondence IP-MAC** in the **ARP** layer
- **Packets** and **bytes** are **duplicated** in the **switch**

→ possible to capture via **state-change analysis**

Packets



Bytes



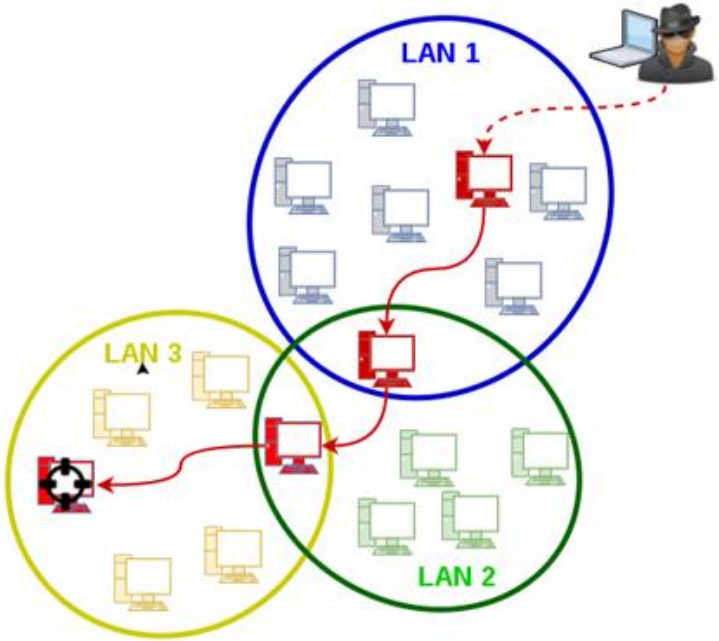
State-change
detected by Phase 2

Prioritisation

Lateral Movement through Pivoting

Once he compromises a host, attacker wants to **move deeper** in the internal network

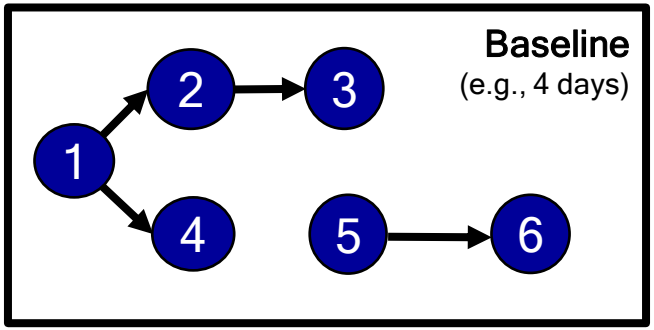
Pivoting is a technique where an attacker **propagate commands** through two or more internal hosts

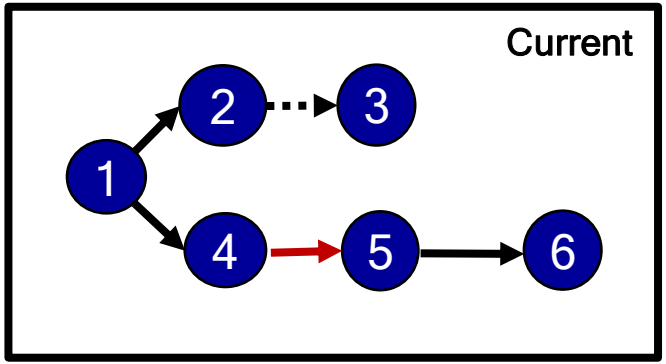


Prioritisation

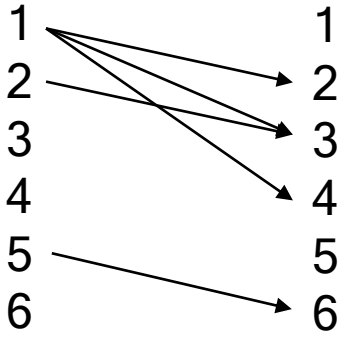
Lateral Movement – Risk score

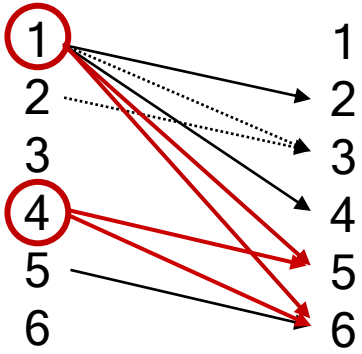
Baseline vs. Current





Reachability graphs



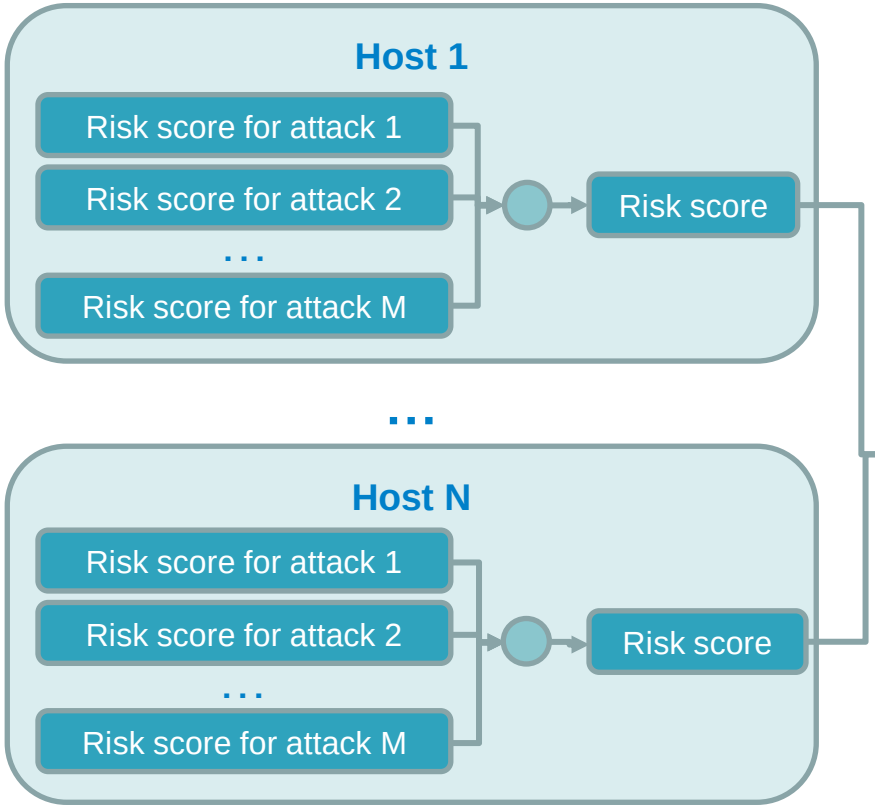


Score intuition: sudden increase in **reachable destinations** + **duration**

Hosts 1 and 4 have increased the number of reachable destinations

Prioritisation

Phase 4: Overall risk score



Prioritized internal hosts

Rank	Host ID	Risk Score
1	**h128**	321
2	**h32**	312
3	**h18**	130
4	**h384**	120
5	**h748**	89
…	…	…

Prioritisation – Results

Injection of **Man in the Middle** of increasing duration

In top-K	15-30min	1-2hr	12-24hr	24-72hr
in top-5	89.8%	98.2%	99.4%	99.8%
in top-10	95.4%	99.1%	99.8%	100%
in top-25	99.0%	99.8%	100%	100%
in top-50	99.7%	100%	100%	100%

Injection of **lateral movement** with different number of hosts involved

In top-K	1 pivoter	3-5 pivoters	8-10 pivoters
in top-5	96.2%	99.7%	99.9%
in top-10	97.9%	99.9%	100%
in top-25	99.1%	100%	100%
in top-50	99.8%	100%	100%

Conclusions

- Protecting enterprise networks is **increasingly challenging**
- Novel approaches for **defending the core** are needed
- **Key proposals**:
  - Correlate **multiple layers** to find (internal) cyber threats
  - **Prioritisation** instead of detection

CCDCOE
NATO Cooperative Cyber Defence Centre of Excellence
Tallinn, Estonia

CyCon
International Conference on Cyber Conflict
30 MAY - 2 JUNE 2017, TALLINN, ESTONIA

Questions & Answers

Fabio Pierazzi
University of Modena, Italy
fabio.pierazzi@unimore.it