Towards Predicting Cyberattacks in Large-Scale Systems

Dr. Edward Chuah

University of Aberdeen, UK

Outline of presentation

- Recent research in understanding network attacks:
  - Challenges in identifying network attacks using NetFlow data.
  - An empirical study of reflection attacks using NetFlow data.
- Research project on predicting cyberattacks in large networks.
- Q&A.

Recent research 1: Identifying network attacks using NetFlow data

E. Chuah, et. al., "*Challenges in Identifying Network Attacks Using NetFlow Data*", in Proceedings of IEEE International Symposium on Network Computing and Applications (NCA), 2021.

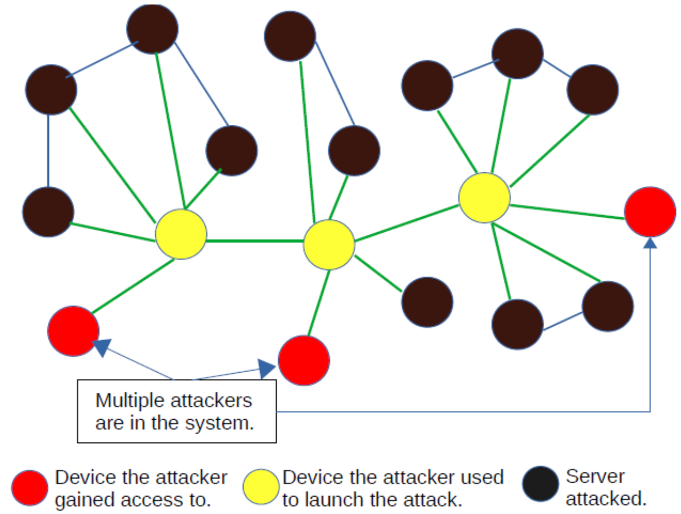
- Background:
  - To better support the processes of attack mitigation, it is helpful to first understand how an attack transpires in practice.
  - Analyzing attacks in any large-scale or complex network require awareness of the sequence of events which lead to an attack. The ***time elapsed between the precursor event and an attack is defined as the lead time***.
  - State-of-the-art approaches have focused on analyzing the security of specific network protocols. However, few works consider the full network software stack to design better attack detection frameworks.

Motivating example

- Multiple attackers may try to compromise a number of hosts and non-attackers may also be attempting to access the hosts. If we assume that a network is composed of multiple hosts, then simultaneous attacks can be defined via correlated events.

- For example, a firewall may be configured to allow port 22 traffic to allow the server to connect to other servers. An attacker can take advantage of such a rule to execute a reflection attack. The events associated with such a reflection attack can occur together in time and target servers in different locations.

- We define:
  - **Temporal correlation** as events which occur together during the same time period and differ in location,
  - **Spatial correlation** as events which occur in the same location and differ in time.



Intuition for simultaneous attacks.

Correlation analysis approach

- We developed a correlation analysis approach that:
  - Traced the events from the source device to the destination device in the netflow data. This included the time of the network events. Correlated the times of the network events to ascertain any network-wide influence evident over multiple dates.
  - Correlated the destination ports in the netflow data to ascertain any abnormal network events over multiple dates. Investigated the requests on the network ports to identify an attack.

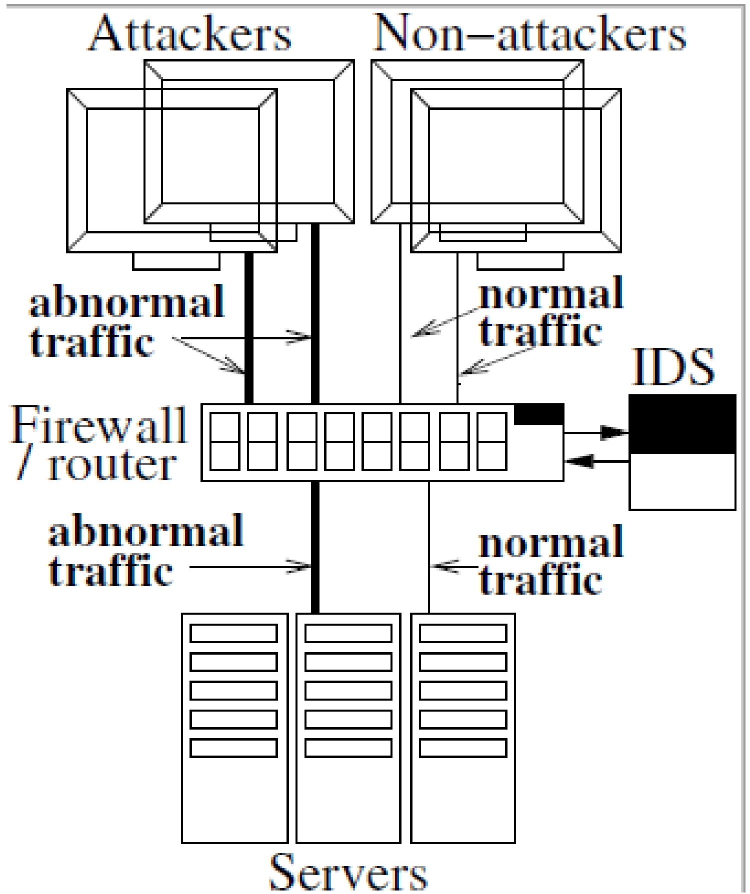


Illustration of the network data collection process.

NetFlow data

- The NetFlow protocol collects IP packets as they flow in and out of a network interface such as a router.

An IP flow record

761, 4434, Comp132598, Comp817788, 6, Port12597, 22, 89159,
85257, 15495068, 69768940

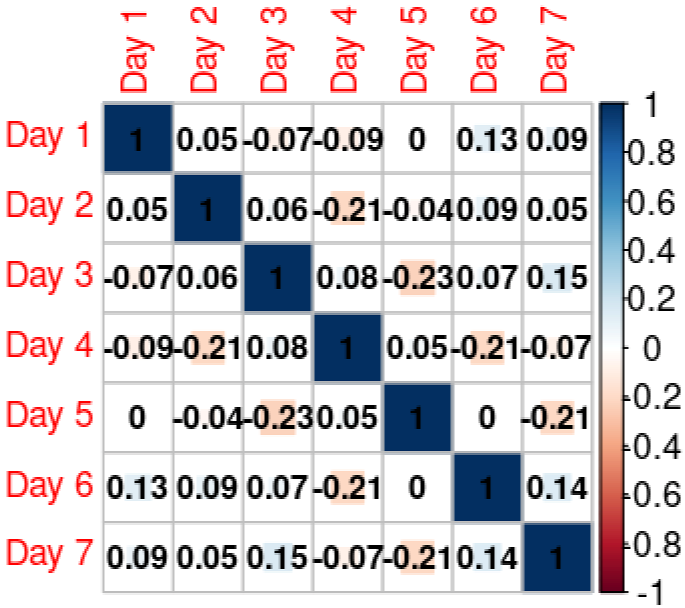
S/N	Description	S/N	Description
1	Start time of the event in epoch format.	7	Port used by the destination device.
2	Duration of the event in seconds.	8	Number of packets the source device sent during the event.
3	Device that likely initiated the event.	9	Number of packets the destination device sent during the event.
4	Receiving device.	10	Number of bytes the source device sent during the event.
5	Protocol number.	11	Number of bytes the destination device sent during the event.
6	Port used by the source device.		

NetFlow data analyzed

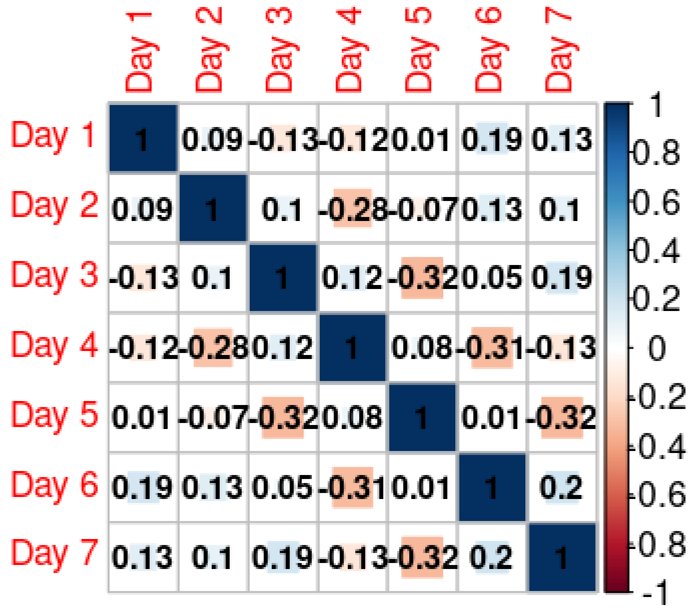
- Enterprise network operated by Los Alamos National Laboratories.
- 60,000 devices (includes hosts, servers and clients).
- Randomly selected 14 days worth of NetFlow data.
- Average 220 million NetFlow records in one day's worth of NetFlow data.
- Dataset is available online at: https://csr.lanl.gov/data/2017/

Phase 1: Temporal correlation

- Goal: To identify dates of a network attack.
  - We correlate the counts of netflow records by their start times on one date to the counts of netflow records by their start times on another date.
  - We apply Pearson and Spearman-Rank correlation algorithms.



Pearson correlation score, Week 1.



Spearman-Rank correlation score, Week 1.

The network events are weakly correlated between all seven days in Week 1, indicating that correlating the dates of the network events by time did not identify dates of an attack.

Phase 2: Spatial correlation

- Goal: To identify dates of a network attack.
  - We correlate the netflow records by their destination port counts on one date to the netflow records by their destination port counts on another date.
  - We apply Pearson and Spearman-Rank correlation algorithms.

Pearson correlation score, Week 1.

Pearson correlation score, Week 3.

A strong positive correlation was obtained for 2 days in Week 1 and 3 days in Week 3.

All the strongly positive correlation coefficients were tested using statistical significance tests. We determined that it is highly unlikely these results would be observed under the null hypothesis.

Phase 3: Identify network attacks

- Goal: To identify the type of attack on day 3 and 4 in Week 1, and day 3, 4 and 7 in Week 3.
  - When a NetFlow record contains the same source and destination device identifiers, it indicates that a reflection attack had occurred.

Reflection attacks on SSH servers

TABLE I
PORT 22 REQUESTS.

Week 1				
Day	Source device	Destination device	Source packets	Destination packets
3	5	4	19	2427
4	6	3	74	9852
Week 3				
Day	Source device	Destination device	Source packets	Destination packets
3	4	4	65	8731
4	4	5	29	2468
7	1	1	6	302

- 0.0005% of destination packets.
- 0.00001% of source packets.

Reflection attacks on DNS servers

TABLE II
PORT 53 REQUESTS.

Week 1				
Day	Source device	Destination device	Source packets	Destination packets
3	2	2	582	58449
4	2	3	65	5131
Week 3				
Day	Source device	Destination device	Source packets	Destination packets
3	4	4	90	6975
4	6	4	146	11735
7	3	3	28	3224

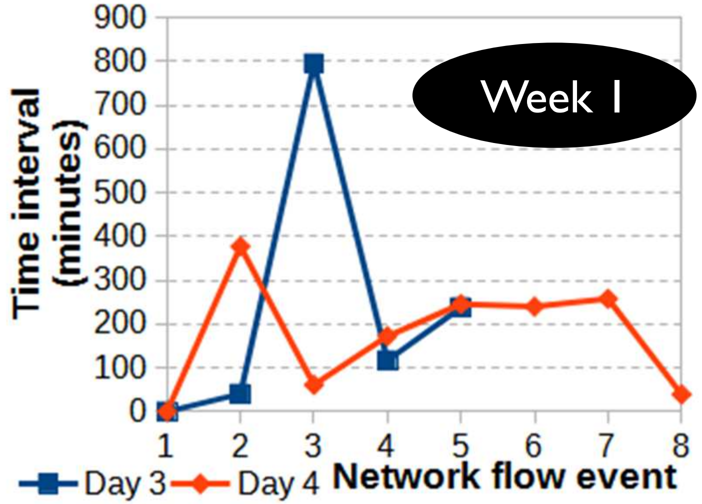
- 0.004% of destination packets.
- 0.00013% of source packets.

Phase 4: Obtain lead times of the attack

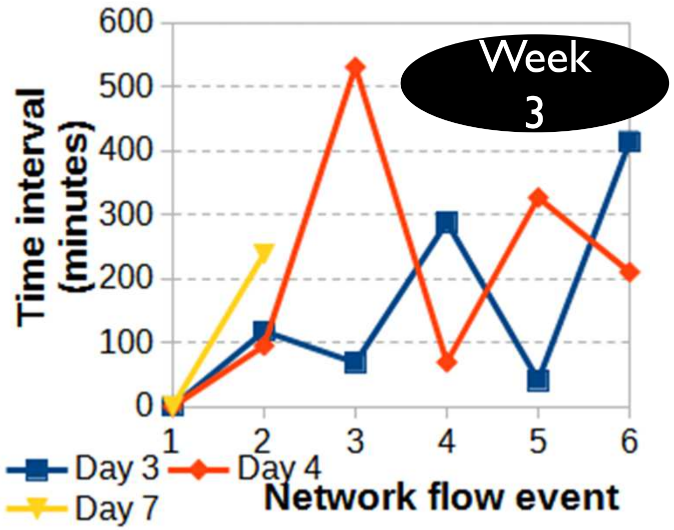
- Goal: To obtain the lead time of an attack. A lead time is defined as the time interval between two NetFlow records.

Reflection attack on the SSH server

- In Day 3 Week 1, the shortest time interval is 40 minutes and the longest time interval is 795 minutes.
- In Day 4 Week 1, the shortest time interval is 39 minutes, and the longest time interval is 377 minutes.



- In Day 3 Week 3, the shortest time interval is 41 minutes and the longest time interval is 415 minutes.
- In Day 4 Week 3, the shortest time interval is 69 minutes, and the longest time interval is 531 minutes.
- In Day 7 Week 3, the time interval is 239 minutes.

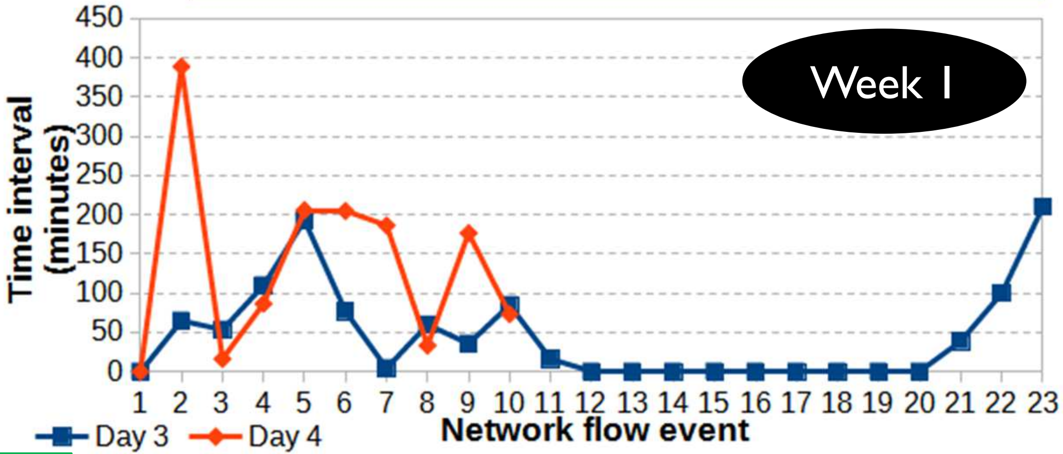


The minimum lead time range from 39 minutes to 239 minutes.

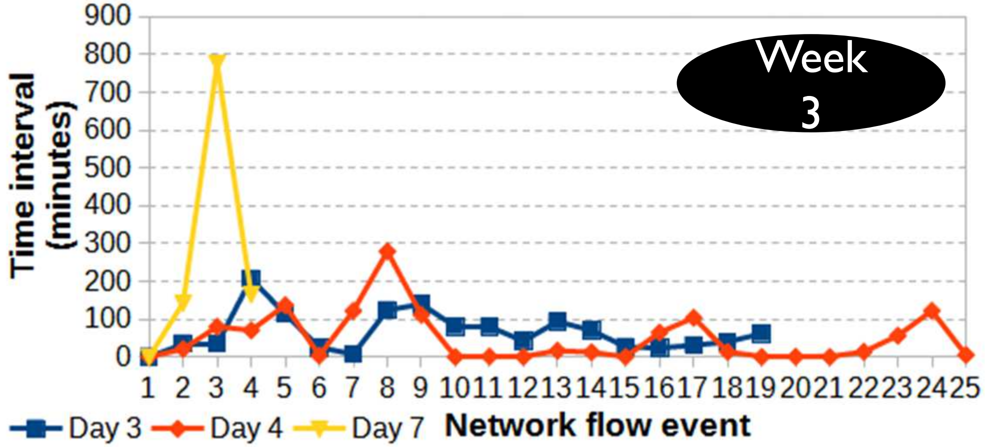
Phase 4: Obtain lead times of the attack (cont'd)

Reflection attack on the DNS server

- In Day 3 Week 1, the shortest time interval is 4 minutes and the longest time interval is 210 minutes.
- In Day 4 Week 1, the shortest time interval is 16 minutes, and the longest time interval is 389 minutes.



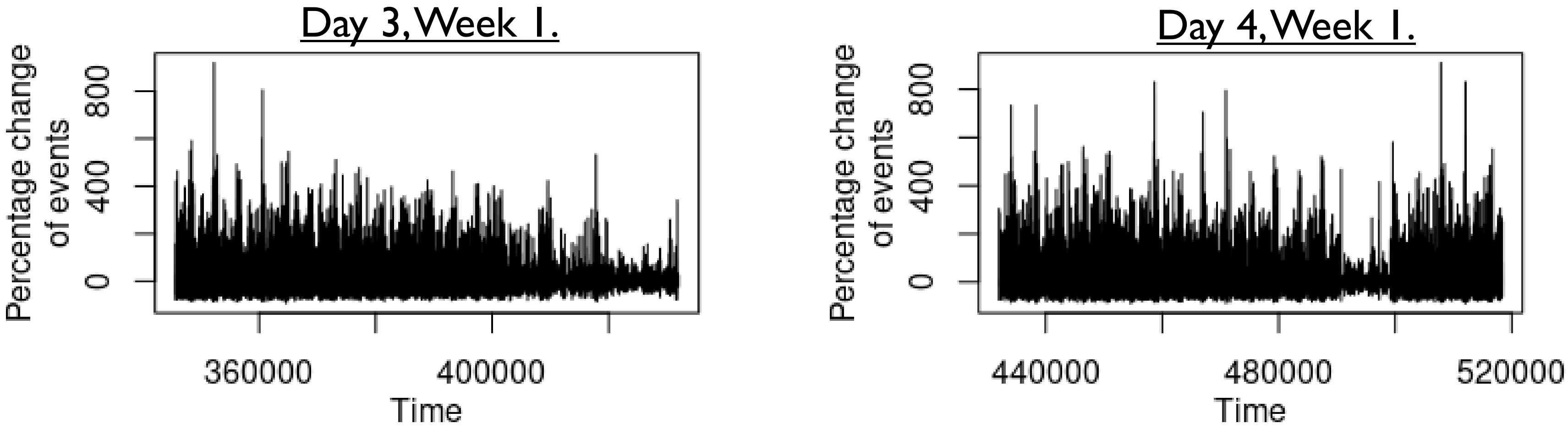
- In Day 3 Week 3, the shortest time interval is 7 minutes and the longest time interval is 207 minutes.
- In Day 4 Week 3, the shortest time interval is 1 minutes, and the longest time interval is 279 minutes.
- In Day 7 Week 3, the shortest time interval is 143 minutes, and the longest time interval is 777 minutes.



The minimum lead time range from 1 minute to 143 minutes.

Phase 4: Obtain lead times of the attack (cont'd)

- We observed that the times of some reflection attacks coincided with large percentage increase in NetFlow records. The times of other reflection attacks coincided with smaller increases in NetFlow records.



- Start times of the reflection attacks on the SSH servers in Week 1:
  - Day 3, Week 1: 353365th to 424737th second.
  - Day 4, Week 1: 433647th to 517197th second.
- Start times of the reflection attacks on the DNS servers in Week 1:
  - Day 3, Week 1: 349522th to 412427th second.
  - Day 4, Week 1: 434754th to 517123th second.

This implies that a large increase of NetFlow records can reveal a reflection attack, but it may also miss other reflection attacks.

Discussion

- We showed that a correlation analysis approach is unsuitable as a means of identifying network attacks.
  - The fact that the majority of NetFlow records are not the primary indicators of an attack is not obvious, for example, an increase in NetFlow records does not necessarily indicate an attack.
  - NetFlow data containing the time of an attack and malicious events imply that a comprehensively labeled cyber-security dataset is important.

- We observed that the traffic generated by the SSH and DNS reflection attacks did not overwhelm the servers.
  - Nonetheless, it is important to equip the IDS and attack predictors to be aware of early signs of an attack to reduce service downtime.

- These recommendations are suitable for diverse networks, since they can also benefit from NetFlow data analysis.

Recent research 2: Empirical study of reflection attacks

E. Chuah and N. Suri, "*An Empirical Study of Reflection Attacks Using NetFlow Data*", Cybersecurity, 2024.

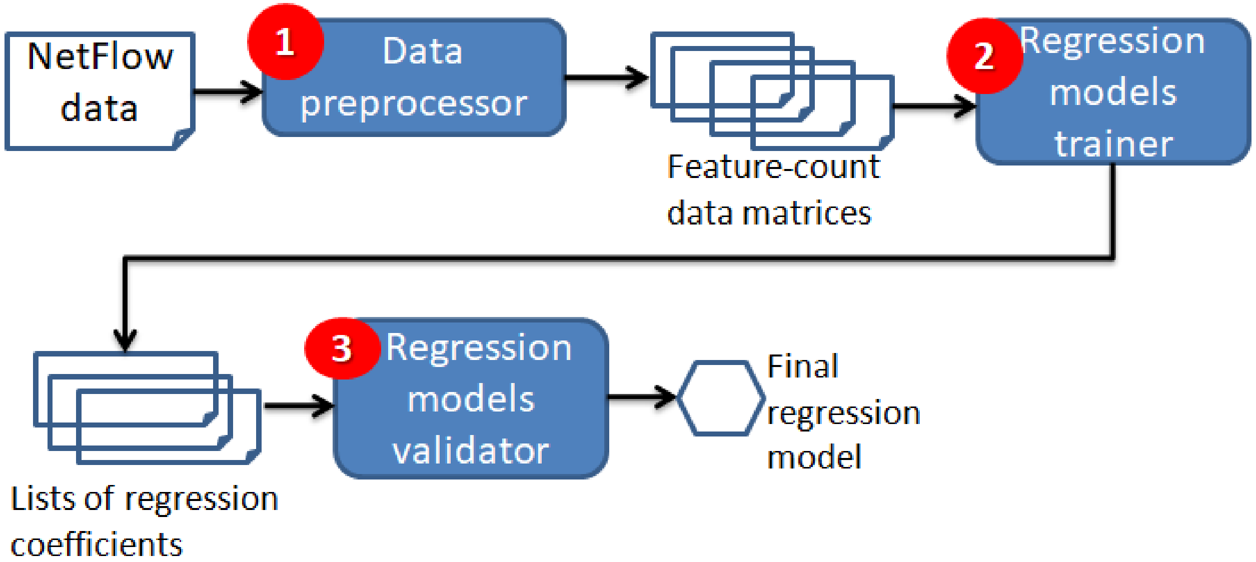
- We have shown that reflection attacks exist in the NetFlow data.
- Several recent works have developed Pearson correlation-based techniques to detect Distributed Denial-of-Service (DDoS) attacks, detect activities of groups of botnets, and detect network intrusions.
- Pearson correlation has some limitations:
  - Only identifies relationships between 2 samples.
  - Security analyst must manually analyze all the correlated samples to identify an attack.
  - Manual analysis is a time-consuming process and incurs a significant delay in identifying correlations of an attack.

Contributions

- We identified reflection attacks on the NetBIOS server and Network Time Protocol (NTP) servers in the NetFlow data obtained from a large enterprise network operated by Los Alamos National Laboratories.
- We provided estimates of reflection attacks on the NetBIOS servers and NTP servers which are not correlated.
- We discussed how our findings can be used to improve the network's security against reflection attacks.
- We obtained the dwell times of reflection attacks on the NTP and NetBIOS servers.

Identifying correlations of reflection attacks

Objective: To determine if reflection attacks are correlated or not correlated.



Research problem:

- Identify the NetFlow records which are assigned the largest positive regression coefficients or the smallest regression coefficients by the regression model.
- Identify devices that are associated with a reflection attack and obtain the amount of traffic generated by the attack.
- Identify the time elapsed between the start times of 2 adjacent NetFlow records which are associated with the reflection attack.

NetFlow data analyzed

- Conducted a comprehensive analysis of 1.7 billion NetFlow records obtained from a large enterprise network operated by Los Alamos National Laboratories.
- 1 day's worth of NetFlow data contains an average of 220 million NetFlow records.
- We randomly selected 8 days worth of NetFlow data for analysis.
- We identified NetFlow records that are associated with reflection attacks on the NetBIOS and NTP servers.

Phase 1: Identify correlations of reflection attacks

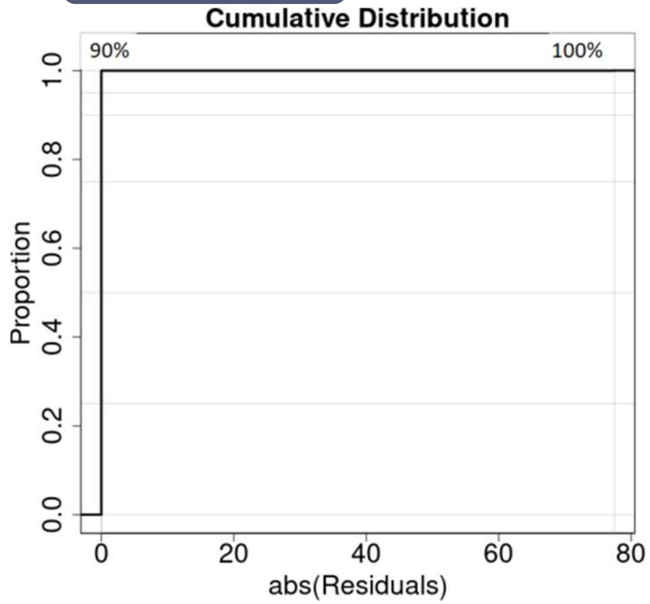
NTP servers

Day 1 ($n = 41125$)				Day 2 ($n = 90891$)			
Metric	Ridge	ENet	LASSO	Metric	Ridge	ENet	LASSO
R^2	0.02	0.02	0.02	R^2	0.05	0.07	0.01
Adj. R^2	0.02	0.02	0.02	Adj. R^2	0.05	0.07	0.01
Day 3 ($n = 88800$)				**Day 4** ($n = 113804$)			
Metric	Ridge	ENet	LASSO	Metric	Ridge	ENet	LASSO
R^2	0.01	0.04	0.02	R^2	0.02	0.02	0.02
Adj. R^2	0.01	0.04	0.02	Adj. R^2	0.02	0.02	0.02
Day 5 ($n = 60863$)				**Day 6** ($n = 48336$)			
Metric	Ridge	ENet	LASSO	Metric	Ridge	ENet	LASSO
R^2	0.03	0.01	0.06	R^2	0.07	0.02	0.01
Adj. R^2	0.03	0.01	0.06	Adj. R^2	0.07	0.02	0.01
Day 7 ($n = 72081$)				**Day 8** ($n = 53942$)			
Metric	Ridge	ENet	LASSO	Metric	Ridge	ENet	LASSO
R^2	0.01	0.03	0.02	R^2	0.03	0.03	0.03
Adj. R^2	0.01	0.03	0.02	Adj. R^2	0.03	0.03	0.03

R^2 and Adj. R^2 values for all 3 regression models are the same.

Adj. R^2 shows if adding more NetFlow records in the 3 regression models increases the R^2 value.

Elastic Net



Proportion of residuals in all 3 regression models are greater than 0.

Phase 1: Identify correlations of reflection attacks (cont'd)

NTP servers

Day 1 ($n = 41125$)				Day 2 ($n = 90891$)			
NetFlow records	4530	12032	24563	NetFlow records	6708	12947	71236
Coeff.	0.0004	0.001	0	Coeff.	0.0001	0.002	0
Day 3 ($n = 88800$)				**Day 4 ($n = 113804$)**			
NetFlow records	7649	26196	54955	NetFlow records	47092	66712	-
Coeff.	0.001	0.005	0	Coeff.	0.003	0	-
Day 5 ($n = 60863$)				**Day 6 ($n = 48336$)**			
NetFlow records	7407	9983	43473	NetFlow records	2968	23095	22273
Coeff.	0.0001	0.002	0	Coeff.	0.002	0.01	0
Day 7 ($n = 72081$)				**Day 8 ($n = 53942$)**			
NetFlow records	12534	20617	38930	NetFlow records	10485	13798	29659
Coeff.	0.0001	0.001	0	Coeff.	0.001	0.03	0

Regression coefficients in the Elastic Net model are close to 0 or equal to 0.

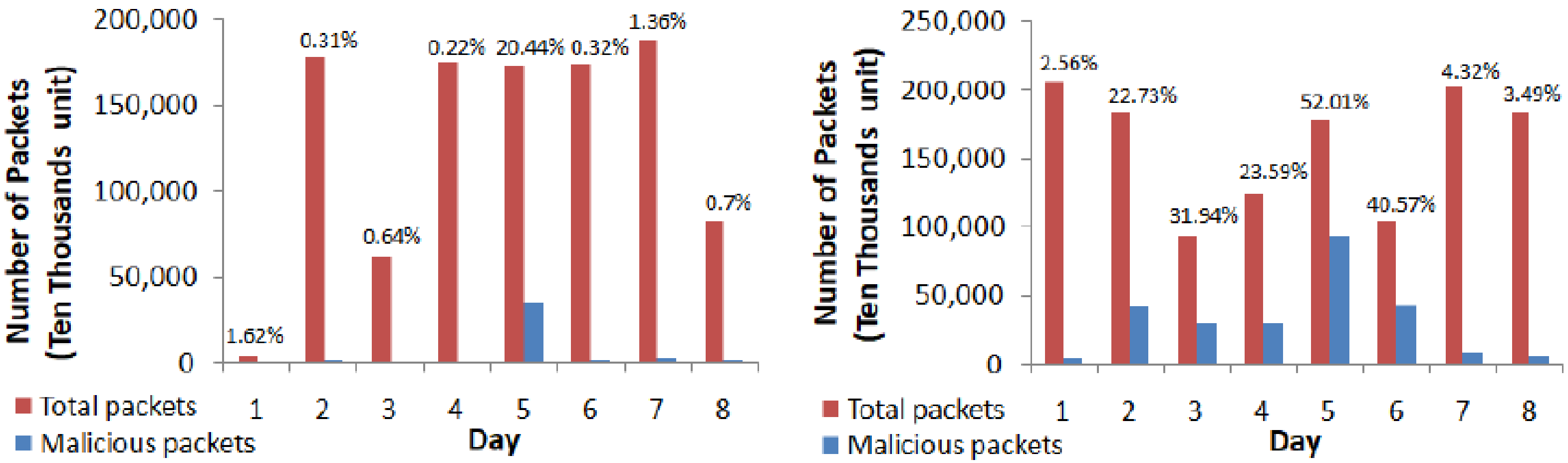
Conclusion: Reflection attacks on the NTP servers are not correlated.

Phase 2: Identify devices and traffic generated by the reflection attack

NTP servers

Day	Qty. source devices	Qty. destination devices	Source packets	Destination packets
1	154	85	682,853	52,715,588
2	230	538	5,451,544	417,472,580
3	208	663	3,914,066	300,596,636
4	247	623	3,807,407	292,454,884
5	227	555	354,300,063	930,826,308
6	381	500	5,517,178	422,559,364
7	188	541	25,678,529	87,543,748
8	124	492	5,793,229	64,289,836

Source and destination devices associated with NTP server reflection attacks.



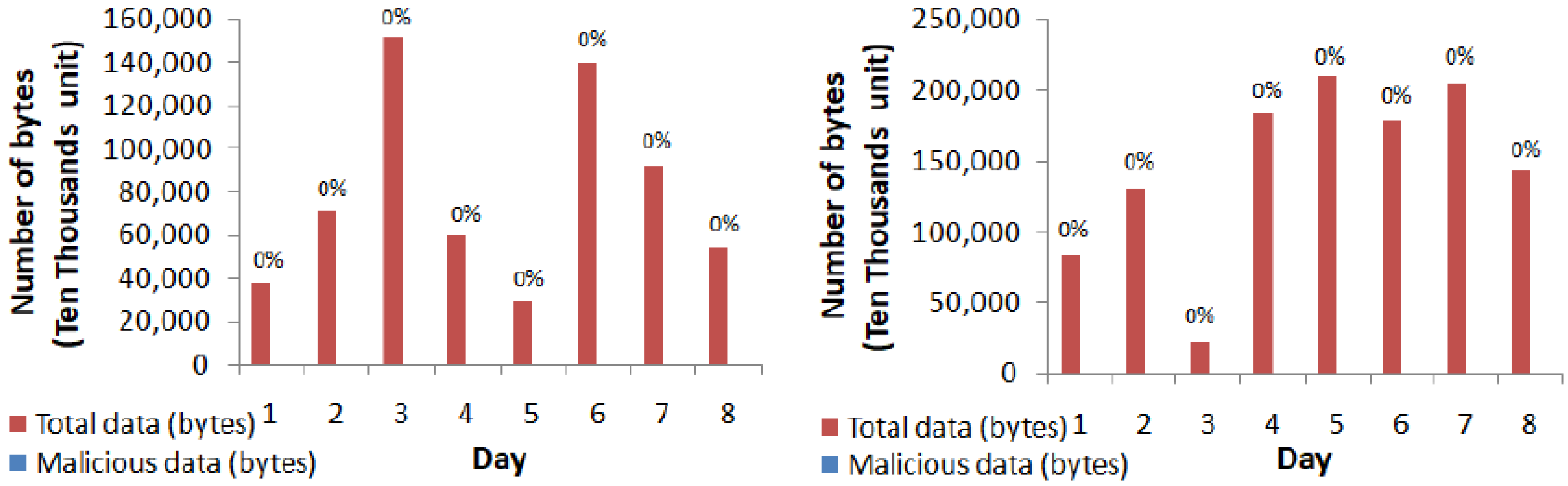
(a) Source devices.

(b) Destination devices.

Number and percentage of malicious packets transmitted in the network.

Phase 2: Identify devices and traffic generated by the reflection attack (cont'd)

NTP servers



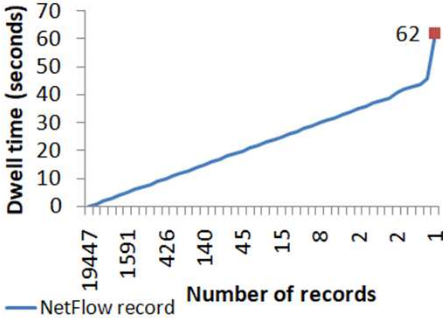
(a) Source devices. (b) Destination devices.

Number and percentage of bytes transmitted in the network. The malicious packets associated with the NTP server reflection attacks contained 0-byte payloads.

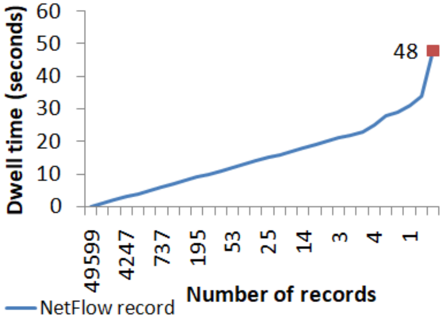
While the percentage of malicious packets sent by the source and destination devices are high for some days, those packets contained 0-byte payloads, indicating that the attack did not overwhelm the NTP servers.

Phase 3: Identify the dwell time of reflection attacks

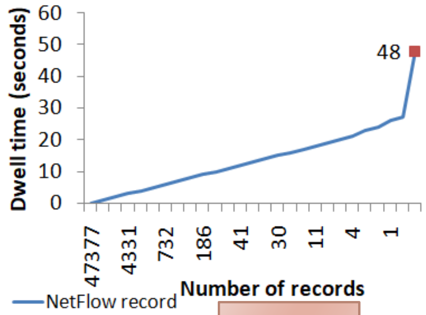
NTP servers



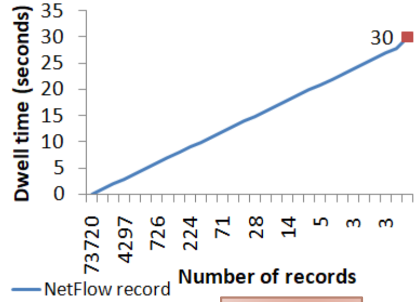
Day 1



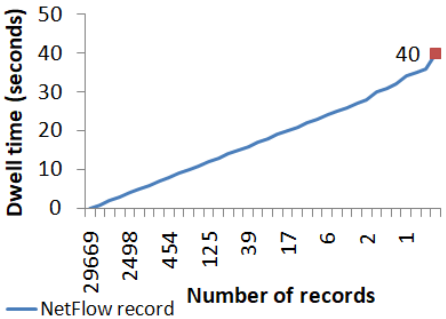
Day 2



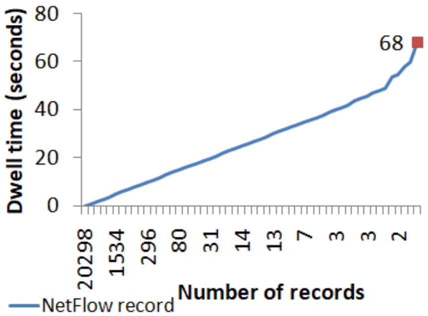
Day 3



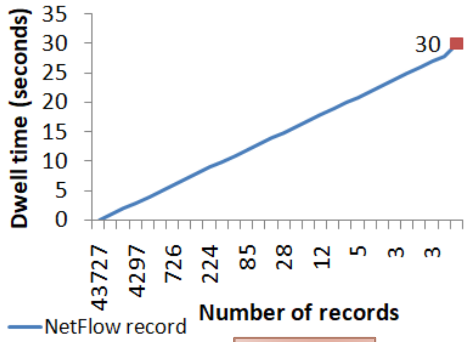
Day 4



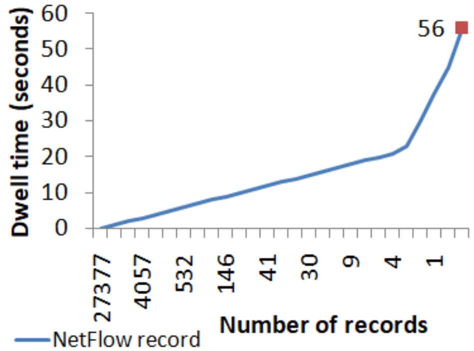
Day 5



Day 6



Day 7



Day 8

Dwell times of NTP server reflection attacks range from 0 seconds to 68 seconds over the 8 days, indicating that the dwell times are too small for predicting reflection attacks on the NTP servers.

Discussion

Finding	Recommendation
Reflection attacks on the NTP and NetBIOS servers are not correlated in the NetFlow data.	Small percentages of network packets can be ignored unless a large percentage of network packets associated with a reflection attack is observed in the NetFlow data.
Spoofed requests triggered reflection attacks on the NTP and NetBIOS servers.	Network administrators can implement ingress filtering on their networks which allows detection of IP packet spoofing.
The dwell times of reflection attacks on the NTP and NetBIOS servers are small.	Network attack mitigation schemes can implement Anycast to scatter the attack traffic and absorb the attack.
The LASSO, Ridge and Elastic Net models did not identify correlations of reflection attacks.	Conducting an empirical study of deep learning models could improve detection of reflection attacks.

Cyberattack prediction problem

- We have shown that the dwell times of reflection attacks are too small to be used for predicting reflection attacks in the NetFlow data.

- When a network is not overwhelmed by the attack, the security analyst can respond to the attack.
  - For example, when the dwell times of a reflection attack are small, a network mitigation scheme that scatters the attack traffic can be used to absorb the attack.

- However, if the network is overwhelmed by the attack, it is too late for the security analyst to respond to the attack.

How can we develop an effective solution to predict cyberattacks on a large system?

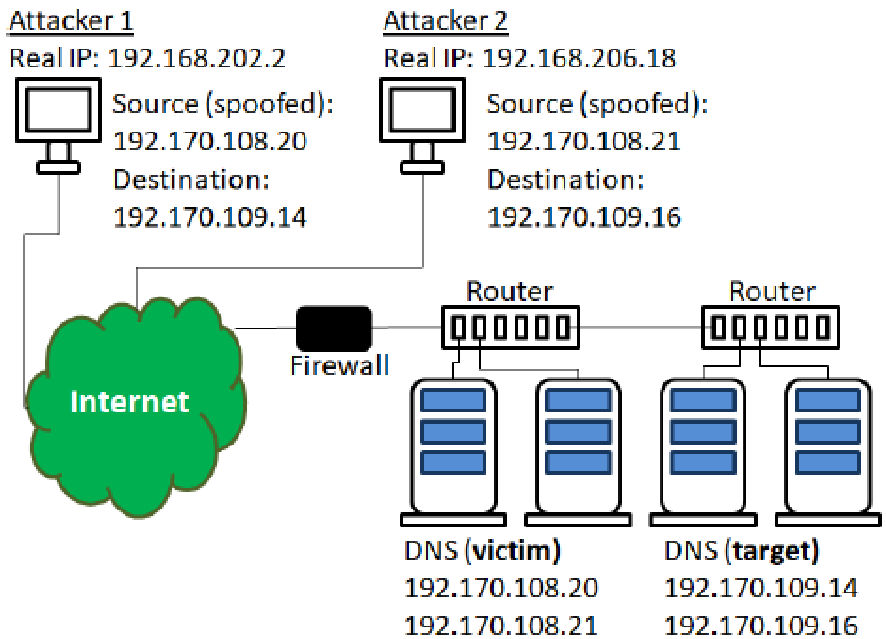
Research project: Predicting cyberattacks in large networks

- Challenges:
  - High quality data is necessary, but insufficient to reduce the number of false positives and false negatives in machine learning models.
  - In general, the dwell times of a cyberattack is too short to be used for predicting the next attack.

➢ Project 1: Determine if deep learning models can predict a cyberattack when it is detected.

➢ Project 2: Develop a new approach to *predict which devices on the network will be attacked*. By predict, I mean identifying sequences of events which precede an attack on the network.

➢ Project 3: Implement the cyberattack predictor and test it on a testbed.



An illustration of the IP spoofing process.

E. Chuah, et. al., "*Deep Learning-based Prediction of Reflection Attacks Using NetFlow Data*", submitted 2024.

Thank you for coming to my talk.

If you have any further enquiries, please feel free to get in touch with me.

thuan.chuah@abdn.ac.uk