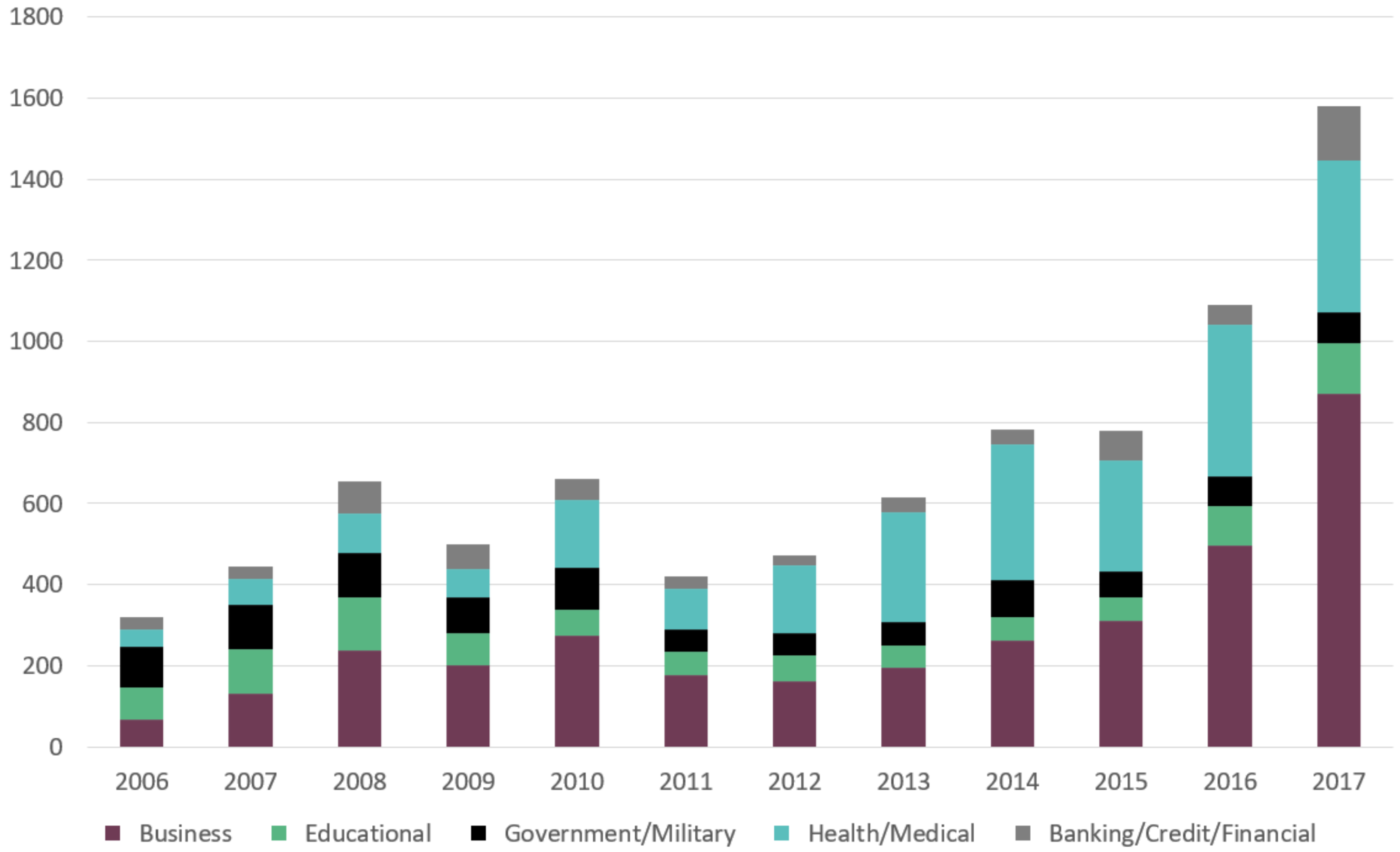
Henry Clausen

Detecting semantic anomalies in network traffic

THE UNIVERSITY *of* EDINBURGH
informatics



Increasing Number of Data Breaches by Industry

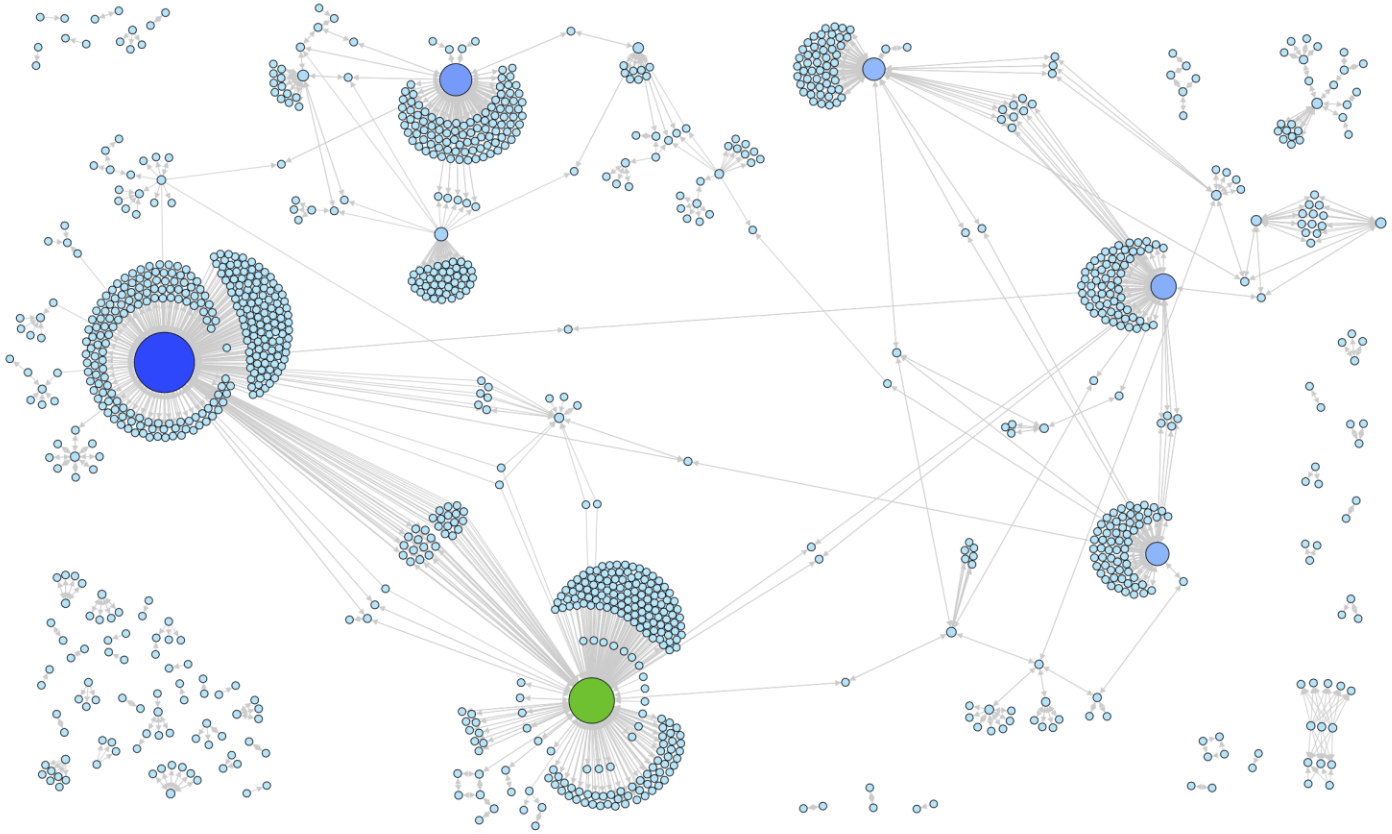
Source: Identity Theft Resource Center: ITRC Breach Report as of Feb 21, 2018

Network intrusion detection

- Monitors network for malicious activity

- Identify intrusion before harm is done
  - Data exfiltration
  - Ransomware
  - Service disruption
  - …

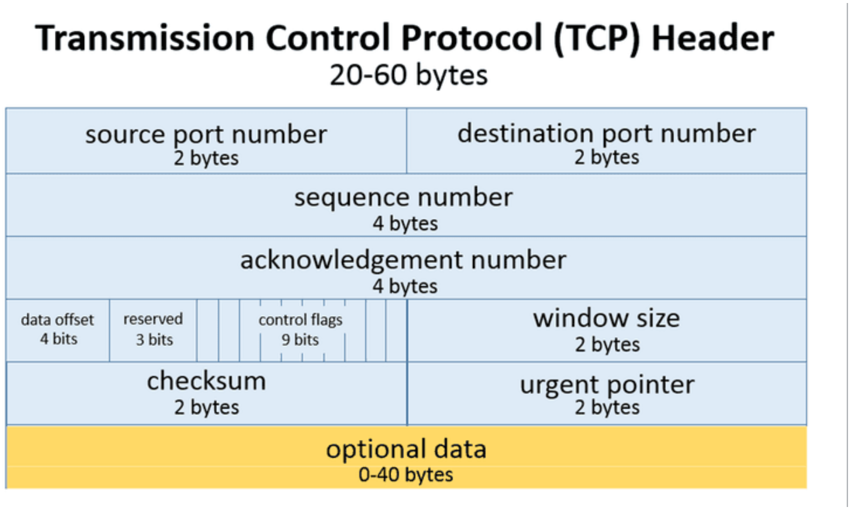
- Second line of defense



THE UNIVERSITY *of* EDINBURGH
informatics

Network intrusion detection

- Analyses in- and outgoing traffic
- Data:
  - Packets
  - Flows
- Often encrypted



Transmission Control Protocol (TCP) Header
20-60 bytes

```
Date flow start           Duration Proto    Src IP Addr:Port       Dst IP Addr:Port      Packets    Bytes Flows
2010-09-01 00:00:00.459      0.000 UDP      127.0.0.1:24920    -> 192.168.0.1:22126          1       46     1
2010-09-01 00:00:00.363      0.000 UDP      192.168.0.1:22126 -> 127.0.0.1:24920            1       80     1
```

Signature-based

- Looking for "known patterns" of detrimental activity

- Benefits:
  - Accurate
  - Low false alert rate
  - Fast

Drawbacks:

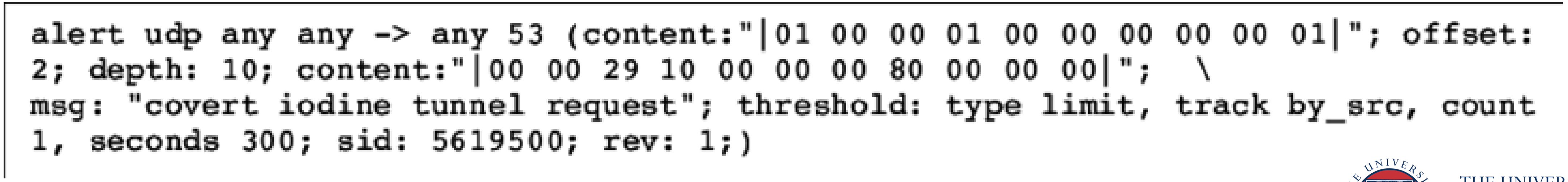
- Need for updated library of signatures
- Ineffective against new attacks

ClamAV

SNORT

yara

OpenIOC



```
alert udp any any -> any 53 (content:"|01 00 00 01 00 00 00 00 00 01|"; offset:
2; depth: 10; content:"|00 00 29 10 00 00 00 80 00 00 00|";  \
msg: "covert iodine tunnel request"; threshold: type limit, track by_src, count
1, seconds 300; sid: 5619500; rev: 1;)
```

Anomaly-based

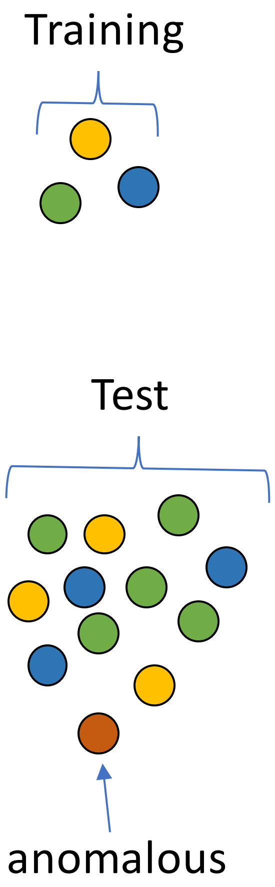
- Use training data to create model of normal traffic
- Compare new traffic against this model

- No assumptions about potential attack

Disadvantages:

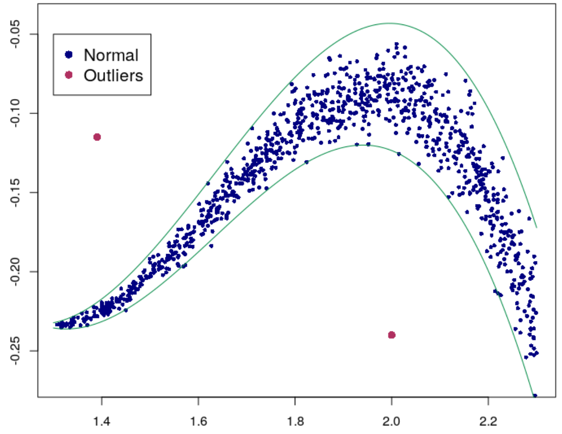
  - Difficult
  - False alerts
  - Computationally more intensive
  - Lack of datasets

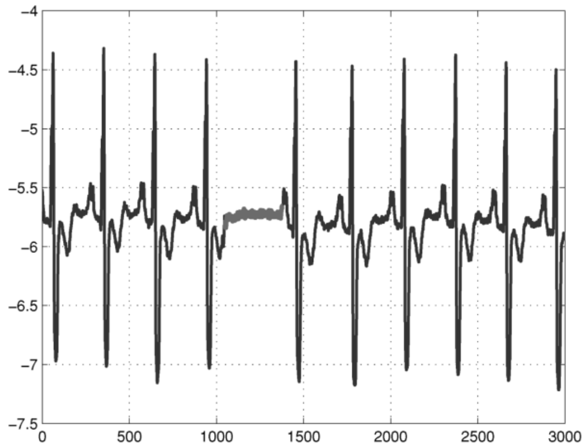
- Increasingly used in industry for unknown attacks


Training

Test

anomalous

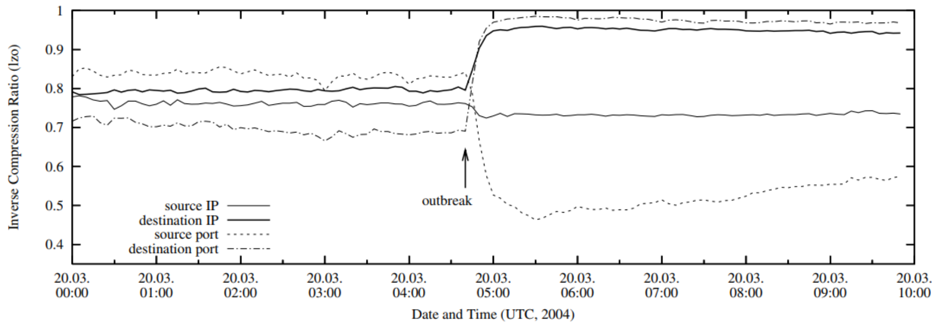


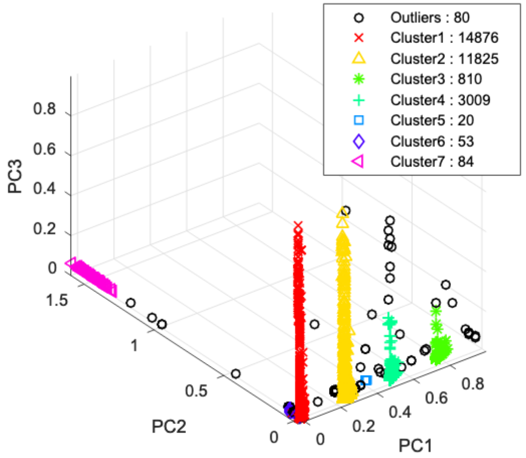


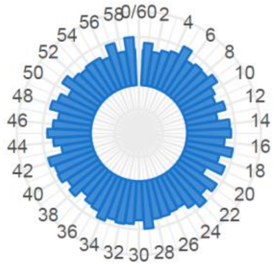
Where it currently works well

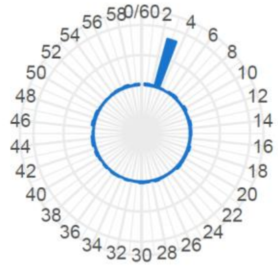
- Group anomalies:
  - DoS attacks
  - Network probing
- Activity-based:
  - User active at strange times
  - Temporal pattern of network activity
- Point anomalies (partly):
  - Odd connection pairs
  - Unusually large flows to specific ports

Figure 1. Blaster - TCP address parameter compressibility









THE UNIVERSITY *of* EDINBURGH
informatics

Semantic gap

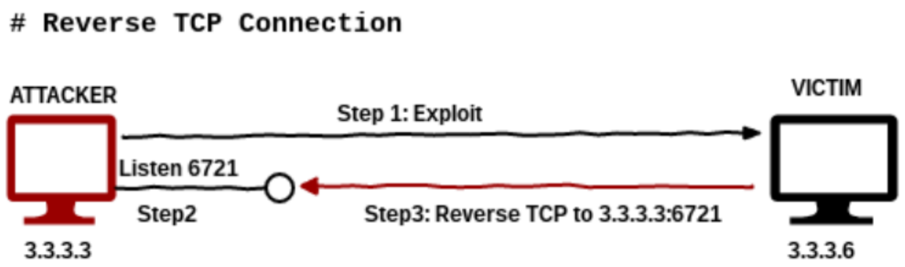
- Many access attack events do not look suspicious when isolated
  - Few events
  - Normal size, length, …
  - Hide in traffic diversity

- However, they are clearly anomalous from a contextual perspective

- How do we close this semantic gap?

Client	Server	Delta-time	Size	Flags
	Passw-req.	0.041	79	A
Passw: …		0.005	961	A
	Failure	0.044	100	AP
	Success	0.022	81	AP
Req: PWD		3.073	89	AP

…



Aim: semantic traffic model

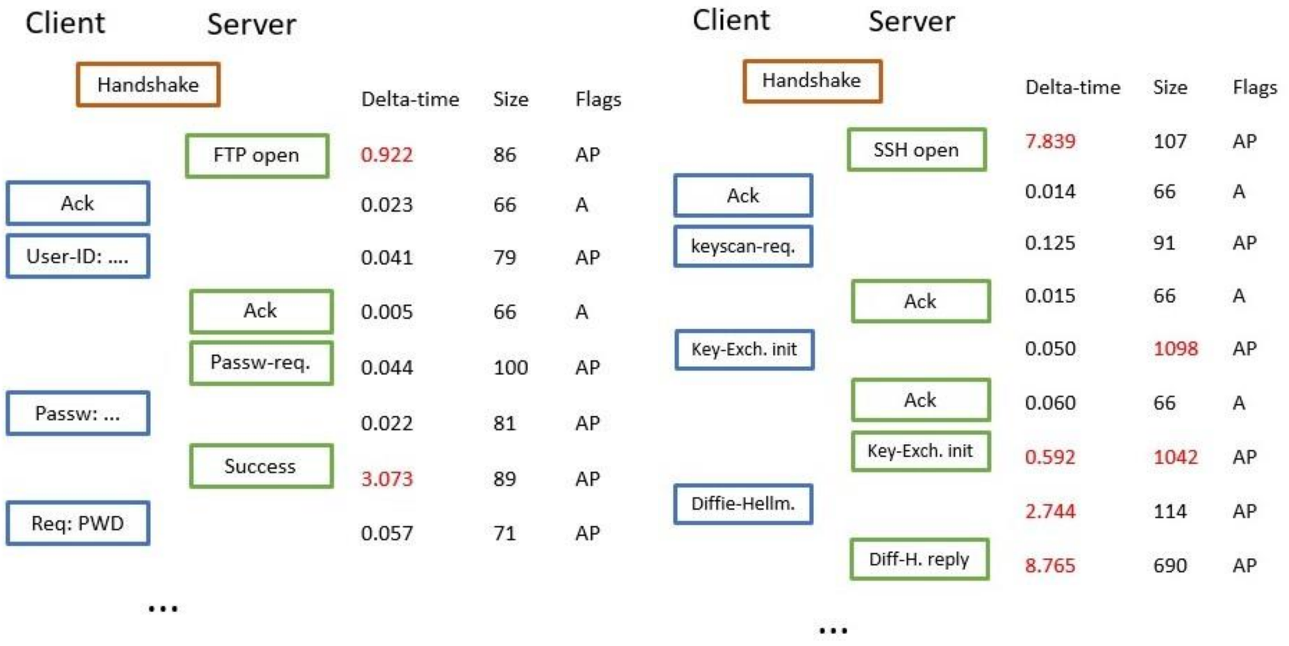
- Applications have finite set of actions
  - Actions correspond to semantic structures in traffic
- Capture representation of semantic substructures using self-prediction
- Inspiration from state-based software models and natural language prediction

Negotiation phase model

- TCP connections typically have a strong semantic structure in the first few packets

- Packet features:
  - Binary: source, flags
  - Continuous: size, time, window size

- Variation can be stronger or softer:
  - packet order or missing/additional packet
  - Input and time
  - Connection restart



Client	Server	Delta-time	Size	Flags
Handshake	Handshake			
	FTP open	0.922	86	AP
Ack		0.023	66	A
User-ID:		0.041	79	AP
	Ack	0.005	66	A
	Passw-req.	0.044	100	AP
Passw: ...		0.022	81	AP
	Success	3.073	89	AP
Req: PWD		0.057	71	AP

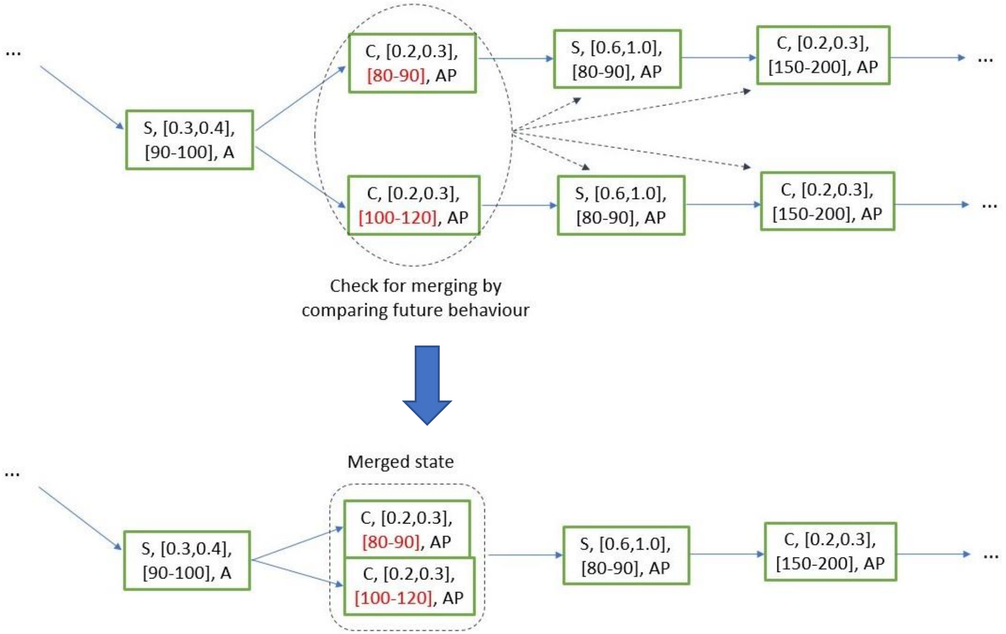
...

Client	Server	Delta-time	Size	Flags
Handshake	Handshake			
	SSH open	7.839	107	AP
Ack		0.014	66	A
keyscan-req.		0.125	91	AP
	Ack	0.015	66	A
Key-Exch. init		0.050	1098	AP
	Ack	0.060	66	A
	Key-Exch. init	0.592	1042	AP
Diffie-Hellm.		2.744	114	AP
	Diff-H. reply	8.765	690	AP

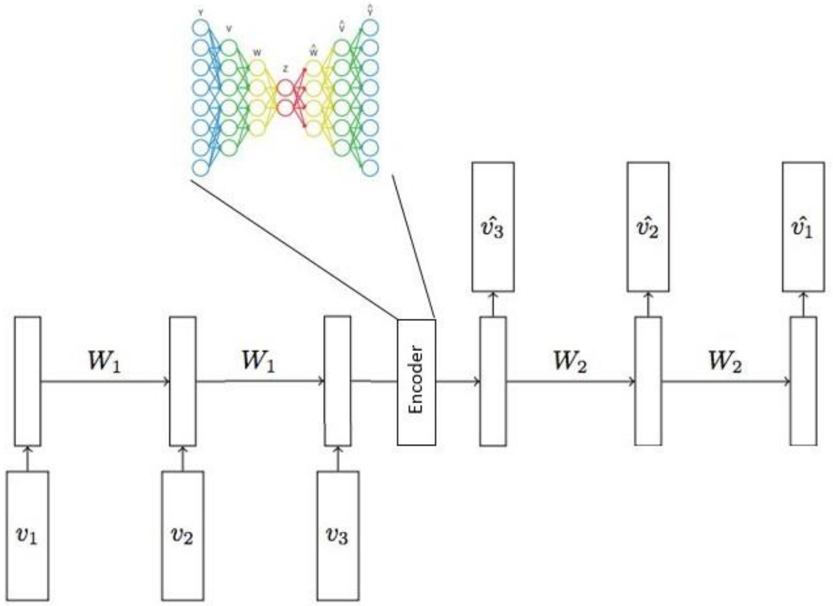
...

Modelling methods

Probabilistic Real-Time Automata


...
S, [0.3,0.4], [90-100], A
C, [0.2,0.3], [80-90], AP
C, [0.2,0.3], [100-120], AP
S, [0.6,1.0], [80-90], AP
S, [0.6,1.0], [80-90], AP
C, [0.2,0.3], [150-200], AP
C, [0.2,0.3], [150-200], AP
...
...
Check for merging by comparing future behaviour
Merged state
...
S, [0.3,0.4], [90-100], A
C, [0.2,0.3], [80-90], AP
C, [0.2,0.3], [100-120], AP
S, [0.6,1.0], [80-90], AP
C, [0.2,0.3], [150-200], AP
...

LSTM-Autoencoder

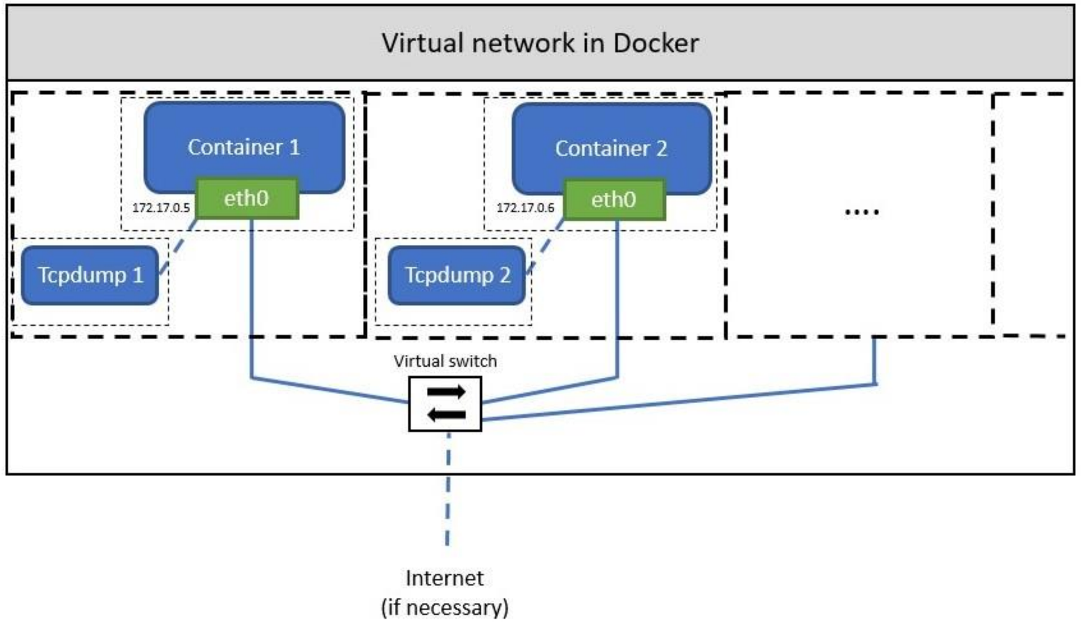


Detection through prediction-deviations

Validation

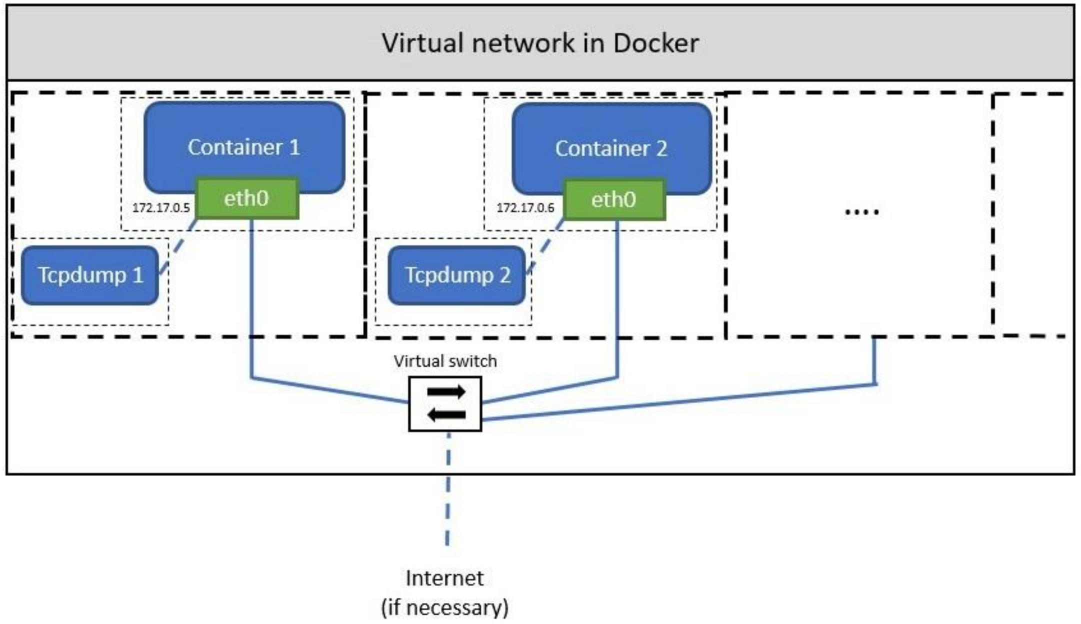
- Detection accuracy in existing datasets
  - Must contain both benign and malicious events
  - Few and not necessarily realistic attacks

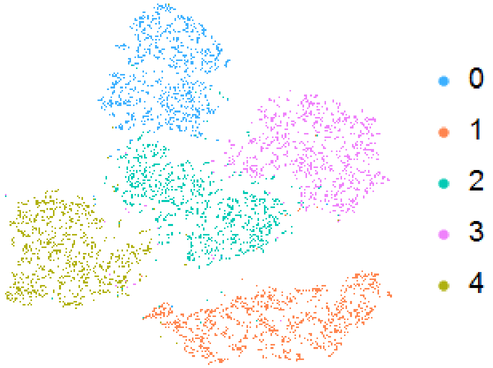
- Need to validate that our model learned meaningful structures
  - Need for ground truth data



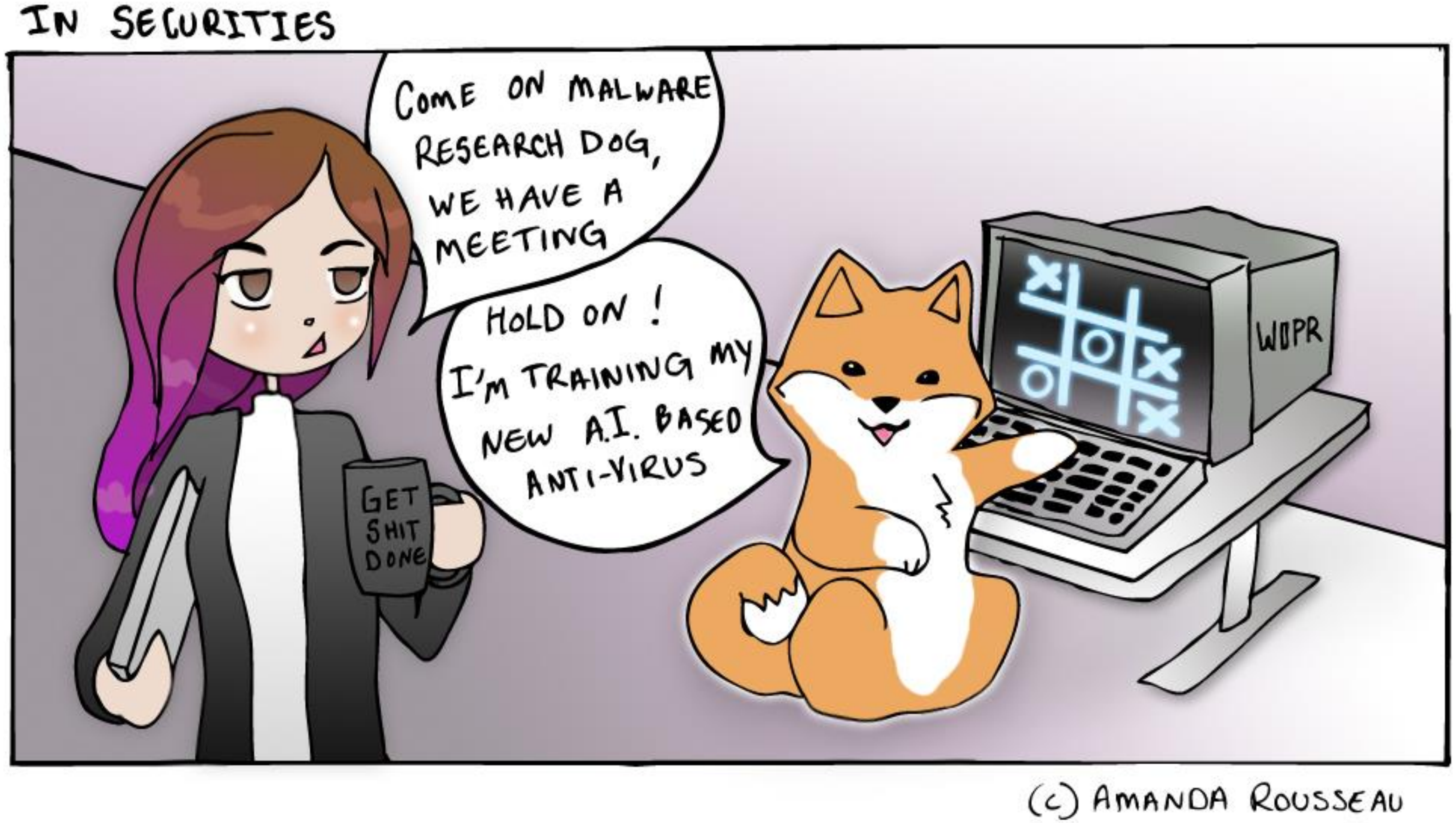
Validation

- Data generation framework:
  - Isolated traffic from set of application/scenarios
  - Randomised passwords, input, etc. to recreate true traffic variation
- Inject isolated instances both in training and test set
- Compare how well applications are recognized
  - Closeness measure for similar actions
  - Anomaly for new actions





The End


IN SECURITIES
COME ON MALWARE RESEARCH DOG, WE HAVE A MEETING
HOLD ON ! I'M TRAINING MY NEW A.I. BASED ANTI-VIRUS
GET SHIT DONE
WOPR
(C) AMANDA ROUSSEAU

THE UNIVERSITY *of* EDINBURGH **informatics**