Henry Clausen, David Aspinall, Gudmund Grov, Marc Sabate

Better anomaly detection for access attacks using deep bidirectional LSTMs

THE UNIVERSITY *of* EDINBURGH
informatics

EPSRC
Pioneering research and skills

The Alan Turing Institute

FFI Forsvarets forskningsinstitutt
Norwegian Defence Research Establishment

Contribution

Novel deep LSTM-model:

- Designed for access attacks
- Flow-based
- Significantly improves detection rates

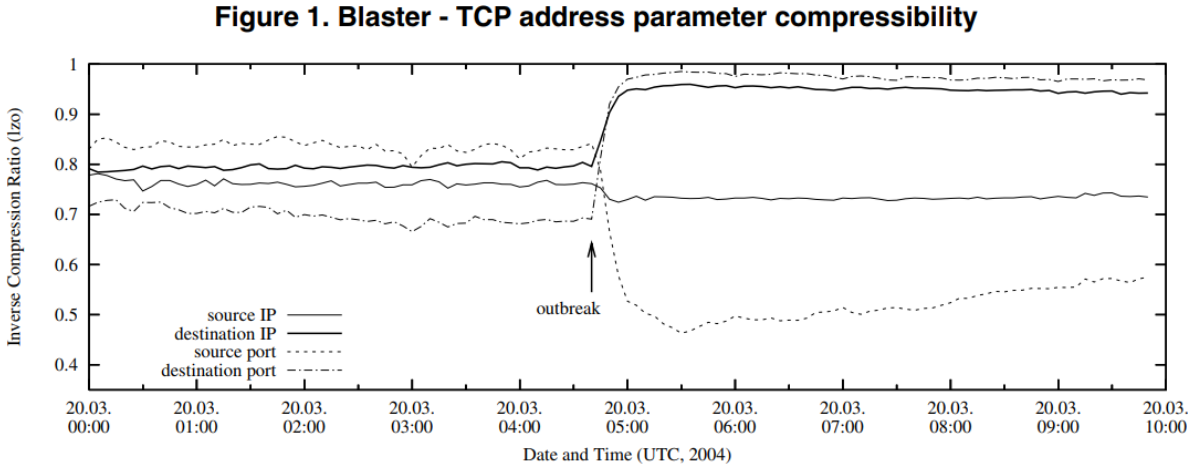
Careful in-depth evaluation

- Comparison to SoA-models
- Longterm evaluation
- AUC-scores and det. Rates

THE UNIVERSITY of EDINBURGH
informatics

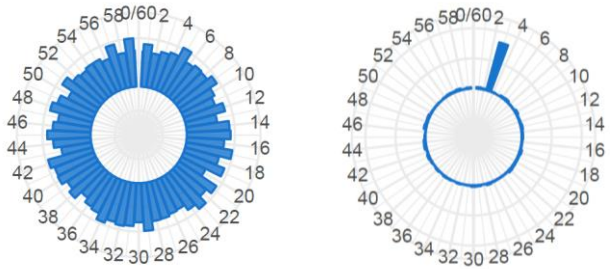
Where network anomaly-detection works

- DoS attacks
- Network probing
- Worms
- User active at strange times



Nisioti et al. (2018):

- Remote2Local & User2Root far less reliably detected
- Evaluation pitfalls make comparison difficult



THE UNIVERSITY of EDINBURGH
informatics

Underlying idea

Src	Dst	DPort	bytes	# packets
A	B	80	247956	315
A	B	80	7544	13
A	B	80	328	6
A	B	80	2601	10
A	B	80	328	6
A	B	80	328	6
A	B	80	380	7
A	B	80	328	6
⋮				

SQL-injection-attack, CICIDS-17 data

Src	Dst	DPort	bytes	# packets
D	C	N33	600	5
C	D	445	77934	1482
D	C	N33	600	5
C	D	445	5202	10

Benign SMB, LANL-16 data

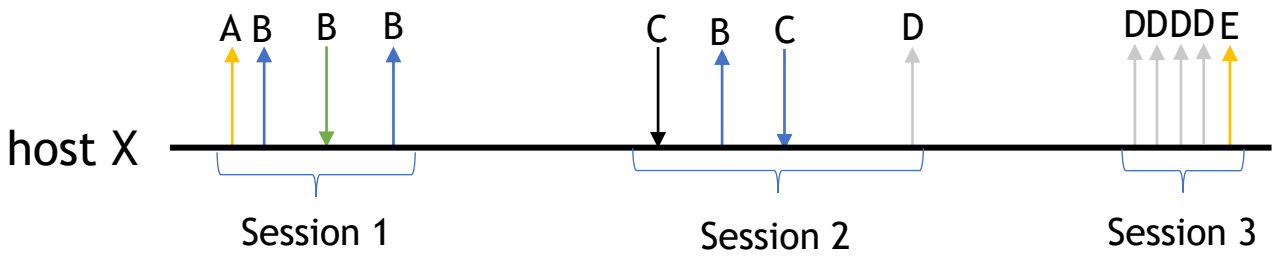
Src	Dst	DPort	bytes	# packets
C	D	445	4106275	2830
C	D	445	358305611	242847

Malicious SMB, LANL-16 data

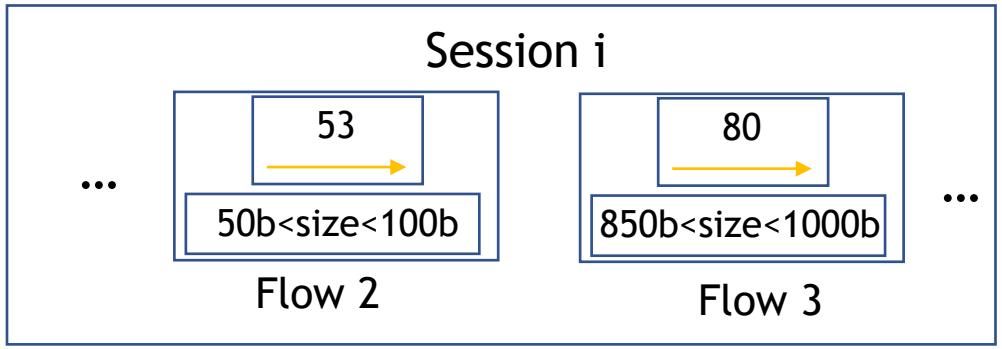
THE UNIVERSITY of EDINBURGH informatics

Modelling – Session construction

- sort outgoing and incoming connections on host X
- group them into intervals
  - flow separation less than 8s

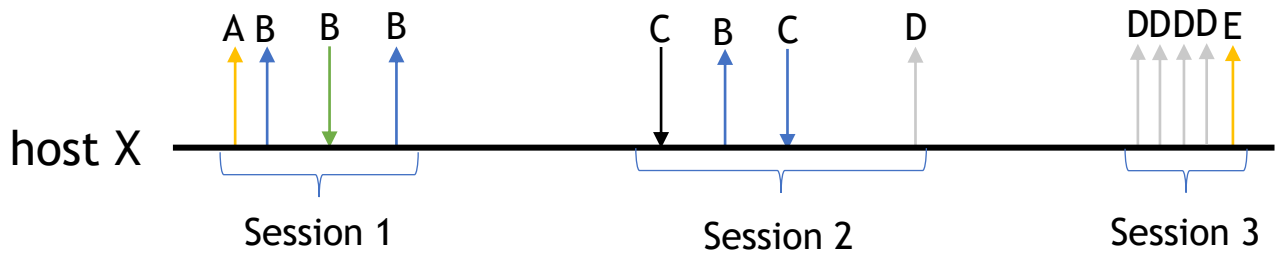


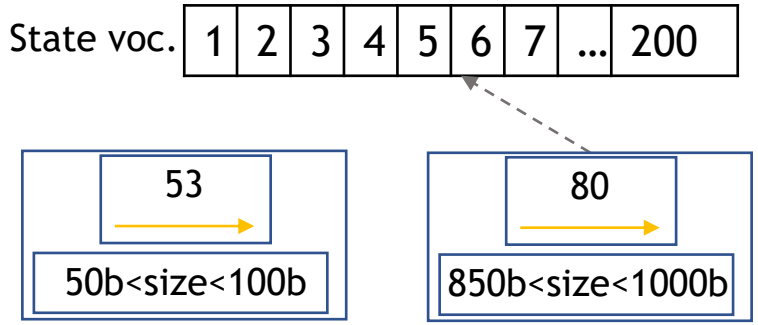
- Tokenise flows:
  - Direction
  - TCP/UDP/ICMP
  - Port
  - Size interval



Modelling – Session construction

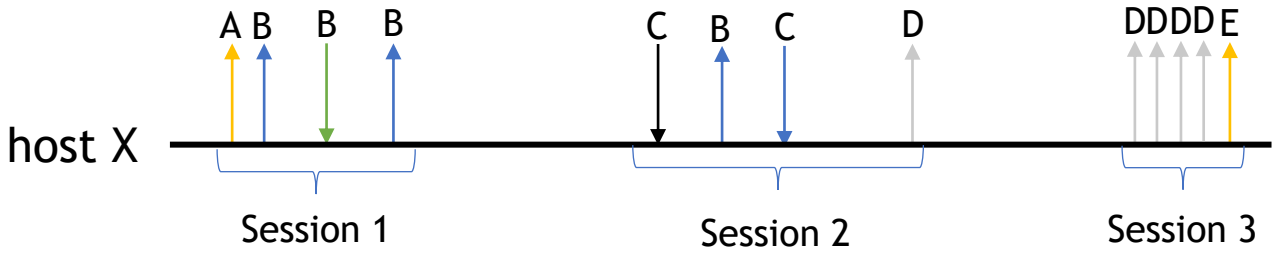
- sort outgoing and incoming connections on host X
- group them into intervals
  - flow separation less than 8s
- Tokenise flows:
  - Direction
  - TCP/UDP/ICMP
  - Port
  - Size interval

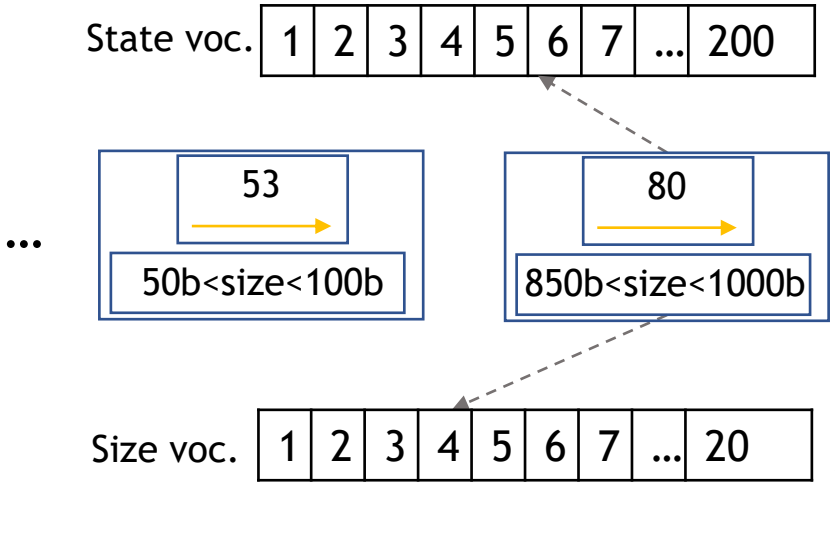




Modelling – Session construction

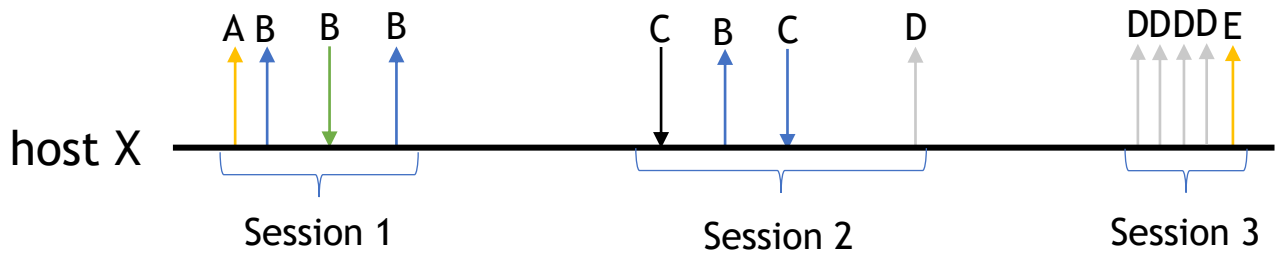
- sort outgoing and incoming connections on host X
- group them into intervals
  - flow separation less than 8s
- Tokenise flows:
  - Direction
  - TCP/UDP/ICMP
  - Port
  - Size interval

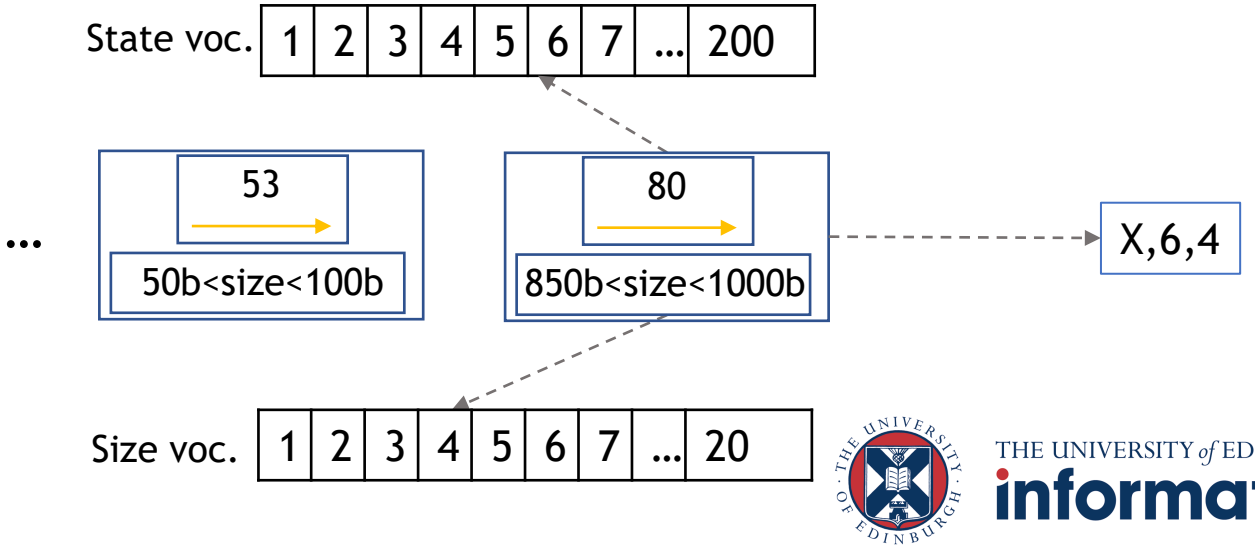




Modelling – Session construction

- sort outgoing and incoming connections on host X
- group them into intervals
  - flow separation less than 8s
- Tokenise flows:
  - Direction
  - TCP/UDP/ICMP
  - Port
  - Size interval

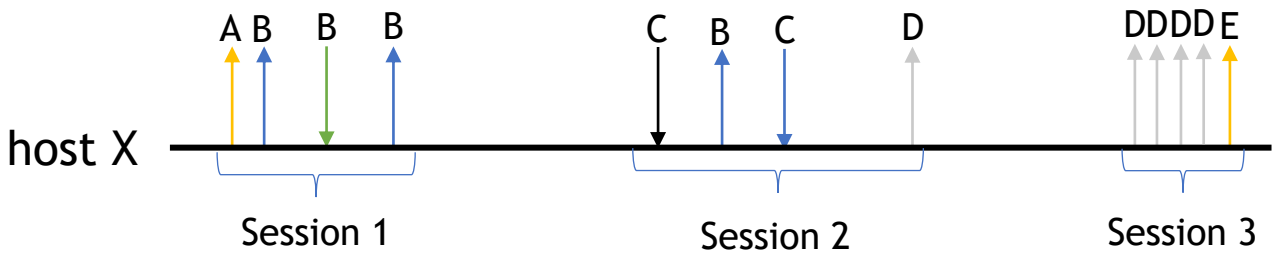


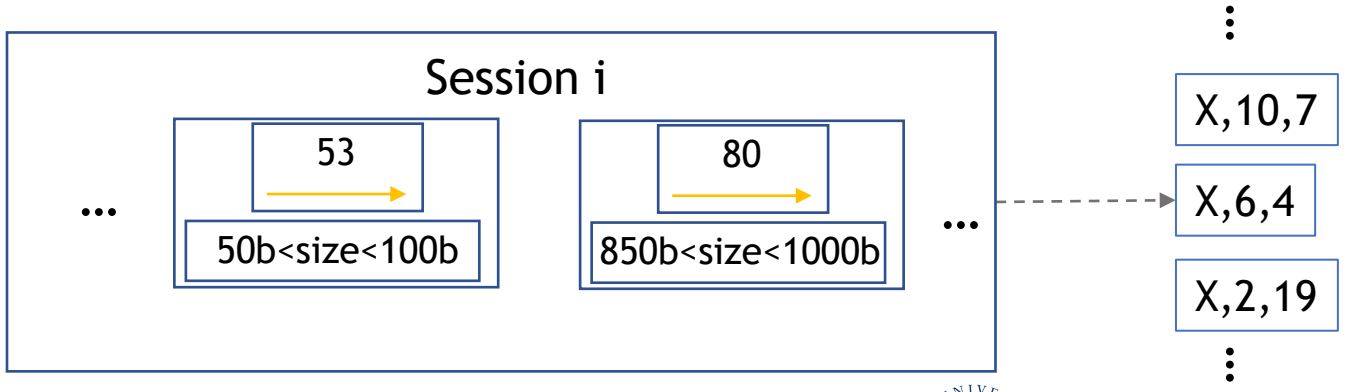


THE UNIVERSITY of EDINBURGH
informatics

Modelling – Session construction

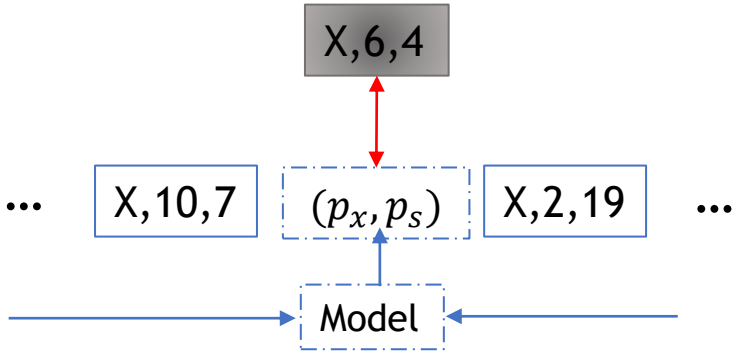
- sort outgoing and incoming connections on host X
- group them into intervals
  - flow separation less than 8s
- Tokenise flows:
  - Direction
  - TCP/UDP/ICMP
  - Port
  - Size interval





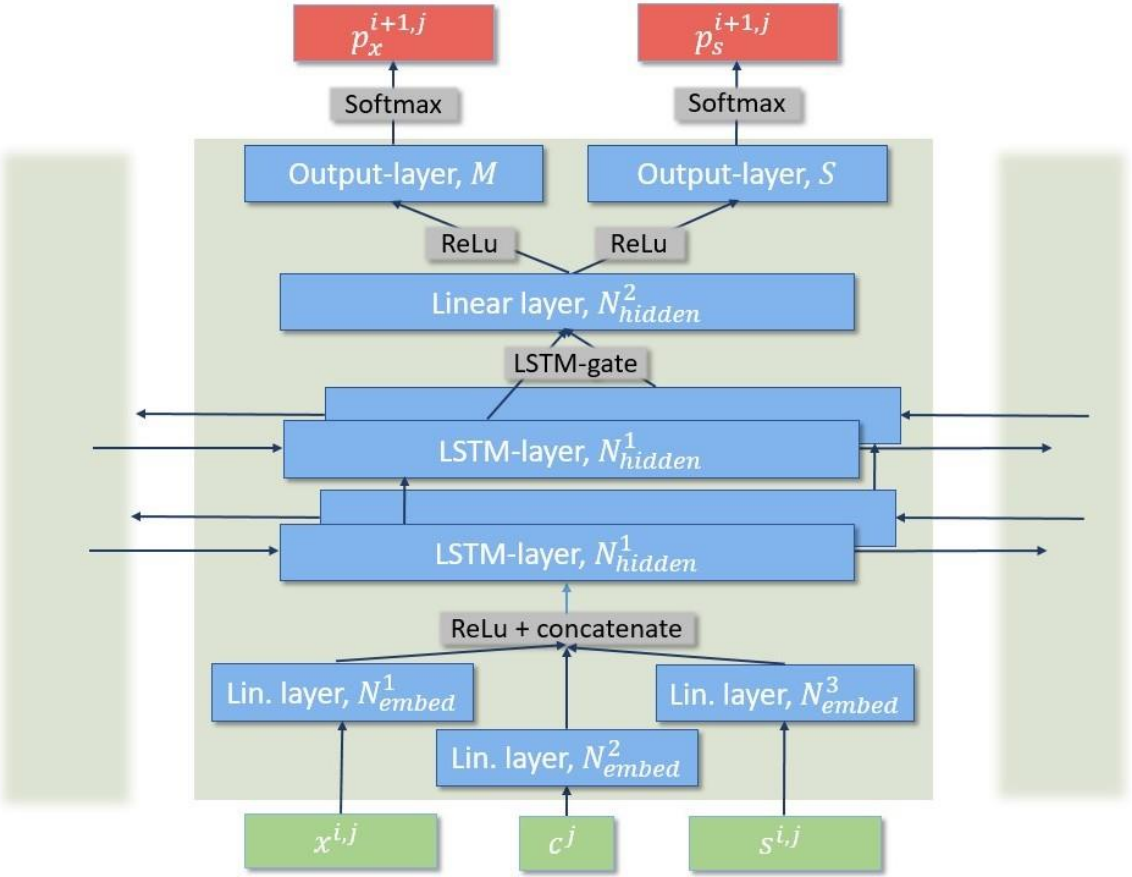
Modelling – Architecture

- Leave-one-out prediction training



- Anomaly-score: averaged likelihood of session

Model architecture



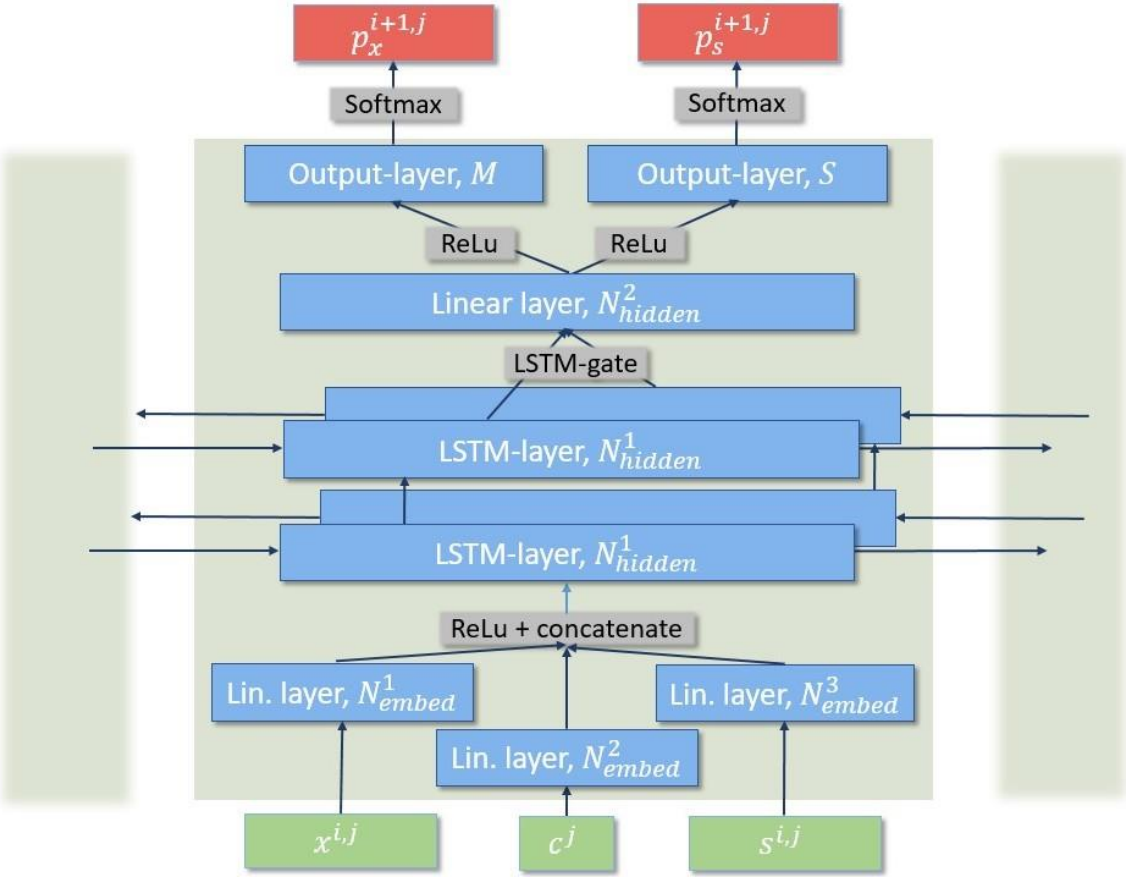
THE UNIVERSITY of EDINBURGH informatics

Modelling – Architecture

- Embedding layer
  - separately to reduce parameters
- Two LSTM layers
  - Both directions
- Linear layer to postprocess
  - Softmax-output for state and size

- $N_{hidden}^{1,2} = 50$
- $N_{embed}^{1,2,3} = 5$

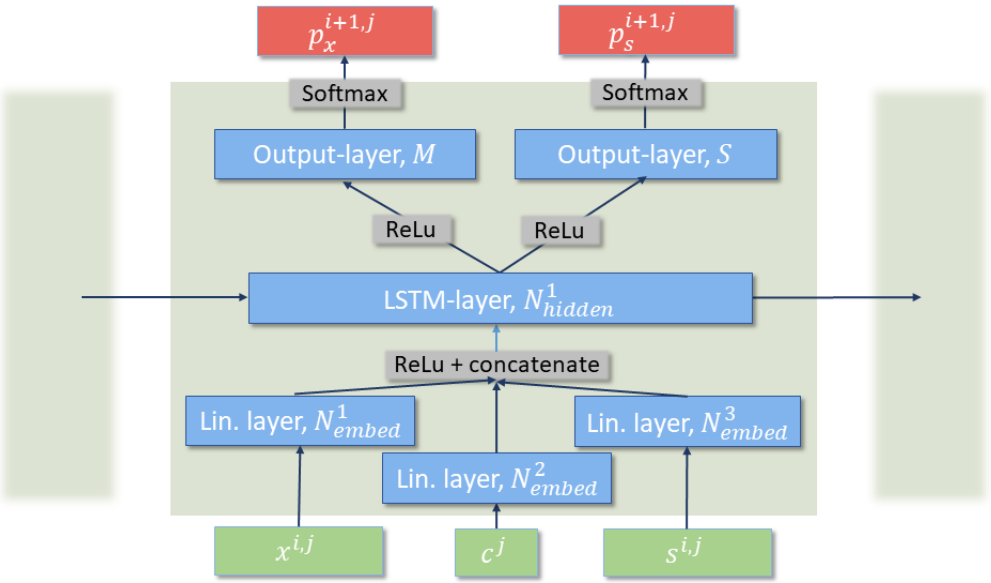
Model architecture



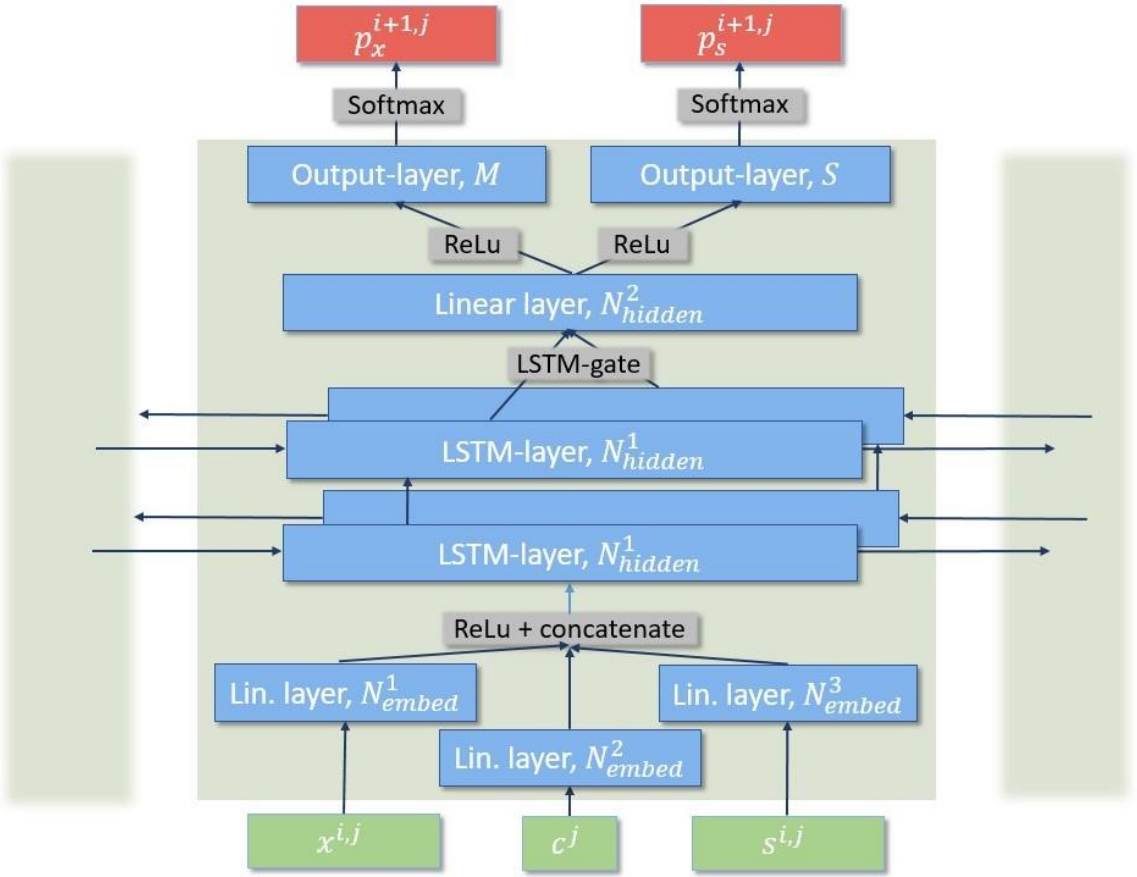
THE UNIVERSITY of EDINBURGH informatics

Modelling – Architecture

Shallow comparison architecture



Model architecture



THE UNIVERSITY of EDINBURGH informatics

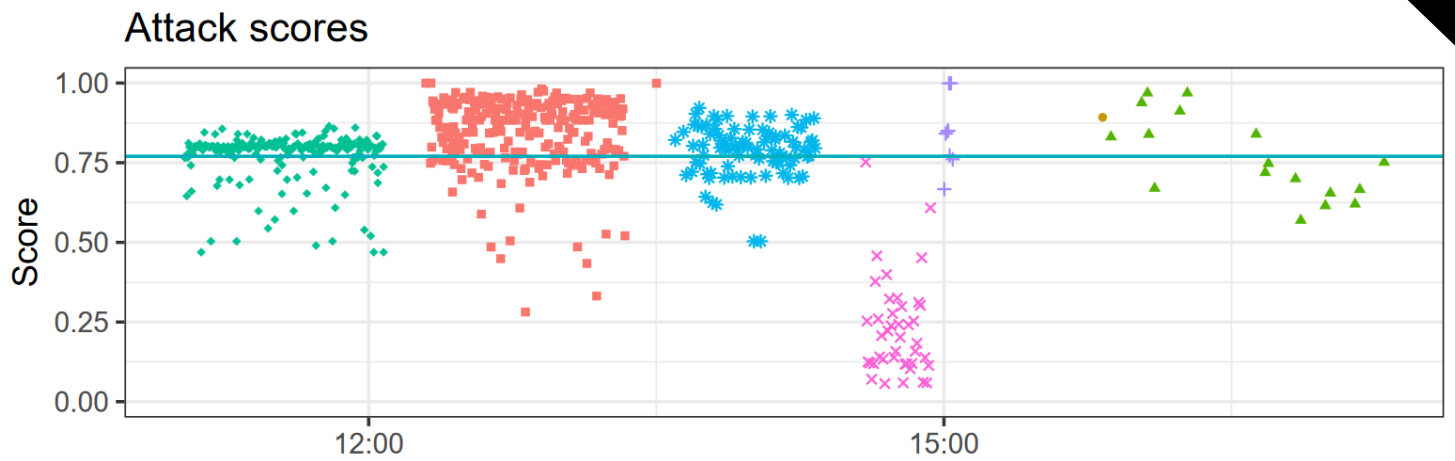
Datasets and comparison

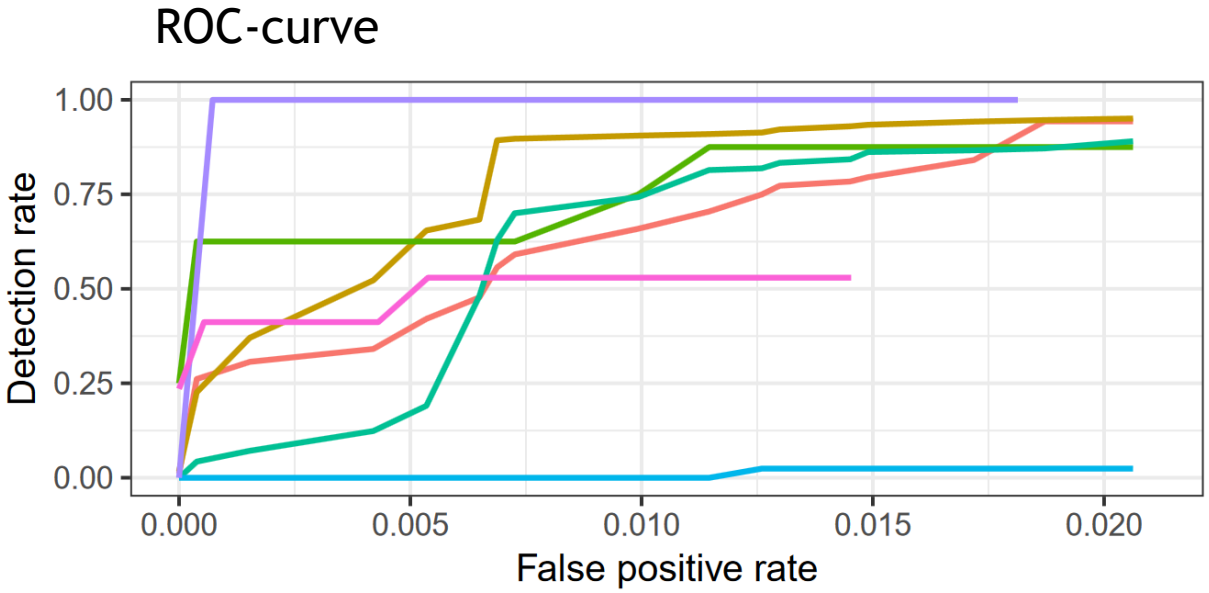
- CICIDS-17
  - 7 access attacks
  - SQL-i., Heartbleed, XSS, …
- UGR-16
  - 6 months
  - longterm evaluation

SoA-models:

- UNIDS (2013)
  - Clustering-based
  - Best access-attack detection rates in survey
- Radford et al. (2018)
  - LSTM-based
- Niyaz et al. (2016)
  - Deep autoencoder

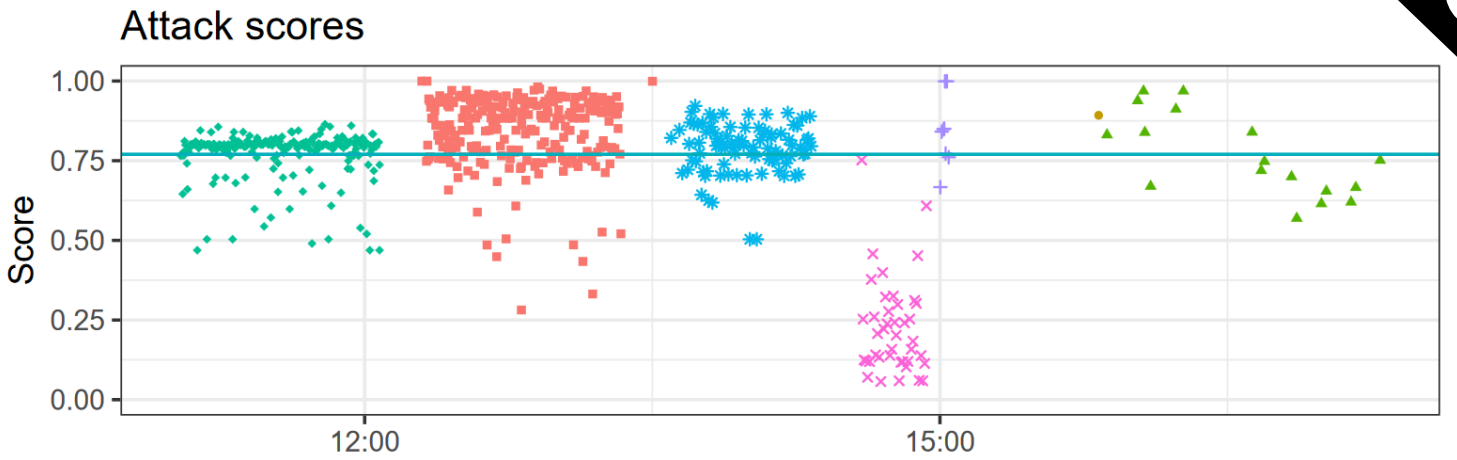
Evaluation

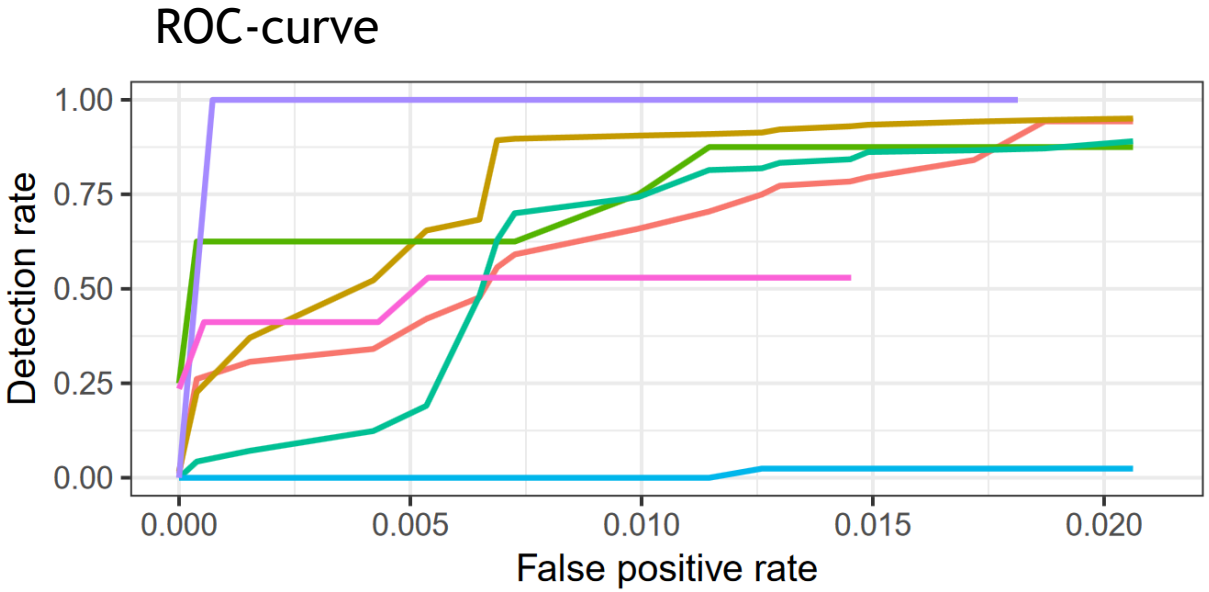




THE UNIVERSITY of EDINBURGH
informatics

Evaluation





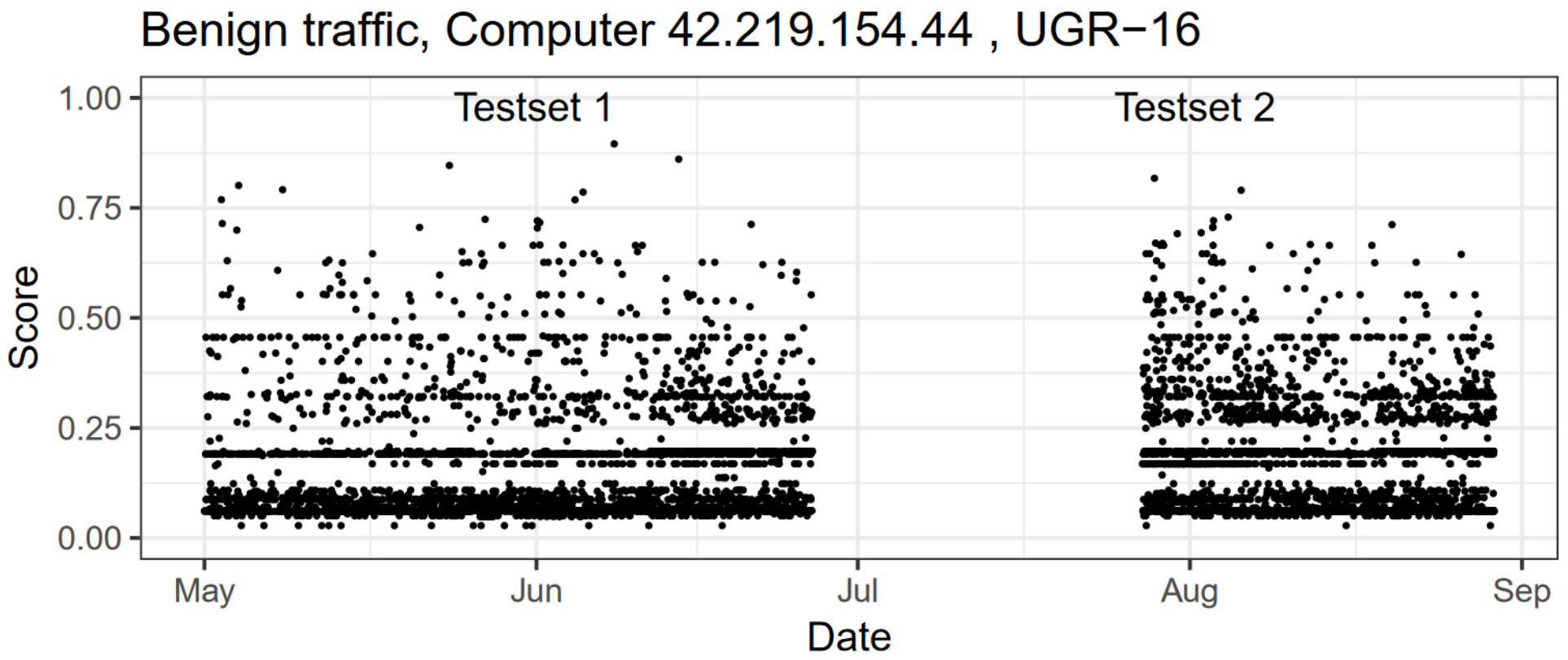
Attack: FTP−P Infilt. Brute−F. XSS Heartbl. SSH−P. SQL

Attack: Brute−F. SQL XSS Infiltr. FTP−P. SSH−P. Heartb.

	1-AUC scores				
	Our model	UNIDS	Radford	Niyaz	shallow m.
Brute Force Web	**0.016**	0.49	0.027	0.32	0.048
FTP-Patator	**0.0025**	0.011	0.0048	0.16	0.0052
Heartbleed	**0.0003**	0.0057	0.032	0.077	0.012
Infiltration	0.046	**0.033**	0.35	0.15	0.11
SQL-injection	**0.005**	0.44	0.497	0.39	0.019
SSH-Patator	**0.009**	0.013	0.035	0.011	0.005
XSS	0.127	**0.02**	0.03	0.16	0.13
Average	**0.044**	0.144	0.135	0.18	0.091

THE UNIVERSITY of EDINBURGH informatics

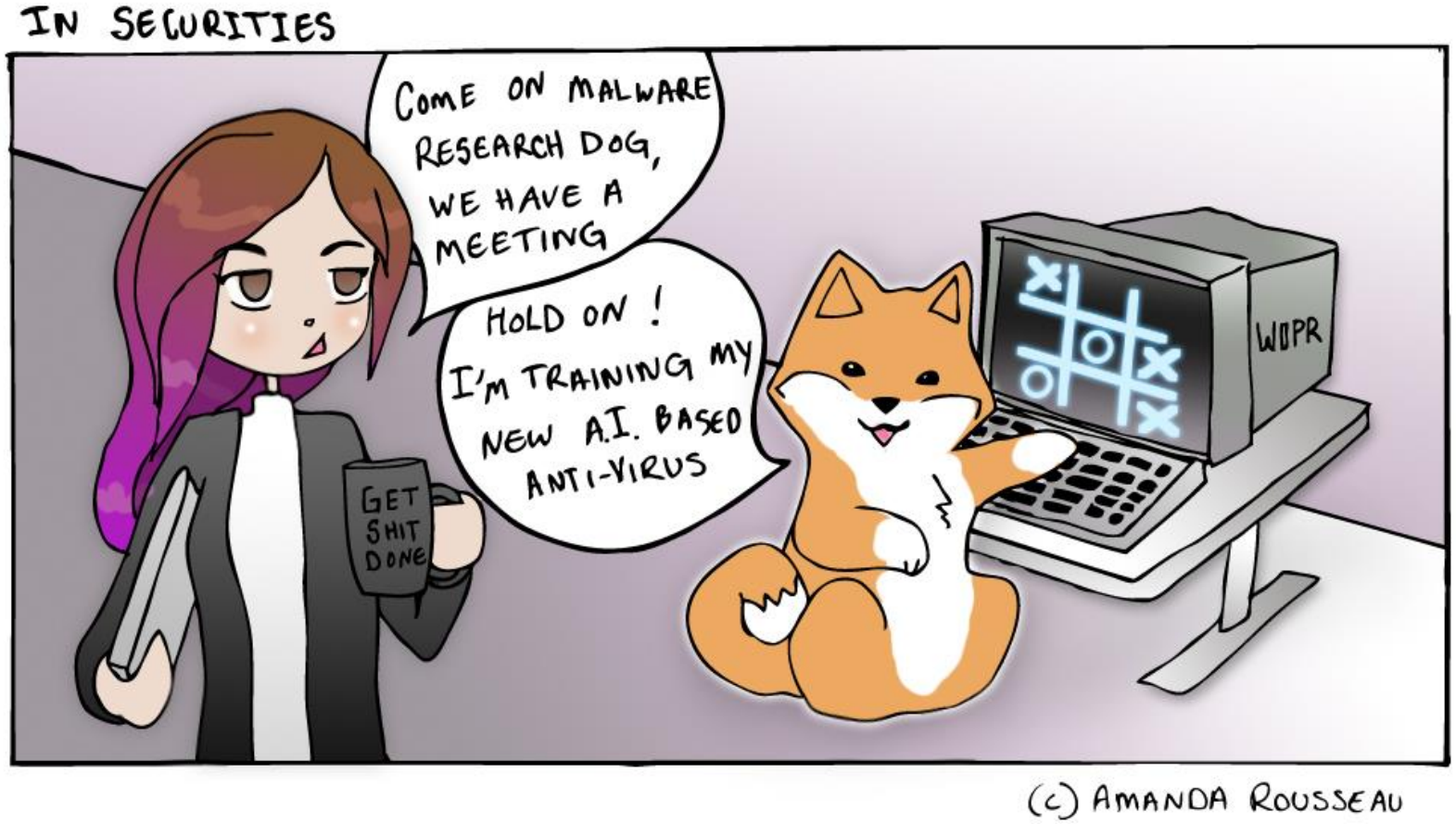
Evaluation – long-term stability



Limitations

- Traffic overlay
- Events separated in time
- Isolated flow events

Thank you for your attention



THE UNIVERSITY of EDINBURGH
informatics

Limitations

- Traffic overlay
- Events separated in time
- Isolated flow events

Conclusion

- Large public dataset
  - Realistic interactions
  - Evasive tactics
  - github.com/detlearsom/detgen/stepping-stone-data
- Evaluation of current state-of-the-art
  - Lower overall detection rates
  - Lack of robustness against chaff
  - Watermarking and deep-learning performs best