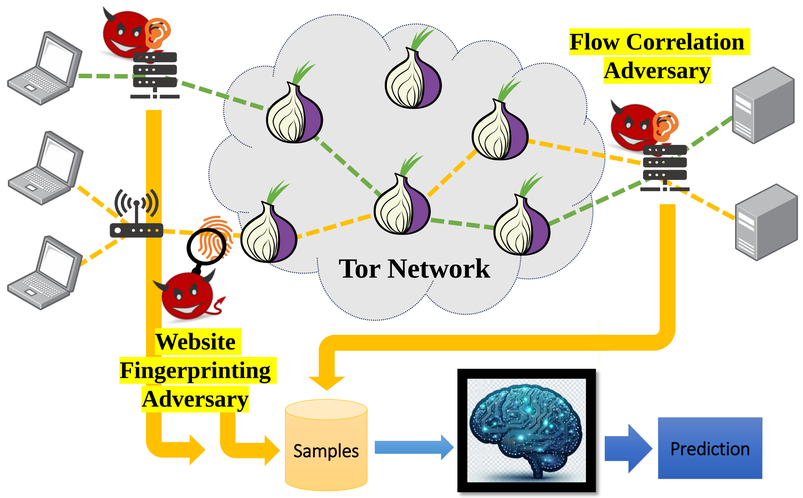
Principal Investigators

Matthew Wright
matthew.wright@rit.edu
Nicholas Hopper
hoppernj@umn.edu
Shanchieh Jay Yang
Jay.yang@rit.edu

Harnessing AI for Advanced Network Security:
From Attacks on Privacy to Defensive Innovations

Research Assistants (Grad.): James K. Holland holla556@umn.edu, Nate Mathews nate.mathews@mail.rit.edu **(Undergrad.):** Annika Clarke, Claire Fischer, Thomas Stone, Justin Kennedy, Zachary Ribback

Privacy Attacks Against Tor



Website Fingerprinting w/ LASERBEAK

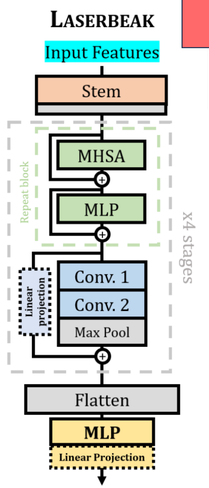
➔ Improving website fingerprinting attack efficacy with advanced **LASERBEAK attack**

➔ **Published in IEEE TIFS 2024,** DOI: 10.1109/TIFS.2024.3468171

★ Hybrid transformer and convolutional neural network architecture, inspired by state-of-the-art language and vision models

★ Multi-channel input that combines fine-grained representation with a variety of traffic processing strategies

➔ **Results:** Up to **+36% attack** efficacy increase against Tor traffic defended with obfuscation



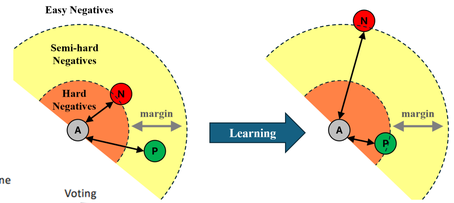
Network Traffic Meta-data as Packet-level Feature Representations

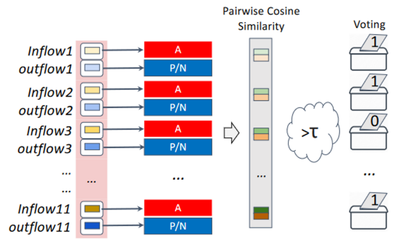
Cumulative Sum of Direction*	1	2	1	0	-1	-2	-3	-2
Direction	+1	+1	-1	-1	-1	-1	-1	+1
Burst Edges	0	0	-2	0	0	0	0	+2
Timestamp*	0.0	0.05	0.3	0.35	0.35	0.4	0.4	0.45
Inter-Arrival Time (IAT)	0.0	0.05	0.25	0.05	0.0	0.5	0.0	0.05
Modified IAT	1.0	1.05	-1.25	-1.05	-1.0	-1.5	-1.0	1.05

Flow Correlation w/ ESPRESSO

★ Build upon insights learned from *LASERBEAK* to advance flow correlation attacks beyond previous *DeepCoFFEA* attack

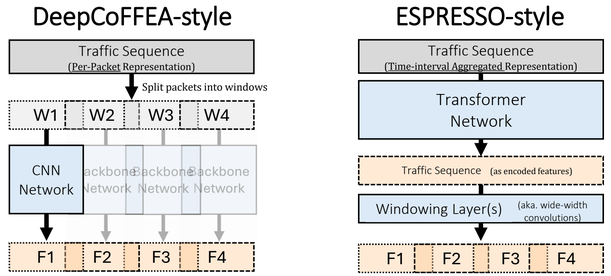
➔ Correlate traffic pairs more effectively using **triplet loss learning** to train feature extractor networks (FENs)

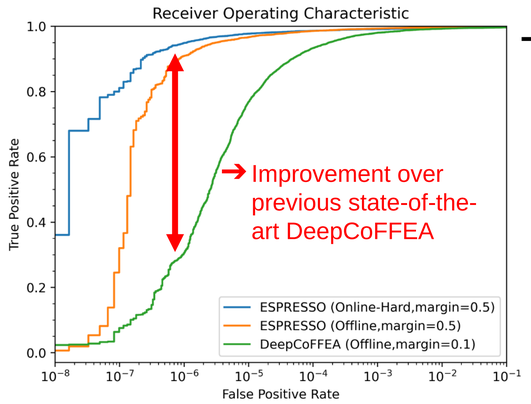




➔ Improve precision by splitting traffic into windows, using **amplification** to reduce false correlations

➔ Use transformer architecture and *time-interval* traffic representation to improve information sharing across windows



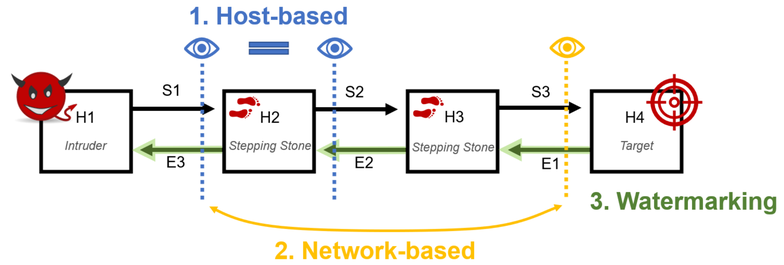


➔ **Results:** Over 90% attack efficacy at *very low* false positive rate

FPR	TPR	
	Deep CoFFEA	ESPRESSO
0.001%	76.8%	96.1%
0.0001%	30.4%	93.1%
0.00001%	7.6%	80.1%
0.000001%	2.3%	66.8%

Stepping-Stone Intrusions

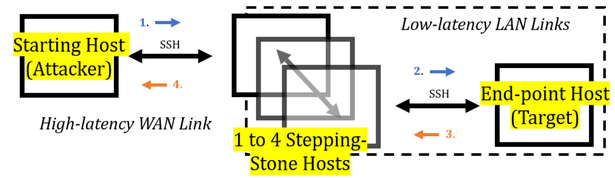
➔ SSI creates tunnels by pivoting traffic through stepping-stones



➔ Frame detection as a traffic correlation problem to link pivoting connections from across different perspectives in the network

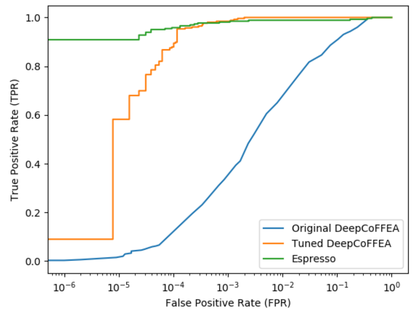
★ Apply *ESPRESSO* for network-based SSI detection

Data Collection & Results

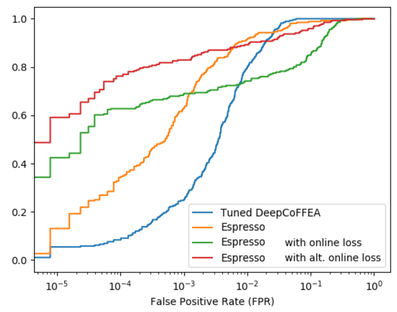


➔ Simulate SSI by constructing tunnels in networked Docker containers
- **Tunnels**: SSH, SOCAT (TCP), dnscat2 (DNS), ptunnelng (ICMP)

SSH-only Intrusions



Mixed-protocol Intrusions



➔ **Results**: Achieves over 90% detection with minimal false alerts for SSH tunnels and exceeds 50% detection for SSI attacks using covert tunneling tools

This project is funded by **NCAE-C-003-2022** under award **#H98230-22-1-0302**.

github.com/notem/Laserbeak-WF-Classifier github.com/notem/ESPRESSO-Flow-Correlation github.com/jkhollandjr/SSID github.com/notem/SSI-Simulator