Stepping-Stone Intrusions can be detected with a much lower false positive rate with DeepCoFFEA

And faster too!

Principal Investigators

Matthew Wright
matthew.wright@rit.edu

Nicholas Hopper
hoppernj@umn.edu

Shanchieh Jay Yang
jay.yang@rit.edu

Students

James Holland
holla556@umn.edu

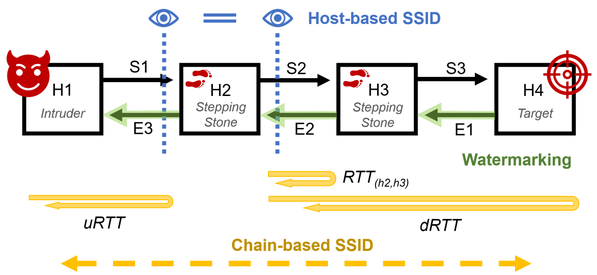
Nate Mathews
njm3308@rit.edu

Annika Clarke
Claire Fischer
Justin Kennedy
Thomas Stone

Introduction

- Stepping-stone intrusions (SSI), also known as pivoting attacks, enable attackers to get into more sensitive systems and networks
- Correlating pairs of traffic flows can be used to identify SSIs
- ★ Leverage our DeepCoFFEA [1] technique for better SSI detection

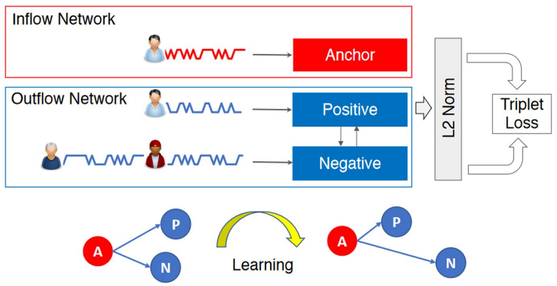
Stepping-Stone Intrusions



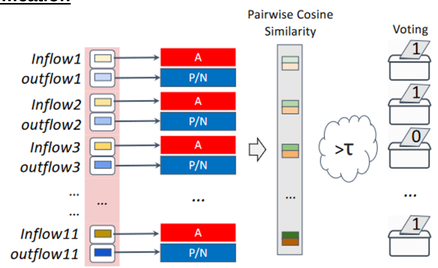
- SSI attacker creates tunnels to target machine by pivoting traffic through stepping-stones
- Limitations of prior research:
  - Unrealistic synthetic datasets
  - Lacking SotA techniques

DeepCoFFEA

- Correlate traffic pairs with much less effort using **triplet loss learning**

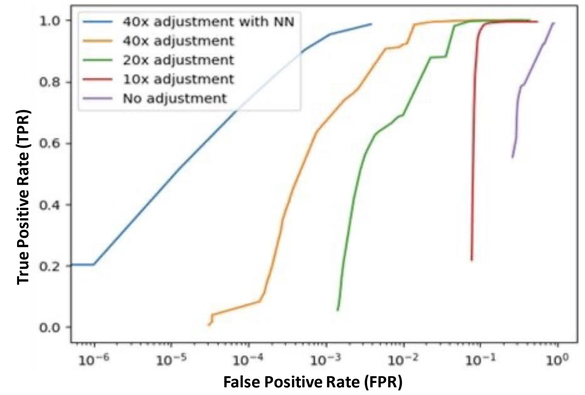


- Improve precision by splitting traffic into time slices and using **amplification**



Adapt DCF to SSID

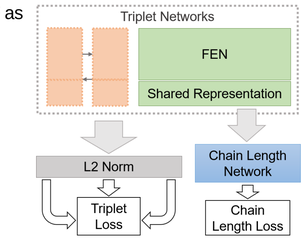
- Modify DCF for improved performance
  - Timestamp scale and window size
  - Replace voting with neural network
  - Improved input representations



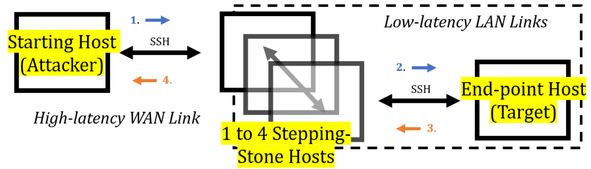
- Significantly outperforms prior SotA [2] at two orders of magnitude faster execution speed

How Long is the SSI Chain?

- Train stand-alone chain-length prediction model
- Integrate with DCF as *multi-task learning* objective



Data Collection



- Develop tool to collect synthetic SSI
  - Docker-based environment with traffic emulating real-world statistics
  - Multiple tunneling protocols
  - github.com/notem/SSI-Simulator
- Building a custom honeynet environment to gather real SSI samples

References

[1] *DeepCoFFEA: Improved Flow Correlation Attacks on Tor via Metric Learning and Amplification* by Oh et al. in S&P'22

[2] *DeepCorr: Strong Flow Correlation Attacks on Tor Using Deep Learning* by Nasr et al. in CCS'2018

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