PivotWall: Combining SDN and Host Context to Defend Against Stepping Stone Attacks

Terrence O’Connor, Akash Verma, William Enck
North Carolina State University
{tjoconno,averma3,whenck}@ncsu.edu

Motivation
Attackers often relay attacks through less sensitive hosts to gain unauthorized access to protected hosts in a network — known as stepping stone attacks.

Network Taint Analysis
PivotWall uses Software Defined Networking (SDN) to gain a network wide perspective.
- SDN Controller acts as a single vantage point with a global view of the network.
- Taint tracking based on flows (src IP, src port, dest IP, dest port, protocol)
- Challenge: How to avoid taint explosion?
  1. Incorporate host-level context to increase tracking precision
  2. Define taint source / sink to minimize the effect of false propagations
     - Taint Source: protected hosts
     - Taint Sink: external network

Flexible Response
SDN provides fast and flexible response to an attack
- Isolate a host by restricting flows to and from its physical port
- Restrict traffic to only specific subnets (e.g., to give time for investigation)
- Redirect traffic to honeynets for analysis
- Dynamically generate network access control rules to address larger threats
- Throttle traffic to specific destinations (e.g., for threats of exfiltration of large amounts of data)

Adding Host-level Context
The PivotWall host agent supplements the network taint analysis by informing the SDN controller of data flows within the host
- SDN controller app informs a host when a new flow is tainted
- Host agent informs the SDN controller app when a new outgoing flow is tainted
- Our current prototype tracks flows on a process and file granularity to balance precision and performance overhead

Research Questions
- How complete is PivotWall in terms of attack coverage?
- How scalable is the solution in varying network sizes?
- What is the performance overhead of Host Agent?
- What is the accuracy of PivotWall in detecting attacks?

Results
- All the attacks that we evaluated against were detected by PivotWall.
- Maximum overhead on Network bandwidth with 100 hosts is 18.27%
- On an average, less than 10% performance overhead on individual hosts.