Detecting Malicious Routers

Alper T. Mızrak, Keith Marzullo, Stefan Savage
University of California, San Diego
Introduction

- Modern packet switched data networks.
- Data forwarded hop-by-hop from router to router towards destination.

- Routers can be compromised,
  To attack on the data plane:
  - E.g. alter, misroute, drop, reorder, delay or fabricate data packets.
Introduction

Goal:
- Fault tolerant forwarding in the face of malicious routers.

Approach:
- Given a routing protocol, the decisions that routers make are predictable.
  ... so this problem is a candidate for anomaly-based intrusion detection

Outline
- Traffic Validation
- Distributed Detection
- Countermeasure
Traffic Validation

- Way to tell that traffic isn’t disrupted en route

Traffic Summary Information:
- How to concisely represent tv_info_r?
- The most precise description of traffic at a router
  - an exact copy of that traffic.
- Many characteristics of the traffic can be summarized far more concisely:
  - Conservation of flow: a counter
  - Conservation of content: a set of fingerprints
  - Conservation of content order: a list of fingerprints
Traffic Validation

- In an idealized network, TV might check
  \[ tv_{info_i} = tv_{info_j} \]
- However, real networks occasionally
  - Lose packet due to congestion.
  - Reorder packets due to internal multiplexing.
  - Corrupt packets due to interface errors.
- Transport protocols deal with such problems.
- TV needs to notice when such behaviors become excessive.
Distributed Detection

- Detect suspicious *path segments*, not individual routers.
- An FD returns a pair \((\pi, \tau)\) where \(\pi\) is a path segment:
  - **\( \alpha\)-Accuracy:** An FD is \( \alpha\)-Accurate if,
    - whenever a correct router suspects \((\pi, \tau)\),
    - then \(|\pi| \leq \alpha\) and some router \(r \in \pi\) was faulty during \(\tau\).
  - **\( \alpha\)-Completeness:** An FD is \( \alpha\)-Complete if,
    - whenever a router \(r\) is faulty at some time \(t\),
    - then all correct routers eventually suspect \((\pi, \tau)\) such that
      - \(|\pi| \leq \alpha\)
      - \(r\) was faulty in \(\pi\) during \(\tau\) containing \(t\).
Protocol $\Pi_{k+2}$

A router $r$ monitors all path segments, $\pi$:
- $\pi$ has $r$ at one end
- $|\pi| \leq k+2$.  
  - $k$ is the maximum number of adjacent faulty routers along a path.

Properties:
- $\Pi_{k+2}$ is $(k+2)$-Accurate:
- $\Pi_{k+2}$ is $(k+2)$-Complete.

Overhead: This algorithm has reasonable overhead
- For each forwarded packet compute a fingerprint.
- Each router must synchronize and authenticate with the other end of each path segment that it monitors.
- Only path segments between nearby routers are monitored.
- Dissemination of the suspected path segments can be integrated into the link state flooding mechanism.
Response

- What happens as a result of a detection?
  - Inform the administrator.
  - Immediate action:
    - Ideally would be part of the link state protocol.
    - That excludes suspected path segments from the routing fabric.

![Diagram](image-url)
Current Status

- We have implemented a prototype system, called *Fatih*.
- Still work-in-progress
The end

- Thank you...
Some protocols

- **WATCHERS [UC, Davis]:**
  - 2-accurate
  - Not complete

- **Highly Secure and Efficient Routing [Avrampoulos et al.]:**
  - 2-accurate
  - 2-complete
  - Extremely expensive: per packet monitoring, source routing, seq numbers, authentication, reserved buffers, timeouts, increase in packet size

- **Early Detection of Message Forwarding Faults [Herzberg et al.]:**
  - 2-accurate
  - 2-complete
  - Suffers from the high overhead.

- **Our own protocol $\Pi_{k+2}$**