Fleet: Defending SDNs from Misbehaving Administrators

Stephanos Matsumoto
Samuel Hitz
Adrian Perrig
Motivation

- The Misbehaving Administrator Problem
  - Administrator affects SDN routing by misconfiguring a correctly functioning controller

- Human error is responsible for 50-80% of all network outages [1]

- Misconfigurations that do not cause outages can be difficult to detect

Fleet's Approach

- The Fleet controller contributes:
  - Threshold signature functionality to switches
  - Resilience by voting on configurations

- Orthogonal Approaches
  - Diversity of hardware/software [2]
  - Policy-based flow rules [3, 4]

Adversary Model

- $k$ misbehaving administrators (out of $n$ total)
  - Network configured to desired level of resilience
  - In practice, $k$ will be small (1 or 2)
- May create policies selecting undesired paths
- Cannot otherwise affect controller operation
Assumptions

- Switches pre-configured with necessary keys
- Administrators:
  - See the same network topology
  - Are loosely time-synchronized
  - Securely communicate out-of-band
  - Share the same routing policy if not malicious
Fleet Controller Architecture

- Intra-Controller Link
- Controller-Switch Link

Administrator Layer

Switch Intelligence Layer

Data Plane (Switches/Links)

Fleet Controller

Admin 1
Admin 2
Admin 3

Shared Data Storage

Controller-Switch Link

Intra-Controller Link
Routing with the Fleet Controller

- Single-configuration
  - Voting protocol using threshold signatures

- Multi-configuration (details in paper)
  - Sources or ingress switches can select per-flow routes
Single-Configuration Approach

--- Intra-Controller Link
--- Controller-Switch Link

Administrator Layer

Switch Intelligence Layer

Data Plane (Switches/Links)

Fleet Controller

Shared Data Storage

Proposal

Admin 1

Admin 2

Admin 3

C

C

C

C

C

KS₁

KS₂

KS₃

Switches/Links

ETH Zürich
Evaluation

- Prototype implementation in Python-based POX controller and Mininet SDN framework
- Tested on random topologies of 20 switches and 50 hosts
- Main question: what dominates recovery time?
Evaluation

- Key size affects voting protocol length
- Successful vote takes less than 1s

![Graph showing time in milliseconds for different numbers of administrators and key sizes](image_url)
Evaluation

- Link failure detection time dominates recovery
Conclusions

- Fleet protects against misconfigurations with little overhead
- Switch intelligence enables useful switch functionality, such as threshold signatures
- Companies can expand their networks to locations where admins may not be as trusted

Thank you! Questions?