Malachite: Firewall Policy Comparison

Dinesha Ranathunga*, Matthew Roughan*, Phil Kernick**,
Nick Falkner*,
* University of Adelaide
** CQR Consulting

Motivation

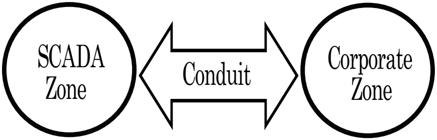
- Current networks depend on *firewalls* to mitigate cyber attacks
  - especially SCADA networks
- Supervisory Control And Data Acquisition networks
  - core to a nation's critical infrastructure
    e.g., power, water, wastewater
  - designed for robustness, real-time performance
  - **NOT** secure

Motivation cont.

- Industry standards exist (*eg.*, Guide to Industrial Control Systems Security by NIST, ANSI/ISA-62443-1-1) for
  - firewall architectures
  - service-specific policies
  - network segregation
- **NO** standards for checking compliance
- Serious firewall misconfigurations are frequent
  - Wool studied 74 corporate firewalls, >80% had serious errors
  - we studied 9 real SCADA firewalls, 100% had serious errors

Existing standards

ANSI/ISA Zone-Conduit model [ANSI/ISA-62443-1-1]:



- **Zone** - groups systems with similar security requirements
  - single zone policy
- **Conduit** - secure communication path between zones
  - firewalls are part of the conduits
- Allows to construct network-wide high-level security policy

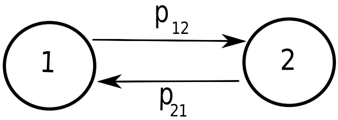
Need automated firewall-policy comparison

- Multiple benefits
  - check best-practice compliance
  - change-impact analysis
  - evaluate multiple policy-designs
- Malachite: mathematical-framework based comparisons
  - precise and unambiguous
  - rule-order independent

Comparison of network policy: a simple example

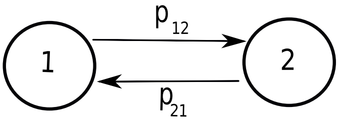
Implemented firewall policy

$\mathcal{P} = (G_1, P_1)$

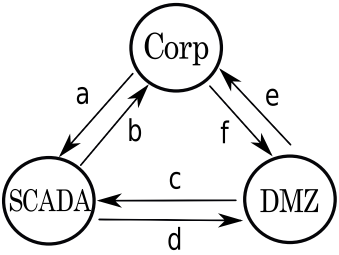


Comparison of network policy: a simple example

Implemented firewall policy
$\mathcal{P} = (G_1, P_1)$



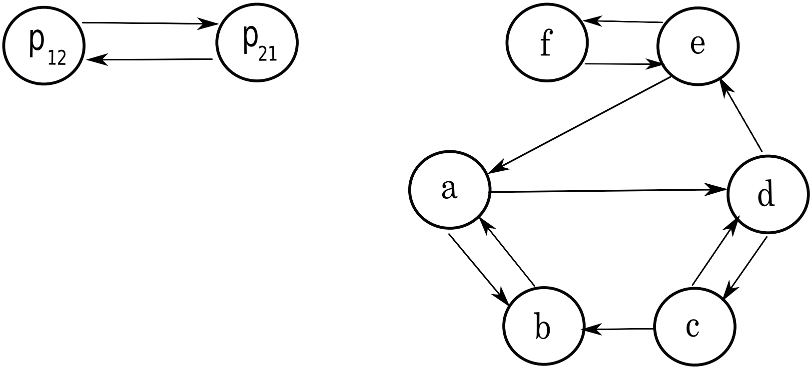
Best-practice firewall policy
$\mathcal{RP} = (G_2, P_2)$



- Is $\mathcal{P}$ equally or more restrictive than $\mathcal{RP}$?

Workaround: use Line Digraphs (LDs)

$\mathcal{L}(G_1)$ $\mathcal{L}(G_2)$



- LD isomorphism $\implies$ potential original-graph isomorphism
  - Harary and Norman 1960

- Compliant if *included* or *incorporated* by best-practice policy

Definition (Partial Incorporation)

If $\mathcal{P} = (G_1, P_1)$, $\mathcal{RP} = (G_2, P_2)$, *policy* $\mathcal{RP}$ partially incorporates $\mathcal{P}$ *iff* G_1 *is a subgraph of* G_2 *and* $\forall e \in G_1$, $p_1^e \subset p_2^e$. *We denote this by* $\mathcal{P} \subset \mathcal{RP}(G_1)$.

Implementation

Is $\mathcal{P} \subset \mathcal{RP}(G1)$? where $\mathcal{P} = (G_1, P_1)$, $\mathcal{RP} = (G_2, P_2)$

1. Derive *semantic partitions* SP_1, SP_2
   - partitions policy into equivalence classes
   - *e.g.*, $SP1 = \{e_1, e_2\};\ e_1 = \{p_{12}\}, e_2 = \{p_{21}\}$
2. Check $SP_1 \subset SP_2$
3. Find all feasible partition-mappings
4. Construct adjacency matrices A_1, A_2 of LDs per mapping
5. If $A_1 = A_2$ then $\mathcal{P} \subset \mathcal{RP}(G1)$

Application to real SCADA case studies

SUC	Firewalls	Zones	Conduit-policies	Equivalence classes	Maximum class size	$\mathcal{RP}$ Compliant?
1	3	7	22	12	7	✘
2	6	21	162	87	8	✘
3	4	10	34	15	8	✘
4	3	9	32	16	5	✘

- large equivalence class sizes $\implies$ an inefficient network.

Conclusions

- Many obstacles to firewall-policy comparison
- Malachite addresses these challenges
  - network and vendor independent policy semantics
  - derives canonical policies for comparison
- Limitations
  - best practice may not always be correct
  - inclusion/incorporation may not always indicate compliance
  - some human intervention still required

Bibliography

[1] E. S. Al-Shaer and H. H. Hamed. “Discovery of policy anomalies in distributed firewalls”. In: *Annual Joint Conference of the IEEE CCS*. INFOCOM. 2004, pp. 2605–2616.

[2] ANSI/ISA-62443-1-1. *Security for Industrial Automation and Control Systems Part 1-1: Terminology, Concepts, and Models*. 2007.

[3] L. Babai. “Graph isomorphism in quasipolynomial time”. In: *arXiv preprint arXiv:1512.03547* (2015).

[4] E. Byres, J. Karsch, and J. Carter. “NISCC good practice guide on firewall deployment for SCADA and process control networks”. In: *NISCC* (2005).

[5] K. D. Gourley and D. M. Green. “Polygon-to-rectangle conversion algorithm.” In: *IEEE CGA* (1983), pp. 31–32.

[6] J. D. Guttman and A. L. Herzog. “Rigorous automated network security management”. In: *IJIS* 4.1-2 (2005), pp. 29–48.

[7] F. Harary and R. Z. Norman. “Some properties of line digraphs”. In: *Rendiconti del Circolo Matematico di Palermo* 9.2 (1960), pp. 161–168.

[8] C. D. Howe. *What’s Beyond Firewalls?* Forrester Research, Incorporated, 1996.

[9] H. Hu et al. “Flowguard: Building robust firewalls for software-defined networks”. In: *Proceedings of the third workshop on Hot topics in software defined networking*. ACM. 2014, pp. 97–102.

Bibliography (cont.)

[10] D. S. Johnson. "The NP-completeness Column". In: *ACM Transactions on Algorithms* 1.1 (July 2005), pp. 160–176. ISSN: 1549-6325. DOI: 10.1145/1077464.1077476. URL: http://doi.acm.org/10.1145/1077464.1077476.

[11] A. X. Liu and M. G. Gouda. "Diverse firewall design". In: *Parallel and Distributed Systems, IEEE Transactions on* 19.9 (2008), pp. 1237–1251.

[12] D. Ranathunga et al. "Identifying the Missing Aspects of the ANSI/ISA Best Practices for Security Policy". In: *1st ACM Workshop on Cyber-Physical System Security (CPSS)*. ACM. 2015, pp. 37–48.

[13] D. Ranathunga et al. "Malachite: Firewall policy comparison, http://bandicoot.maths.adelaide.edu.au/public/PolicyComparison.pdf". In: *21st IEEE Symposium on Computers and Communications*. 2016.

[14] A. Wool. "A quantitative study of firewall configuration errors". In: *Computer, IEEE* 37.6 (2004), pp. 62–67.

[15] A. Wool. "Architecting the Lumeta Firewall Analyzer." In: *USENIX Security Symposium*. 2001, pp. 85–97.

Firewall policy rule representation

$$p_A(s) = \begin{cases} s, & \text{if } s \in A, \; // \; accept \\ \phi, & \text{if } s \in A^c, // \; deny. \end{cases} \quad (1)$$

- $A \subset \mathcal{A}$ where $\mathcal{A}$={Atomic packet sequences}
- Only consider packet modifications that don't effect other rules (e.g., QoS, TTL changes)
  - no NAT, VPN functionality
  - no creation of packets by rules (e.g., logging)

Zone-Conduit policy snippet

Policy p_0 { Z1 $\rightarrow$ Z2: https, dns;
Z2 $\rightarrow$ Z1: http; }

- Positive, explicit policies conditional on an implicit deny-all rule

Conduit-policy comparison

Definition (Equivalence)

Two policies p^X *and* p^Y *are* equivalent *on* $\mathcal{A}$ *iff* $p^X(s) = p^Y(s)$, $\forall s \in \mathcal{A}$. *We denote this equivalence by* $p^X \equiv p^Y$.

Definition (Inclusion)

A policy p^X *is* included *in* p^Y *on* $\mathcal{A}$ *iff* $p^X(s) \in \{p^Y(s), \phi\}$, *i.e.,* X *has the same effect as* Y *on* s*, or denies* s*, for all* $s \in \mathcal{A}$. *We denote inclusion by* $p^X \subset p^Y$.

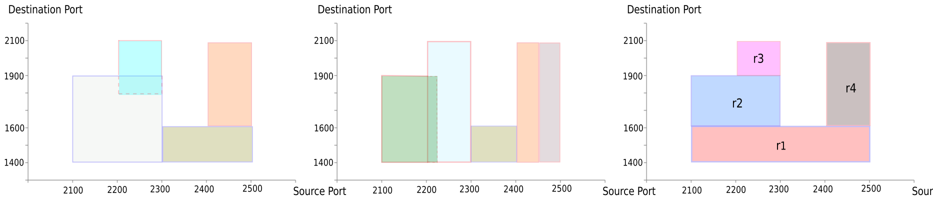
Canonical policies

Lemma

Policies $p^X \equiv p^Y$ *iff* $c(p^X) = c(p^Y)$.

- $c : \Phi \rightarrow \Theta$, where Φ is the policy space and Θ is the canonical space of policies

Canonicalisation of distinct rule sets of a policy



- Policy polygon horizontally partitioned using a Polygon to Rectangle conversion algorithm

Time complexity analysis of policy equivalence

algorithm component	time complexity	comments
cannonicalise policy	$O(n)$	$n =$ policy count
construct line digraph	$O(n^2)$	
derive SPs	$O(n^2)$	
check partitions are equal	$O(m^2)$	$m =$ equiv class count
evaluate mappings	$O(\prod_{i=1}^{m} c_i!)$	$c_i = \lvert e_i \rvert$

- Worse case time complexity: $O(n!)$, best case: $O(n^2)$

Semantic partitions

Definition

The semantic partition *SP of a set of policies P is given by $SP = \{e_m\}$ where $P = \cup_m e_m$ and the $e_m \subset P$ are the minimal number of equivalence classes, i.e., for all $p_i, p_j \in e_m$ we have $p_i \equiv p_j$.*

Definition (plain)

[SP Equivalence and Inclusion] The semantic partitions SP_1 and SP_2 of policies P_1 and P_2, respectively, are equivalent *iff $|SP_1| = |SP_2|$ and $\forall e_1 \in SP_1, \exists e_2 \in SP_2$ such that for any $p_1 \in e_1$ and $p_2 \in e_2$, we have $p_1 \equiv p_2$. We denote this by $SP_1 \equiv SP_2$.*
Semantic partition SP_1 includes *SP_2 iff $\forall e_2 \in SP_2\ \exists e_1 \in SP_1$ s.t. $e_2 \subset e_1$. We denote this by $SP_2 \subset SP_1$.*

Semantic difference

Definition

The semantic difference between policies p^X *and* p^Y *is given by* $p^X - p^Y = (p^X \oplus p^Y) \otimes (p^X \otimes p^Y)^c$, *where* $(p_A)^c = p_{A^c}$ *and* A^c *is* A*'s complement.*

Example SUC Zone-Conduit model