Verifiable Policy-Defined Networking for Security Management

Dinesha Ranathunga*, Matthew Roughan*, Phil Kernick**, Nick Falkner*, Hung Nguyen*, Michelle McClintock*, Marian Mihailescu*

* University of Adelaide

** CQR Consulting

Motivation

- Policy Defined Networking (PDN) paradigm exists

What's missing?

- We need be be really sure network is managed correctly
  - particularly it's security

Why aren't we sure?

- Lack of Verifiability
  - *E.g.*, is the policy correctly mapped to network devices?[1]

[1] D. Ranathunga et al. "The Mathematical Foundations for Mapping Policies to Network Devices". In: *SECRYPT*. 2016.

What should we verify?

- Policy is correct
- Policy is compatible with target network and technology
- Expected security outcome prior to deployment
- Expected security outcome post-deployment

Verify policy is correct

Need

- Transparency
- Human-comprehensible policy
- Specialisation within networking

Verify policy compatible with network and technology

- Target network may be different to that perceived
- Underlying technology may not support policy
- We developed a mathematical framework to check compatibility[2]

[2] D. Ranathunga et al. "Malachite: Firewall policy comparison". In: *21st IEEE Symposium on Computers and Communications*. 2016.

Pre-deployment verification

- Policy-author oversights can cause security holes
- Check expected security outcome using
  - emulated networks
  - pathological traffic tests

Post-deployment verification

- Policy may still not work as expected post-deployment due to
  - software bugs
  - upgrade and/or patching
- Monitor security status using firewall reports[3]

[3] D. Ranathunga et al. "Towards Standardising Firewall Reporting". In: *1st Workshop on the Security of Cyber Physical Systems (WOS-CPS)*. LNCS. 2015.

Conclusions

- Lack of verifiability in Policy Defined Networking (PDN) renders little assurance that the expected security outcome is consistent pre- and post-deployment
- We propose Formally-Verifiable PDN with verifiability built in to overcome the shortfall

Bibliography

[1] C. J. Anderson et al. "NetKAT: Semantic foundations for networks". In: *ACM SIGPLAN Notices* 49.1 (2014), pp. 113–126.

[2] Anonymous. *Identifying the missing aspects of the ANSI/ISA best practices for security policy, http://tinyurl.com/q4hjoxs*.

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

[4] Y. Bartal et al. "Firmato: A novel firewall management toolkit". In: *ACM TOCS* 22.4 (2004), pp. 381–420.

[5] BBC. *Hack attack causes 'massive damage' at steel works, http://www.bbc.com/news/technology-30575104*.

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

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

[8] D. Ranathunga et al. "Malachite: Firewall policy comparison". In: *21st IEEE Symposium on Computers and Communications*. 2016.

[9] D. Ranathunga et al. "The Mathematical Foundations for Mapping Policies to Network Devices". In: *SECRYPT*. 2016.

Bibliography (cont.)

[10] D. Ranathunga et al. "Towards Standardising Firewall Reporting". In: *1st Workshop on the Security of Cyber Physical Systems (WOS-CPS)*. LNCS. 2015.

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