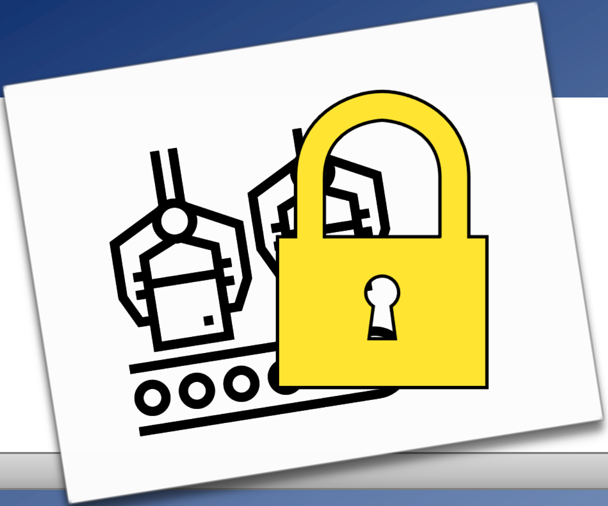

Enhancing Security and Privacy with In-Network Computing

https://www.ietf.org/id/draft-fink-coin-sec-priv-03.txt

Ina Fink, Klaus Wehrle

COIN RG @ IETF 112, November 11 2021

Scope of this Draft and What's New

Protection Mechanisms

Intrusion & Anomaly Detection

Network Monitoring

- Idea: Implement security and privacy mechanisms in the network
  - Performance and security enhancements in comparison to middle boxes: low latency, high scalability, fast reaction close to source, …
  - Use cases:
    - Retrofit security for resource-restricted or legacy devices
    - Industrial networks with high performance requirements
    - Scalable and transparent anonymization
- Goal of draft: Provide insight into potential, research questions and challenges

Draft v03: Recent related work with practical examples for research & applications

https://www.ietf.org/id/draft-fink-coin-sec-priv-03.txt

Update: Related Work w.r.t. Encryption and Integrity Checks

Protection Mechanisms

Intrusion & Anomaly Detection

Network Monitoring

Secure cryptographic functions not supported by current programmable switches by design *but*:

- Chen et al. (2020) [1]: AES encryption with scrambled lookup tables on P4-based hardware switches
- Yoo et al. (2021) [2]: Cryptographically secure keyed hash functions on P4-based hardware switches

→ Foundation for security and privacy applications, e.g., security protocols, onion routing, message authentication

1. Chen, X., "Implementing AES Encryption on Programmable Switches via Scrambled Lookup Tables", In Proceedings of the SIGCOMM 2020 Workshop on Secure Programmable Network Infrastructure, August 2020.
2. Yoo, S. and X. Chen, "Secure Keyed Hashing on Programmable Switches", In Proceedings of the ACM SIGCOMM 2021 Workshop on Secure Programmable Network Infrastructure, August 2021.

Update: Related Work w.r.t. Authentication

Protection Mechanisms

Intrusion & Anomaly Detection

Network Monitoring

(Continuous) authentication in the network without latency overhead or middle-boxes

Almaini et al. (2021) [3]: Authentication in the data plane of P4-based hardware switches

- ➢ Port-knocking
- ➢ One-Time-Password

3. Almaini, A., Al-Dubai, A., Romdhani, I., Schramm, M., and A. Alsarhan, "Lightweight edge authentication for software defined networks", Computing 103, 291-311 (2021), August 2020

Update: Related Work w.r.t. Anonymization

Protection Mechanisms

Intrusion & Anomaly Detection

Network Monitoring

Scalable, transparent and light-weight anonymization

- Moghaddam et al. (2019) [4]: Use P4-based hardware switches to rewrite source addresses and hide path information, e.g., using randomization
- Wang et al. (2020) [5]: Encrypt IPv4 addresses to obfuscate traffic on P4-based hardware switches

→ Address performance and usability issues of existing anonymity tools

4. Moghaddam, H. and A. Mosenia, "Anonymizing Masses: Practical Light-weight Anonymity at the Network Level", arXiv:1911.09642 [cs.CR], November 2019.
5. Wang, L., Kim, H., Mittal, P., and J. Rexford, "Programmable In-Network Obfuscation of Traffic", arXiv:2006.00097 [cs.NI], 2020.

Update: Related Work w.r.t. IDS

Protection Mechanisms

Intrusion & Anomaly Detection

Network Monitoring

In-line detection of and reaction to anomalies, reduce load on Intrusion Detection Systems (IDS)

- Lewis et al. (2019) [6]: Outsource IDS functionality / preprocessing to P4-based software switches to reduce load on subsequent IDS
  - ➢ Rule-based prefiltering based on data plane
  - ➢ Up to 75% traffic reduction at IDS

6. Lewis, B., Broadbent, A., and N. Race, "P4ID: P4 Enhanced Intrusion Detection", 2019 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN), November 2019.

Update: Related Work w.r.t. Network Monitoring

Protection Mechanisms

Intrusion & Anomaly Detection

Network Monitoring

Efficient network monitoring, e.g., used for network forensics

- Sonchack et al. (2018) [7]: Flow monitoring with P4-based hardware switches
  - ➢ Preprocess packets in the data plane
  - ➢ Create flow records in the control plane

→ High performance, cost-efficient

[7] Sonchack, J., Aviv, A., Keller, E., and J. Smith, "Turboflow: Information Rich Flow Record Generation on Commodity Switches", In Proceedings of the Thirteenth EuroSys Conference, April 2018.

Conclusion

- Increasing interest of the research community
- Recent publications show relevance and feasibility
  - High-ranked venues (USENIX Security, SIGCOMM SPIN Workshop, EuroSys, …)
  - First proofs of concept using **programmable hardware switches**
  - Hot research topic, many ideas left to investigate
- Draft indicates broad and valuable potential of COIN

Strongly looking for feedback and / or contributions to drive this draft forward

Ina Fink
fink@comsys.rwth-aachen.de