Enhancing Security and Privacy with In-Network Computing

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

Ina Fink, Klaus Wehrle
Scope of this Draft and What’s New

- 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
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

---


[https://www.ietf.org/id/draft-fink-coin-sec-priv-03.txt](https://www.ietf.org/id/draft-fink-coin-sec-priv-03.txt)
Update: Related Work w.r.t. Authentication

Protection Mechanisms

(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

Intrusion & Anomaly Detection

Network Monitoring


https://www.ietf.org/id/draft-fink-coin-sec-priv-03.txt
**Update: Related Work w.r.t. Anonymization**

### Protection Mechanisms

- **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

### Intrusion & Anomaly Detection

### Network Monitoring


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


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


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

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