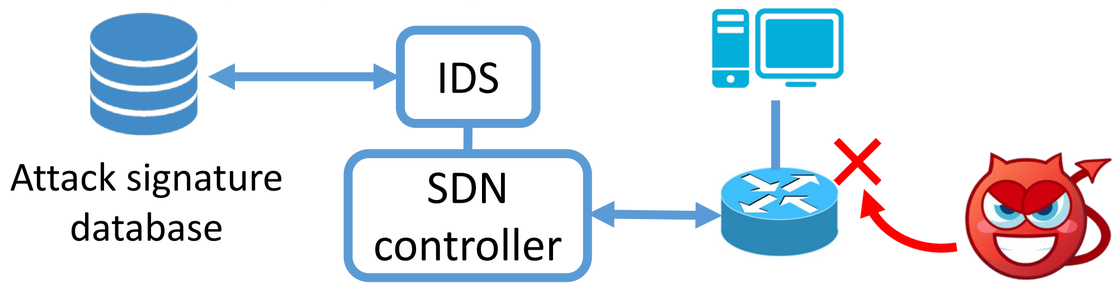
Efficient & Effective Network Protocol Attack Signature Generation for SDN Based Intrusion Detection Systems

Qi Alfred Chen and Z. Morley Mao, University of Michigan

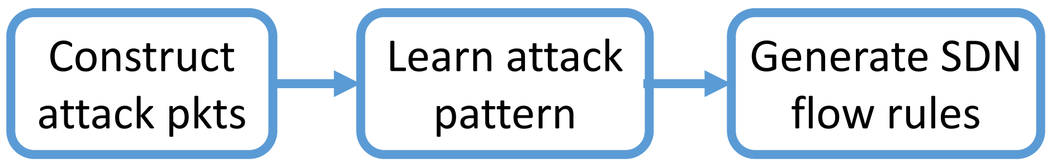
SDN-based IDS

- **Network protocol attacks**: a big threat today
  - New variants of fast TCP packet injection: [Qian et al., S&P'12], [Qian et al., CCS'12], PacketGuardian [Chen et al., CCS'15]
  - NTP time shifting attack [Malhotra et al., NDSS'16]
  - Read & modify TLS traffic by downgrade attack: FREAK, Logjam [Adrian et al., CCS'15]
- To protect clients, deploy **IDS with SDN support** to flexibly specify and update attack signatures



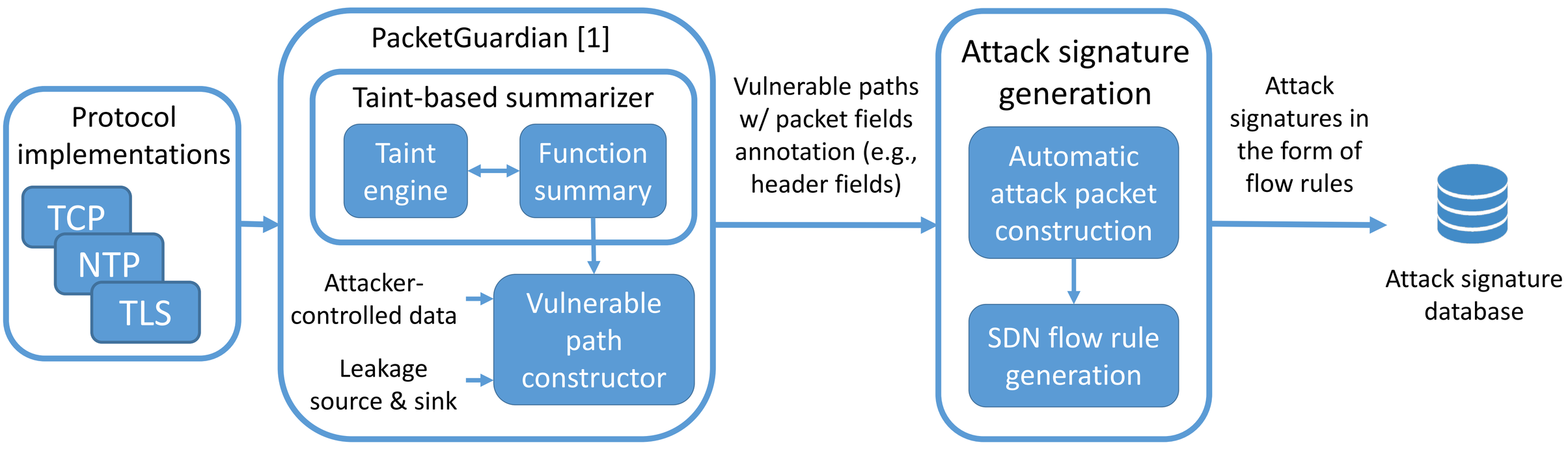
Challenge: Attack signature generation

- Lack of efficient and effective approach to identify vulnerabilities
  - Manual approach: slow, error prone
- Non-trivial to translate from vulnerabilities to signatures for SDN apps



- Need to support different implementations: make traditional approach even harder to scale
  - Attack patterns can be very different due to implementation details [Qian et al., CCS'12], [Chen et al., CCS'15]
- ***Call for a more efficient and effective approach***

Efficient & effective attack signature generation with static analysis



[1] Static Detection of Packet Injection Vulnerabilities -- A Case for Identifying Attacker-controlled Implicit Information Leaks
Qi Alfred Chen, Zhiyun Qian, Yunhan Jack Jia, Yuru Roy Shao, Z. Morley Mao
Proceedings of ACM Conference on Computer and Communications Security (CCS) 2015.

Initial progress

- **Attack type**: off-path packet injection attack
- **Codebases**:
  - Linux kernel TCP, SCTP, and DCCP
  - RTP: oRTP, PJSIP, VLC
- **Results**: Able to efficiently output vulnerable paths, allowing us to identify both ***known vulnerabilities*** and ***a number of new ones***
  - 17 new TCP packet injection attack paths
  - 2 of 3 RTP implementations found vulnerable

Next step

- Automatically construct attack packets
  - Applying constraint solving techniques, e.g., SMT solver in symbolic execution
- Learn signatures & generate flow rules that are directly usable in SDN-based IDS app
- Tool improvement:
  - Support more classes of network attacks
    - Heartbleed, NTP attack, etc.
  - Support binary analysis

INFORMATION TRUST INSTITUTE
ILLINOIS
SCIENCE OF SECURITY VIRTUAL ORGANIZATION