Testbed Evaluation of an Attestation-Capable, Programmable Software Switch

Alexander Wolosewicz, Nishanth Shyamkumar, Nik Sultana

ILLINOIS INSITUTE OF TECHNOLOGY

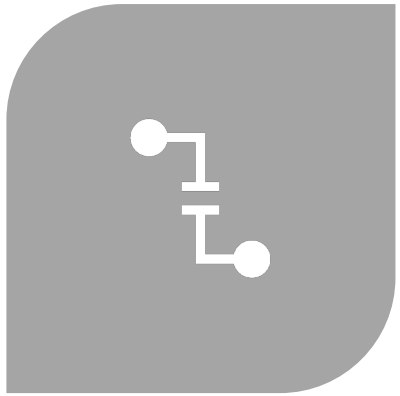
Thank you: Mohammad Firas Sada (IIT), Sean Cummings (IIT), Hyunsuk Bang (IIT), Chris Neely (AMD/Xilinx), Ben Ujcich (Georgetown), Deborah Shands (SRI), Vinod Yegneswaran(SRI), Ashish Gehani (SRI), the FABRIC testbed operators, and INDIS organizers.
Partial support from the Defense Advanced Research Projects Agency (DARPA) under Contract No. HR0011-19-C-0106. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of funders.

Programmability in Switches

- A shift from Fixed function ASICs to Programmable ASICs.
- Flexibility in packet protocols, quick prototyping, and fast time to deploy.
- **Programmable nature of switch introduces security concerns.**
- Corruption of packets, dropping packets or modifying the dataplane.

Identifying a compromised network

FRAMEWORK AS MENTIONED IN 'A CASE FOR REMOTE ATTESTATION IN PROGRAMMABLE DATAPLANES'
(FOLLOW THE QR CODE)



END HOSTS CREATE A CHALLENGE, AND THE PROGRAMMABLE NETWORK DYNAMICALLY RESPONDS

ATTESTER CREATES THE EVIDENCE, VERIFIER CONFIRMS THE EVIDENCE IS CORRECT, THE END HOSTS ARE INFORMED OF THE VERIFICATION RESULT

Mechanics of Remote Attestation

- Identifying the state that is used to generate the evidence
- The final representation of the evidence
- How is the evidence shared with other participating nodes in the remote attestation framework
- In-band / Out-of-band
- See our prior papers for further details:

Working, Open-Sourced Implementation!

Open-source fork of the BMv2 **software switch**:
https://github.com/awolosewicz/bmv2-remote-attestation

Uses IPv6 extension headers (Hop by Hop) to encode the required evidence in the packet.

Prevents a malicious P4 program from modifying the generated evidence.

Come to our Demo on Tuesday (11/14) at 4:40pm at the Showfloor of SCInet Theater (Booth 1275).
Or contact us for more information.