The behavior of network equipment has been subverted in attacks that surreptitiously reconfigured the equipment to enable subsequent attacks.

We need a systematic way to recognize that the configuration of network devices is not aligned with our instructions.

Using Remote Attestation we can enable dynamic assessment of network security and configuration characteristics.

**Motivation**

1) Adapt third-party, “black box” equipment to provide verifiable evidence about its configuration and behavior.
2) Construct a stateful, secure network function that provides this functionality at line rate.
3) Design distributed systems that can validate evidence integrity of multiple target switches to detect tampering.

**Approach**

- Two AMD-Xilinx U280 Smart NICs are used to “sandwich” a switch that is treated as a “black box”.
- Control Planes of Xilinx U280 (consumers) synchronously retrieve configuration from the host of black-box switches (producer) and updates lookup tables on Xilinx U280s.
- Ingress Xilinx U280 embeds the switch evidence into the packet.
- Egress Xilinx U280 verifies the integrity of evidence to detect alterations through checksum calculation and P4 lookup table.
- Python scripts automate site and network configurations for ease of implementation and result reproducibility.

**Results**

- We used 12 Xilinx U280s, configured as shown in Fig 1.
- We compare the HBH header (Fig 2) as seen at the receiver and verify that the state values have been transmitted successfully and correctly.
- We monitor the output from the egress Xilinx U280 to see whether a predicted/unpredicted changes has been made
- We use iperf (Fig 3) across the first ingress sites and the last egress sites. The software switch is the performance bottleneck.

We thank the KNIT8 organizers for a travel stipend that enabled the first author to present this work in person.

**References**

http://transparnet.cs.iit.edu/