SC24 Network Research Exhibition: Demonstration Abstract

In-Network Remote Attestation for ScienceDMZ

Hyunsuk Bang, Illinois Institute of Technology
Chris Neely, AMD Inc
Nik Sultana, Illinois Institute of Technology

Abstract

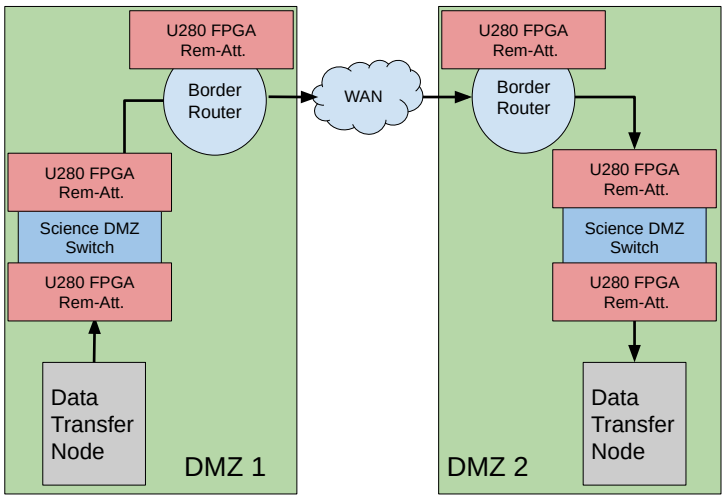
Modern scientific research often involves large data transfers between research institutions, but these transfers can be hindered by network appliances at the institutions' network perimeter. The ScienceDMZ network design pattern removes some "friction" to these transfers by placing transfer nodes in the DMZ, but in some institutions, this creates a tension with their site security policy, and generally requires more careful vetting of the machines in the ScienceDMZ. This demo showcases a new idea: adapting the concept of "Remote Attestation" to machines in the ScienceDMZ to improve their security and compliance. This involves in-band control signaling of transfer authorization information across two research institutions. The rest of this paper outlines what form this Remote Attestation takes, and how it is being adapted for ScienceDMZ.

Description

This demo uses the FABRIC testbed to carry out a large data transfer between two servers and shows how to secure that transfer using Remote Attestation. Those servers represent Data Transfer Nodes (DTNs) in two ScienceDMZs [1]. The sending DTN uses DPDK to create a 100Gbps data stream to the receiving DTN.

In this setting, Remote Attestation [2] involves creating a digest of the sending system's configuration and using that for making forwarding decisions at both ends of the transfer. This is all done "in the network" – meaning that the DTNs are oblivious to this logic. In our demo, this logic is carried out on U280 Alveo FPGA cards. These cards have 2x100Gbps Ethernet ports and provide a flexible and low-overhead platform for high-throughput network experiments.

In our demo, these cards interpose on the traffic between two DTNs and carry out the attestation and verification logic. Our demo also shows how failure modes are handled – that is, in case a transfer is not authorized, or if its authorization only covers a smaller bandwidth allocation.



The diagram shown above captures the setup. The Alveo cards are connected to existing network equipment to carry out Remote Attestation and encrypt attestation records for remote verification. This demo forms part of research that is described at http://transparnet.cs.iit.edu/

Goal

The demo shows a DTN-style 100Gbps transfer across FABRIC sites – for example, between FABRIC's New York and Los Angeles nodes – and measures the overhead induced by the attestation logic.

Resources

All the resources needed by this demo are obtained from the FABRIC testbed, and this demo can be reproduced by other FABRIC users. These resources consist of high-capacity network links, U280 Alveo FPGA cards, and VM resources for configuring those cards and for carrying out the data transfer. For SC24, we plan to use the mobile FABRIC site provided by Ciena. That site will be managed through FABRIC's existing control interface (requiring only a minor configuration change for our demo to use this node).

Results

This experiment used four U280 Alveo FPGA cards and two Mellanox ConnectX-6 network adapters, all provisioned by the FABRIC testbed. The FPGA cards are deployed across four sites: MICH, UTAH, NCSA, and CLEM, with traffic flows generated sequentially in this order. The sites MICH, UTAH, and NCSA belong to DMZ1, while CLEM is part of DMZ2. The U280s positioned between the black-box switches handle remote attestation, while the two U280s located at the edge encrypt attestation data. Additionally, the edge U280s on NCSA and CLEM perform stateful network functions, such as counting the number of packets processed under a specific event ID and calculating the time intervals between consecutive packets.

The sender node generates traffic, and the number of packets and bytes processed by each U280 is recorded. To assess the U280's performance impact, two scenarios are considered. In the first scenario, the U280 simply forwards packets from one port to another without processing. In the second scenario, the U280 receives packets from one port, processes them with synthesized artifacts, and then transmits them to the other port. Both scenarios are recorded five times, with throughput averaged over one-minute intervals. Since this experiment focuses on DTNs between two science DMZs – where most traffic consists of elephant flows – a packet size of 1024 bytes is used.

	MICH (DMZ1)	UTAH (DMZ1)	NCSA (DMZ1)	CLEM (DMZ2)
1	97.91	94.13	94.15	92.81
2	97.70	94.00	94.04	92.69
3	97.74	94.02	94.05	92.86
4	97.87	94.13	94.12	93.20
5	97.85	94.10	94.14	93.25

Throughput when bypassing P4 application (Gb/s),

	MICH (DMZ1)	UTAH (DMZ1)	NCSA (DMZ1)	CLEM (DMZ2)
1	97.92	94.64	94.66	93.62
2	97.82	94.56	94.60	93.42
3	97.93	94.68	94.72	93.70
4	98.01	94.67	94.72	93.93
5	98.02	94.70	94.70	93.57

Throughput with P4 application (Gb/s)

The results indicate that the remote attestation network function does not adversely affect the throughput of the data being transferred. Some level of throughput degradation is expected when conducting experiments on the FABRIC testbed since the infrastructure is usually shared with other users. Performance can vary depending on how the experiment's network topology is mapped to FABRIC's infrastructure. However, in a controlled lab environment, the same artifact design achieves line-rate performance consistently, regardless of packet size.

Conclusion

The results from our demonstration of in-network remote attestation for ScienceDMZs showed an approach that balances high-speed data transfers with a novel idea to safeguard the data's integrity. This demonstration was conducted using the FABRIC testbed and showed that the U280 Alveo FPGA cards can handle attestation operations with stateful in-network packet processing at line-rate speeds. Future work will focus on refining the attestation mechanisms and expanding the range of stateful functions.

Acknowledgement

We thank Nishanth Shyamkumar, Mert Cevik, and the NRE organizers for technical assistance. This work was supported by the National Science Foundation (NSF) under award 2346499. 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.

References

[1] Eli Dart, Lauren Rotman, Brian Tierney, Mary Hester and Jason Zurawski, "The Science DMZ: A network design pattern for data-intensive science," *SC '13: Proceedings of the International Conference on High Performance Computing, Networking, Storage and Analysis*, Denver, CO, USA, 2013, pp. 1-10, doi: 10.1145/2503210.2503245.

[2] Nik Sultana, Deborah Shands, and Vinod Yegneswaran. 2022. A case for remote attestation in programmable dataplanes. In Proceedings of the 21st ACM Workshop on Hot Topics in Networks (HotNets '22). Association for Computing Machinery, New York, NY, USA, 122–129. https://doi.org/10.1145/3563766.3564100