Remote Attestation in Science DMZ with Xilinx-U280

by Hyunsuk Bang

$ whoami

- M.S of Computer science
- Site Reliability Engineer
- Interests
  - Distributed Systems
  - Computer Networking

Acknowledgement

Nishanth Shyamkumar
Research Software Engineer
Illinois Institute of Technology

Christopher E. Neely
Research Engineer
AMD/Xilinx

Nik Sultana
Assistant Professor
Illinois Institute of Technology

Science DMZ

“A Scalable Network Design Pattern for Optimizing Science Data Transfers”

Targeting near the laboratory's local network

Optimized for high-performance science applications

Characteristics of Science DMZ

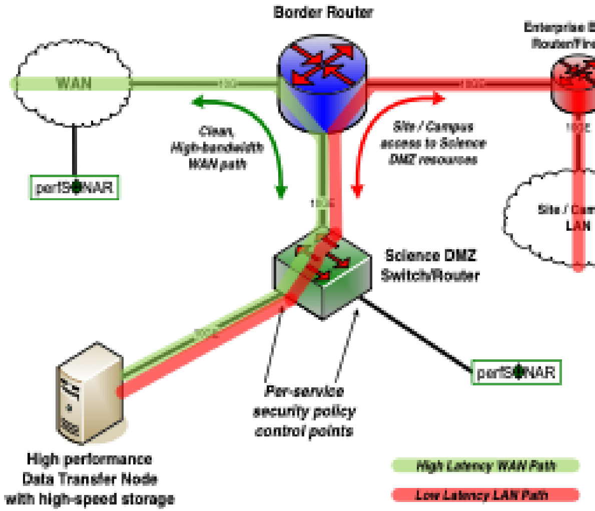
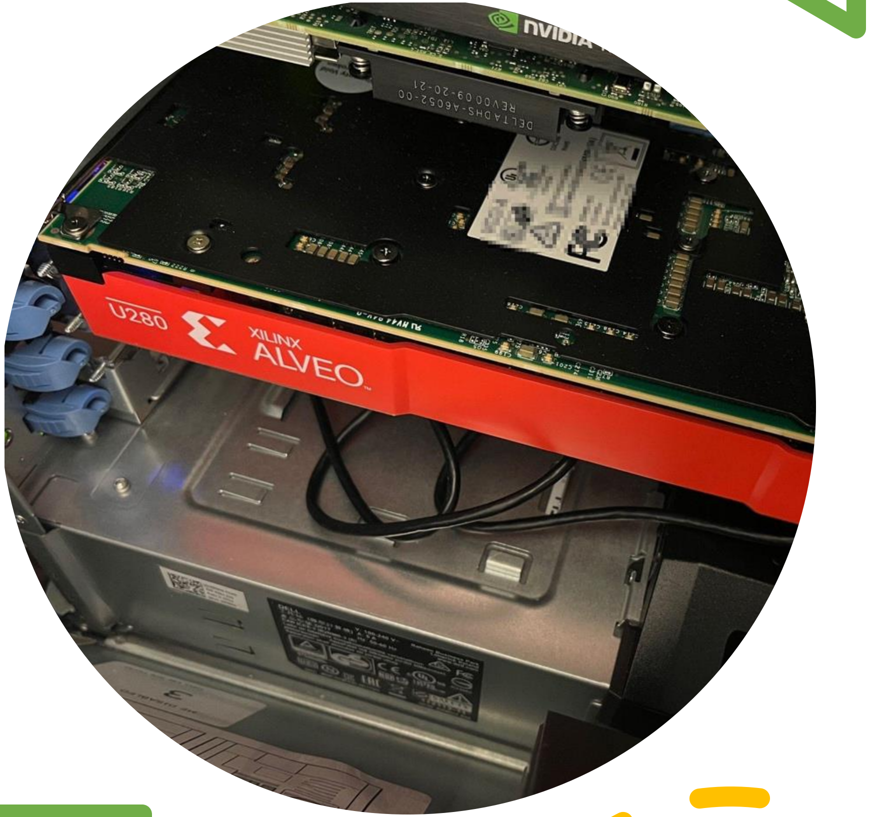

Border Router
Enterprise Border Router/Firewall
WAN
10GE
10GE
Clean, High-bandwidth WAN path
Site / Campus access to Science DMZ resources
10GE
perfSONAR
10GE
Site / Campus LAN
Science DMZ Switch/Router
10GE
perfSONAR
Per-service security policy control points
High performance Data Transfer Node with high-speed storage
High Latency WAN Path
Low Latency LAN Path

Figure 3: Example of the simple Science DMZ. Shows the data path through the border router and to the DTN (shown in green). The campus site access to the Science DMZ resources is shown in red.

- Located at perimeters of the network (close to WAN)
- Isolated from general purpose network
- **“Secured and Performant”**

E. Dart, L. Rotman, B. Tierney, M. Hester and J. Zurawski, "The Science DMZ: A network design pattern for data-intensive science," SC '13: Proceedings of the International Conference onHigh Performance Computing, Networking, Storage and Analysis, Denver, CO, USA, 2013, pp. 1-10, doi: 10.1145/2503210.2503245. keywords: {Security;Packet loss;Data transfer;Wide area networks;Monitoring;Throughput;Performance;Reliability;Design;Measurement},

AMD-Xilinx U280



- FPGA-Powered SmartNIC
- Capable of processing packets at line rates (100Gbps)

FPGA on Science DMZ

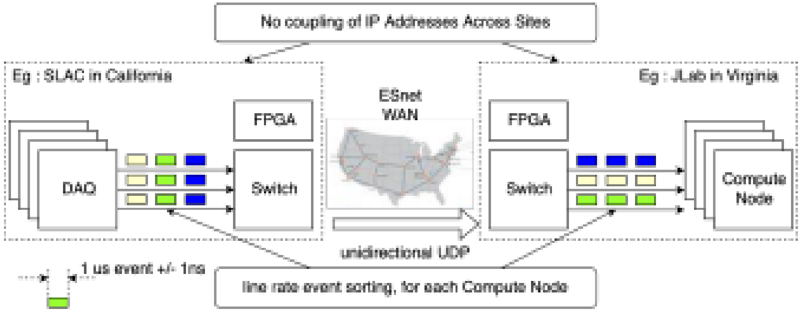


Fig. 1. DAQ to Compute Node Dataflow

- Edge-to-edge, dynamic load balancer
- Horizontally scalable by adding more FPGA

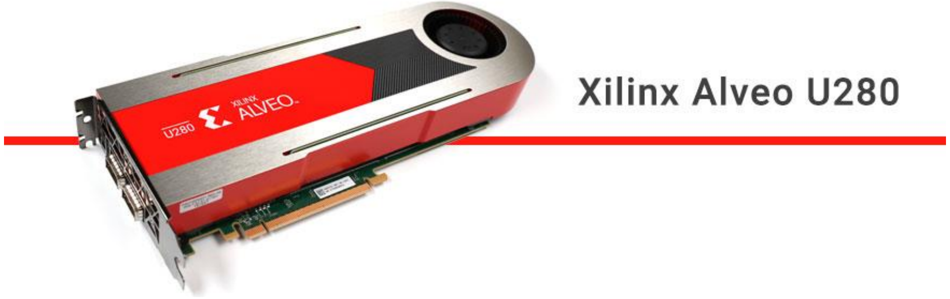
S Sheldon, Y. Kumar, M. Goodrich and G. Heyes, "EJ-FAT Joint ESnet JLab FPGA Accelerated Transport Load Balancer," 2022 IEEE/ACM International Workshop on Innovating the Network for Data-Intensive Science (INDIS), Dallas, TX, USA, 2022, pp. 32-40, doi: 10.1109/INDIS56561.2022.00010. keywords: {Data centers;Instruction sets;Production;Load management;Throughput;Real-time systems;Telemetry;EJ-FAT;P4;UDP;Load Balancer;FPGA},

Remote Attestation

- **“Change detection”**
- Used for validating device authenticity
- Ensure integrity of software and hardware configurations

Science DMZ
+
Remote Attestation
+
AMD-Xilinx U280

For more secure performant Science DMZ



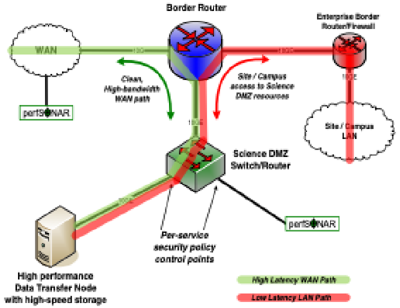

Border Router
Enterprise Border Router/Firewall
WAN
perfSONAR
Clean, High-bandwidth WAN path
Site / Campus access to Science DMZ resources
Site / Campus LAN
Science DMZ Switch/Router
perfSONAR
Per-service security policy control points
High performance Data Transfer Node with high-speed storage
High Latency WAN Path
Low Latency LAN Path

Figure 3: Example of the simple Science DMZ. Shows the data path through the border router and to the DTN (shown in green). The campus site access to the Science DMZ resources is shown in red.

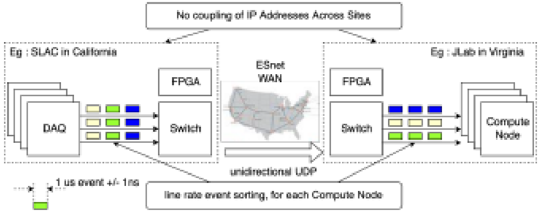


Fig. 1. DAQ to Compute Node Dataflow

Role of U280

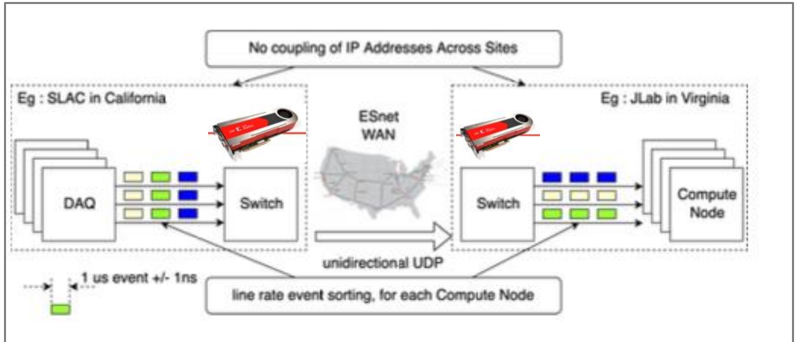


Fig. 1. DAQ to Compute Node Dataflow

- **Timestamp Management**
- **Header Insertion**
- **Verification**

Prerequisite

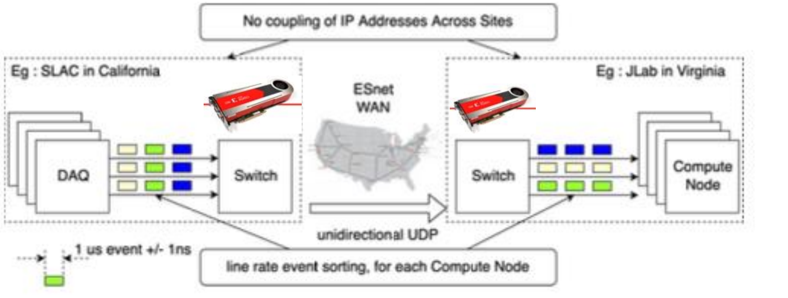
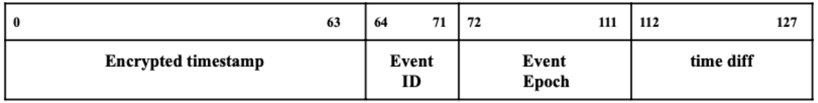


Fig. 1. DAQ to Compute Node Dataflow



0 63	64 71	72 111	112 127
Encrypted timestamp	Event ID	Event Epoch	time diff

Figure3
new remote attestation header for DMZ networks

- Before two Science DMZ sends and receive data across Wide Area Network, both parties must exchange **Event ID and Keys**

DMZ to WAN

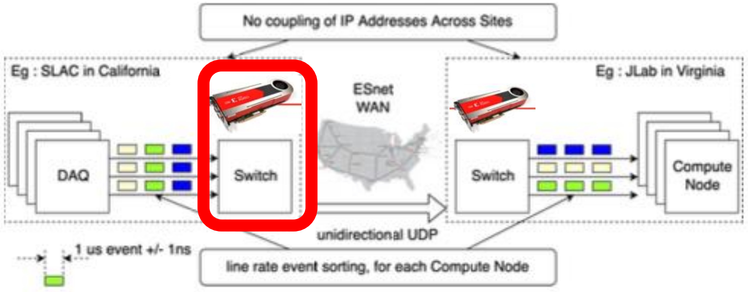
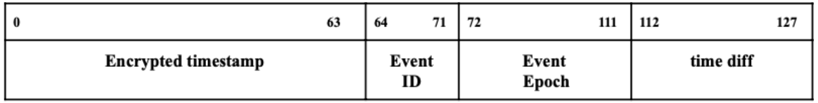


Fig. 1. DAQ to Compute Node Dataflow



0 63	64 71	72 111	112 127
Encrypted timestamp	Event ID	Event Epoch	time diff

Figure3
new remote attestation header for DMZ networks

For every outgoing packets U280

1. Fetch timestamp
2. Fetch Event ID
3. Encrypt
4. Insert Header

WAN to DMZ

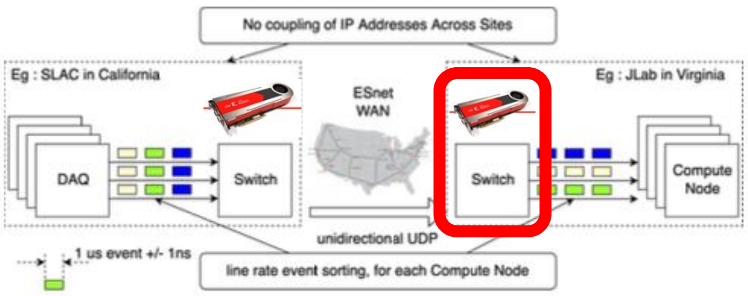
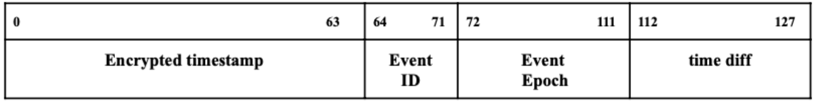


Fig. 1. DAQ to Compute Node Dataflow



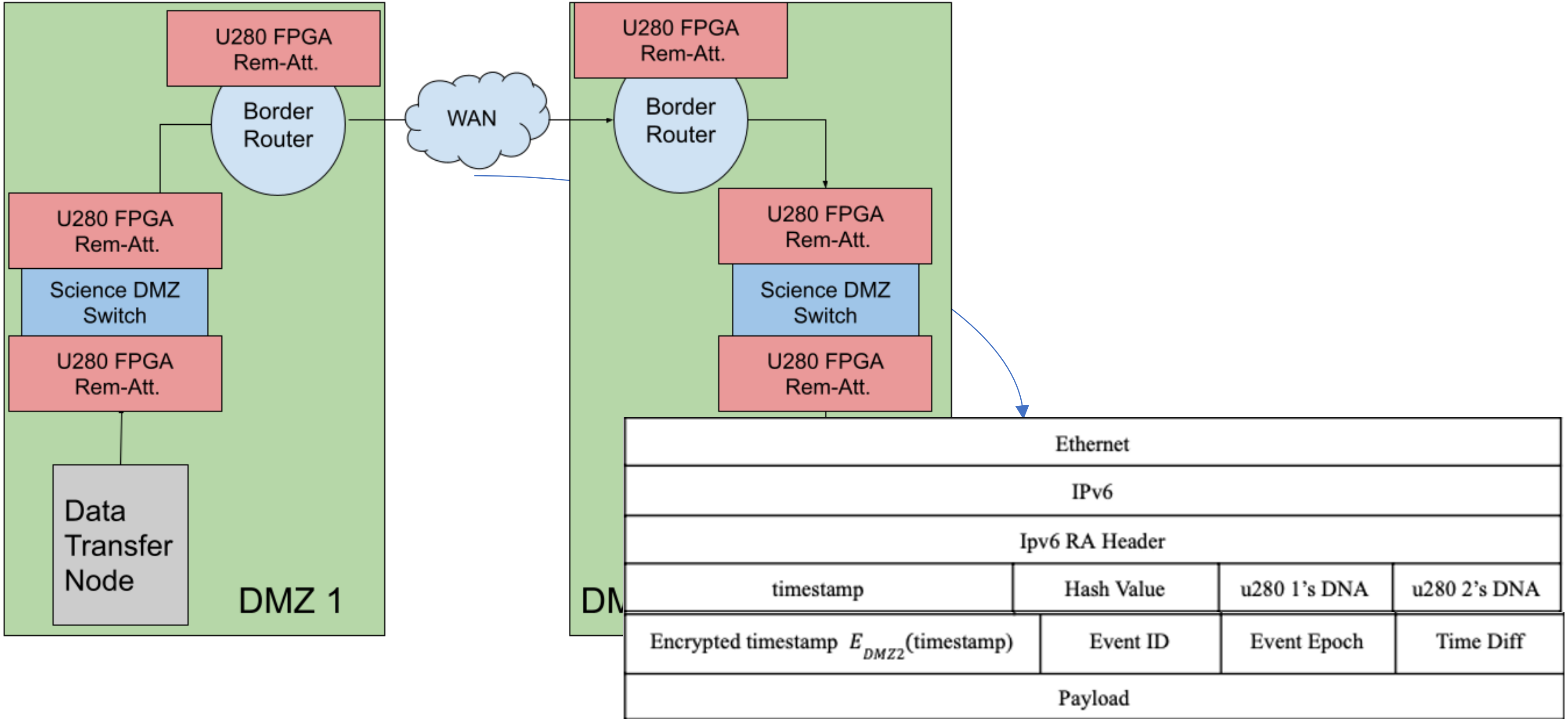
0 63	64 71	72 111	112 127
Encrypted timestamp	**Event ID**	**Event Epoch**	**time diff**

Figure3
new remote attestation header for DMZ networks

For every incoming packets

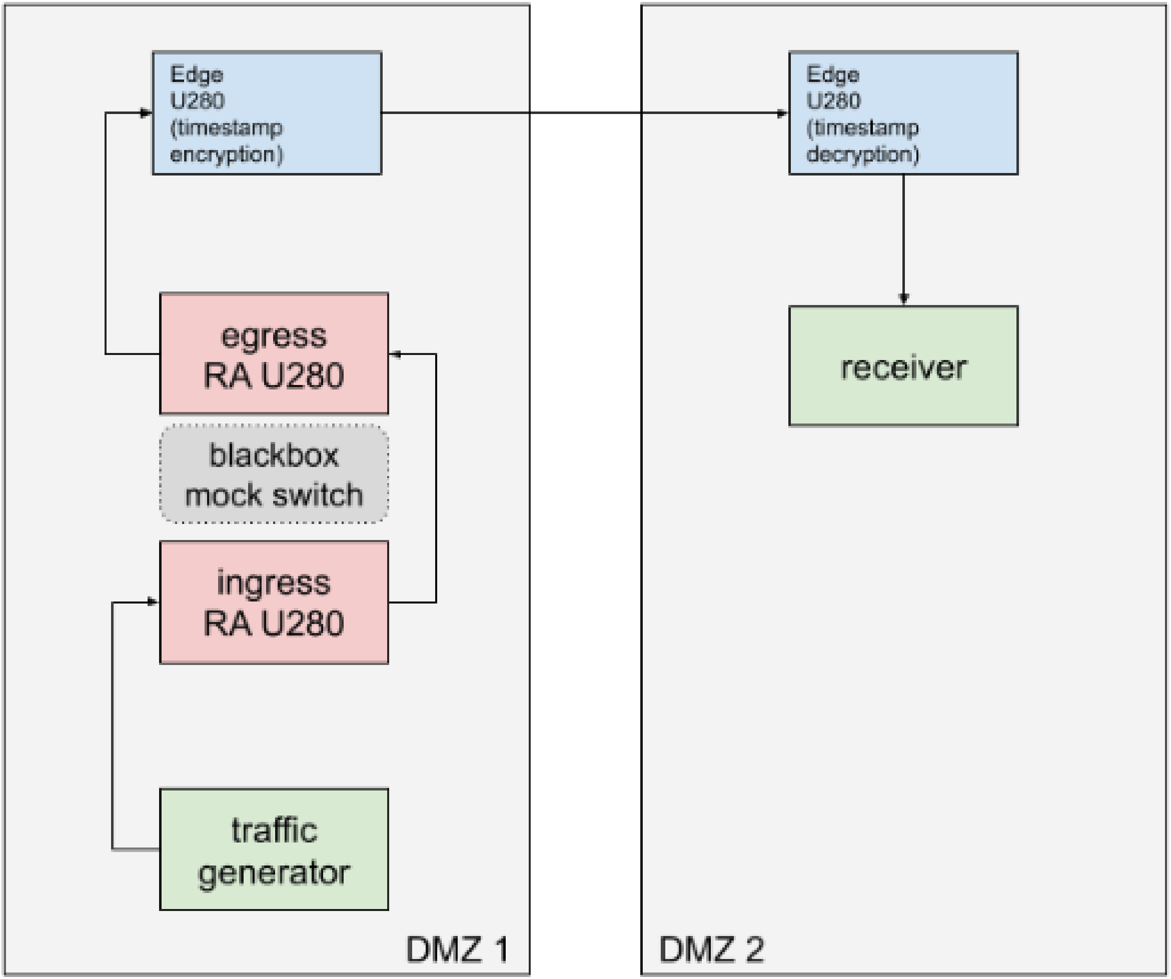
1. Decrypt Header

2. Redirect for deep packet inspection
   - timestamp is malformed
   - out of sync keys

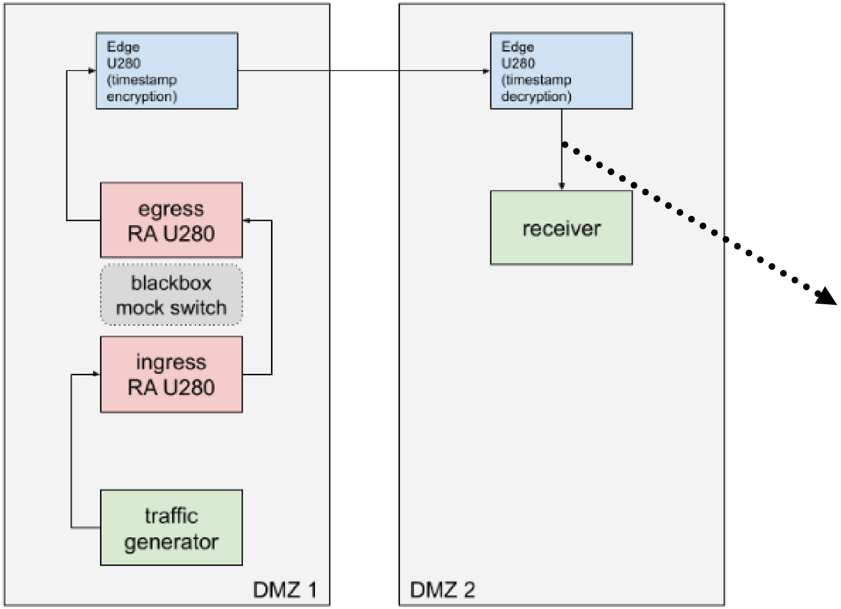


Ethernet			
IPv6			
Ipv6 RA Header			
timestamp	Hash Value	u280 1’s DNA	u280 2’s DNA
Encrypted timestamp E_{DMZ2}(timestamp)	Event ID	Event Epoch	Time Diff
Payload			

Demo


Edge
U280
(timestamp
encryption)
egress
RA U280
blackbox
mock switch
ingress
RA U280
traffic
generator
DMZ 1
Edge
U280
(timestamp
decryption)
receiver
DMZ 2

Example Packet Capture



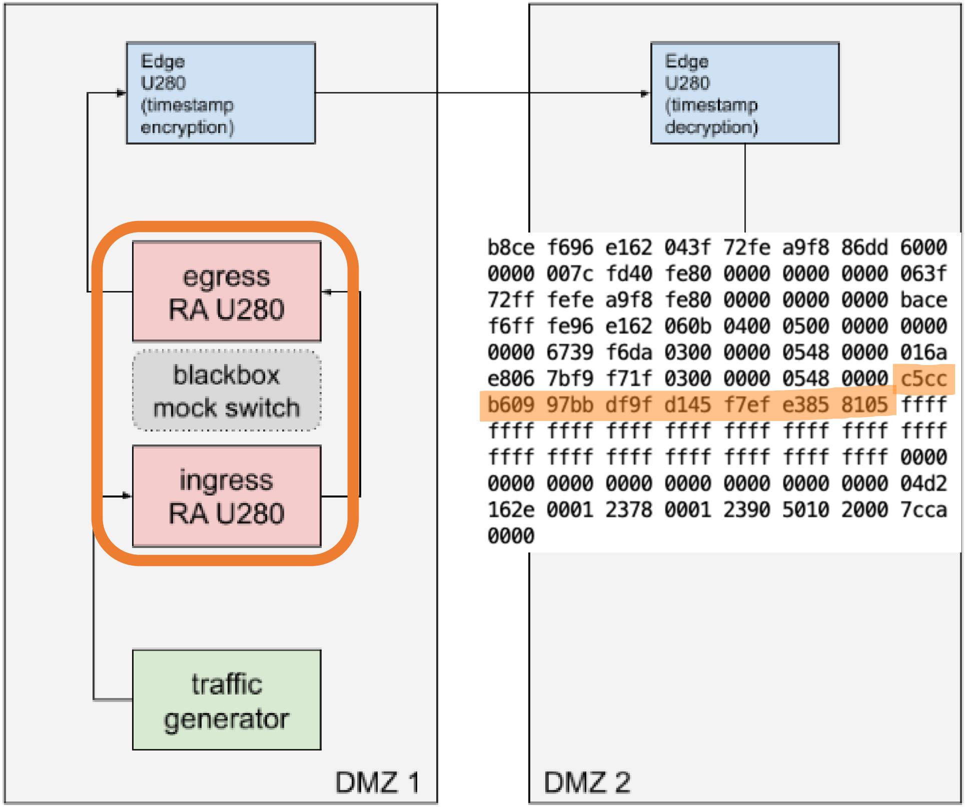
```
b8ce f696 e162 043f 72fe a9f8 86dd 6000
0000 007c fd40 fe80 0000 0000 0000 063f
72ff fefe a9f8 fe80 0000 0000 0000 bace
f6ff fe96 e162 060b 0400 0500 0000 0000
0000 6739 f6da 0300 0000 0548 0000 016a
e806 7bf9 f71f 0300 0000 0548 0000 c5cc
b609 97bb df9f d145 f7ef e385 8105 ffff
ffff ffff ffff ffff ffff ffff ffff ffff
ffff ffff ffff ffff ffff ffff ffff 0000
0000 0000 0000 0000 0000 0000 0000 04d2
162e 0001 2378 0001 2390 5010 2000 7cca
0000
```

Field	Value
L2	b8ce f696 e162 043f 72fe a9f8 86dd
L3 (Ipv6)	6000 0000 007c fd40
L3 Src IPv6	fe80 0000 0000 0000 063f 72ff fefe a9f8
L3 Dst Ipv6	fe80 0000 0000 0000 bacef6ff fe96 e162
RA – Extention Header	060b 0400 0500 0000

Next header is TCP

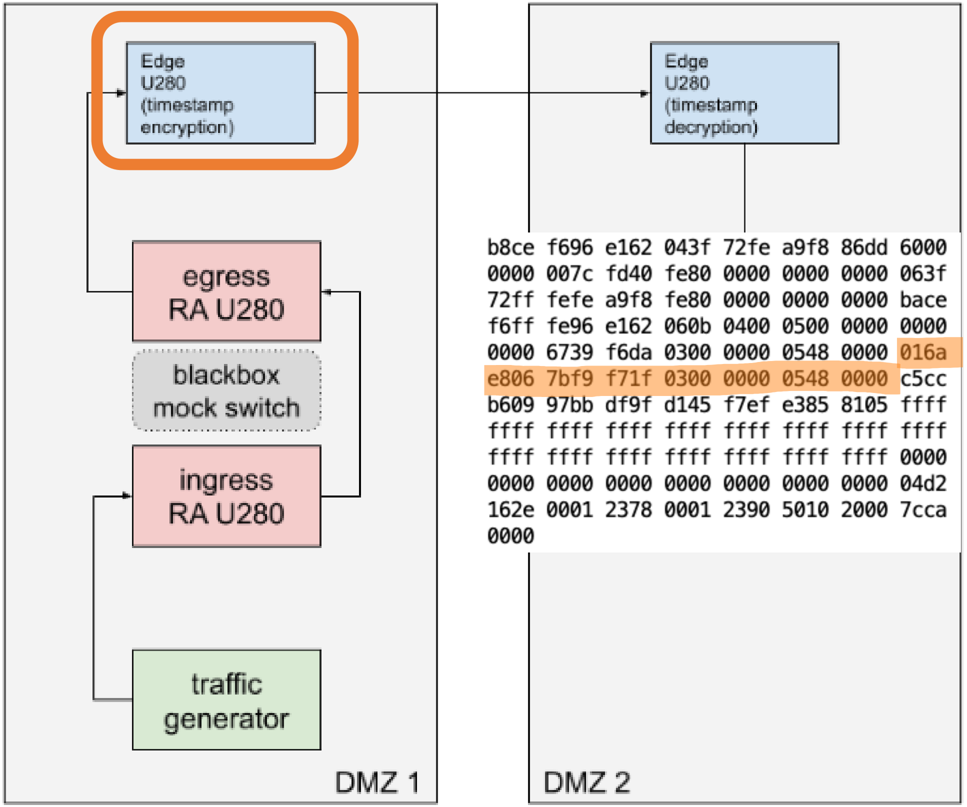
Payload length

Magic number



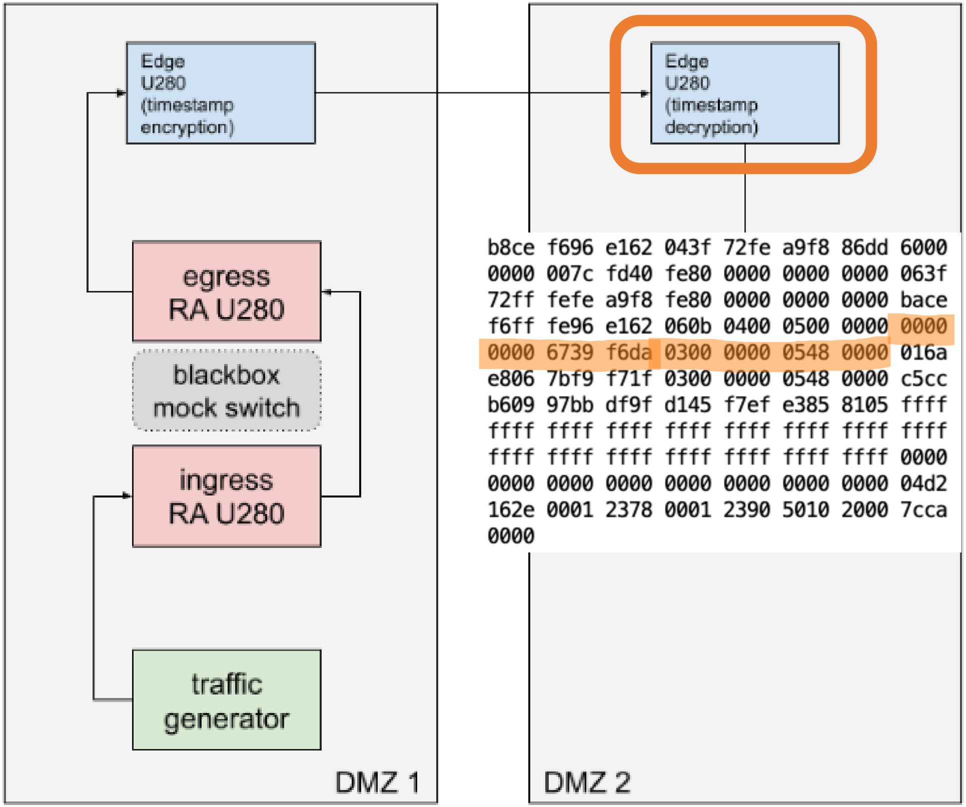
```
b8ce f696 e162 043f 72fe a9f8 86dd 6000
0000 007c fd40 fe80 0000 0000 0000 063f
72ff fefe a9f8 fe80 0000 0000 0000 bace
f6ff fe96 e162 060b 0400 0500 0000 0000
0000 6739 f6da 0300 0000 0548 0000 016a
e806 7bf9 f71f 0300 0000 0548 0000 c5cc
b609 97bb df9f d145 f7ef e385 8105 ffff
ffff ffff ffff ffff ffff ffff ffff ffff
ffff ffff ffff ffff ffff ffff ffff 0000
0000 0000 0000 0000 0000 0000 0000 04d2
162e 0001 2378 0001 2390 5010 2000 7cca
0000
```

Field	Value
RA timestamp	c5cc b609 97bb df9f Timestamp value from mock switch
RA Switch Hash	d145 f7ef Hash value of target device
Attestor Device number (ingress)	e385
Attestor Device number (egress)	8105



```
b8ce f696 e162 043f 72fe a9f8 86dd 6000
0000 007c fd40 fe80 0000 0000 0000 063f
72ff fefe a9f8 fe80 0000 0000 0000 bace
f6ff fe96 e162 060b 0400 0500 0000 0000
0000 6739 f6da 0300 0000 0548 0000 016a
e806 7bf9 f71f 0300 0000 0548 0000 c5cc
b609 97bb df9f d145 f7ef e385 8105 ffff
ffff ffff ffff ffff ffff ffff ffff ffff
ffff ffff ffff ffff ffff ffff ffff 0000
0000 0000 0000 0000 0000 0000 0000 04d2
162e 0001 2378 0001 2390 5010 2000 7cca
0000
```

Field	Value
Encrypted timestamp (Unix)	016a e806 7bf9 f71f
Event-ID	03
Event Count	00 0000 0548
Time diff	0000 Time difference between two consecutive packets with same event-id in milliseconds

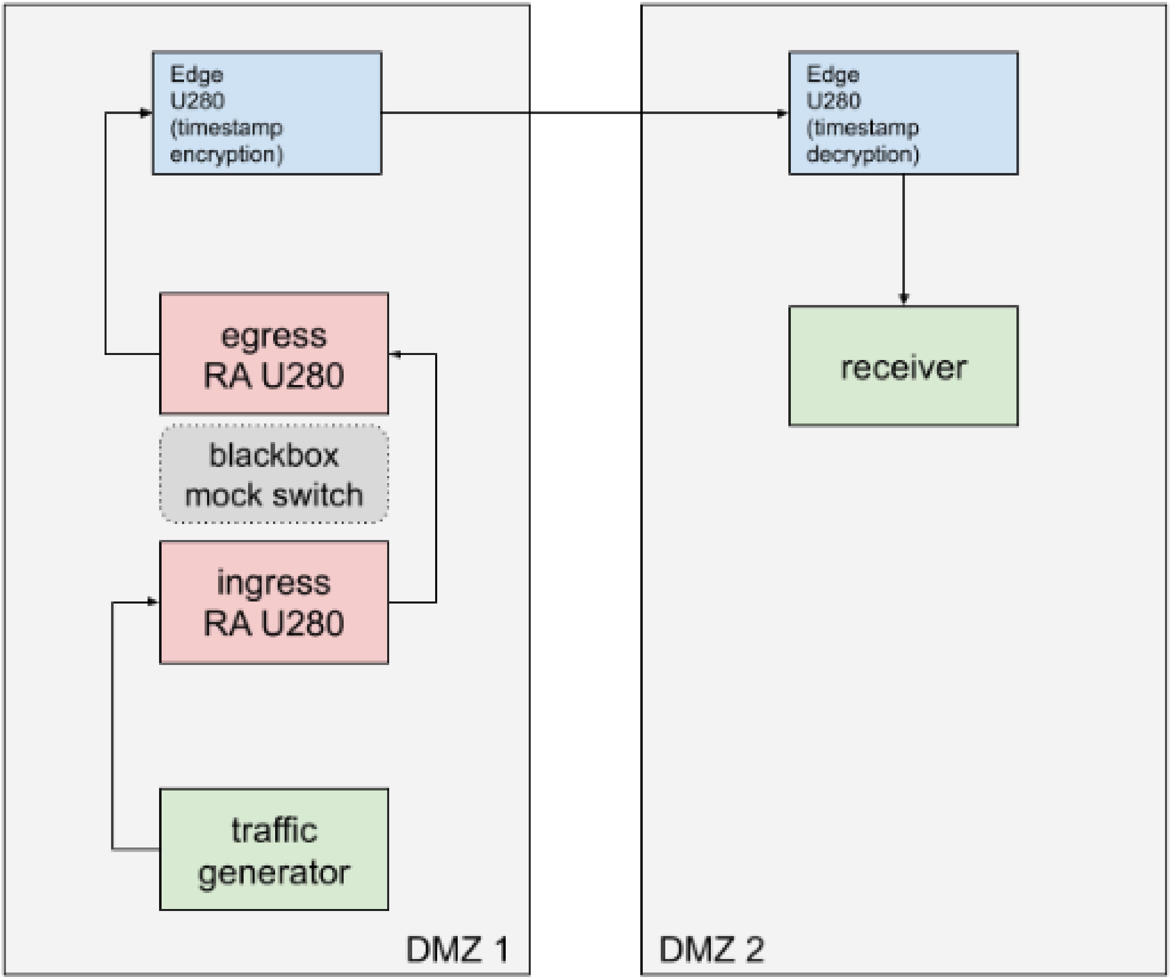


```
b8ce f696 e162 043f 72fe a9f8 86dd 6000
0000 007c fd40 fe80 0000 0000 0000 063f
72ff fefe a9f8 fe80 0000 0000 0000 bace
f6ff fe96 e162 060b 0400 0500 0000 0000
0000 6739 f6da 0300 0000 0548 0000 016a
e806 7bf9 f71f 0300 0000 0548 0000 c5cc
b609 97bb df9f d145 f7ef e385 8105 ffff
ffff ffff ffff ffff ffff ffff ffff ffff
ffff ffff ffff ffff ffff ffff ffff 0000
0000 0000 0000 0000 0000 0000 0000 04d2
162e 0001 2378 0001 2390 5010 2000 7cca
0000
```

Field	Value
Decrypted timestamp (Unix)	0000 0000 6739 f6da 11/17/2024 @. 2:32 PM (UTC)
Event-ID	03
Event Count	00 0000 0548
Time diff	0000 Time difference between two consecutive packets with same event-id in milliseconds

Scenario 2
Key Mismatch

Performance



Thanks!

Nik Sultana

Christopher Neeley

Nishanth Shyamkumar