



Introduction

- User-Plane Function (UPF) devices provide essential services to 5G networks.
- Programmable dataplanes can serve as UPF to offer flexibility through programmability.
- However, a programmable dataplane has potential for misuse if an attacker gains control.
- Thus, we need to ensure the programmable resource is in a trusted state.
- This demo examines what a modern version of the “Athens Affair” attack could look like on a 5G UPF controlled by a programmable dataplane, and how Remote Attestation defends against it.

Motivation

1. Demonstrate use of programmable dataplane as 5G UPF Device.
2. Explore modern version of the Athens Affair, a notable past attack on a telecom network.
3. Explore defense techniques in 5G and beyond.

Acknowledgement

This work was partly supported by 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.

Approach

- A programmable network element (**BMv2 Simple Switch**) is extended to support **Remote Attestation** primitives that verify the trustworthiness of the switch state.
- This switch serves as a UPF in a mock 5G network.
- We simulate normal **5G Network Control Functions** including IP assignment and bandwidth monitoring.
- A dedicated port connects the switch to an **RA Verifier** which confirms that the UPF is executing expected code and detects attempts to tamper with it.

Verifier detects unlogged change

```
RuntimeCmd: get_ra_data
Registers: D41D8CD98F00B204E9800998ECF8427E
Tables: CAF1A3DFB505FFED0D024130F58C5CFA
Program: 99914B932BD37A50B983C5E7C90AE93B
```

```
Monitoring UPF
Warning! Potentially unauthorized program change
Old: 99914b932bd37a50b983c5e7c90ae93b
New: d9762af1dc0cf30c0e59c381dc39a538
```

Results

- The verifier confirms the switch state is correct when initialized in the correct state.
- When the program is overwritten, though the switch still reports it is correct, the verifier correctly detects that the program alteration.

SMF Adds Table Entries, Monitors Usage

New UL entry recorded
 Added new DL entry for UE with IP 32.0.1.1 as entry 1
 UE with IP 32.0.1.1 has used (974 bytes, 16 packets) of data on DL

