ILLINOIS TECH
College of Computing

Attestation-Capable, Programmable Switch as 5G UPF

Alexander Wolosewicz, Nishanth Shyamkumar, Ashok Sunder Rajan, Nik Sultana

Illinois Tech Illinois Tech Intel Corp Illinois Tech

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

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

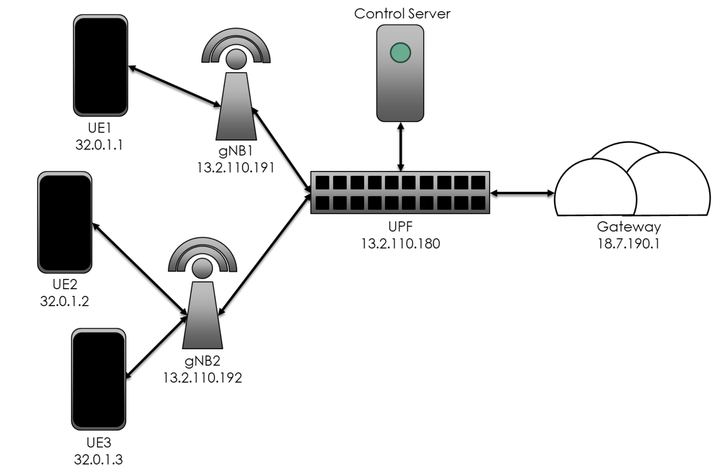
1. Demonstrate use of programmable dataplane as 5G UPF Device.
2. Explore modern version of the Athens Affair, a notable past attack on a telecom network.
3. Explore defense techniques in 5G and beyond.

Approach

- A programmable network element (**BMv2 Simple Switch**) is extended to support **Remote Attestation** primitives which 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.

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.



./start_upf.sh: Egress() {}

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

Monitoring UPF
```

./hostile_upf.sh: Egress() { clone() }

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

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

Acknowledgement

Our collaborators Ben Ujcich (Georgetown University) and Deborah Shands (SRI Intl), Vinod Yegneswaran (SRI Intl), and Ashish Gehani (SRI Intl). This work was 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.