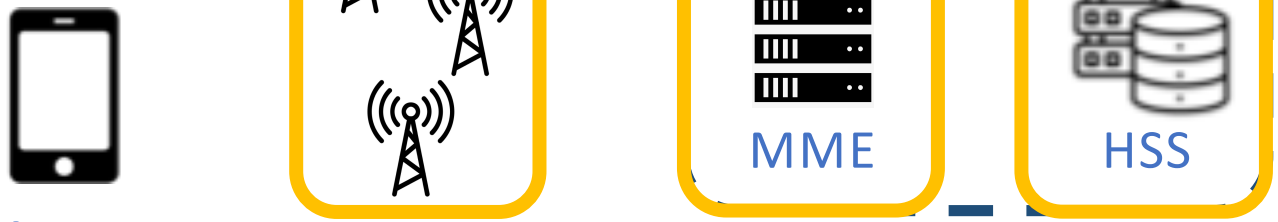
Device-Centric Detection and Mitigation of Diameter Signaling Attacks against Mobile Core

Zhaowei Tan, Boyan Ding, Zhehui Zhang,
Qianru Li, Yunqi Guo, Songwu Lu

UCLA WiNG Wireless Networking Group

Cellular Network Architecture



Phone Devices

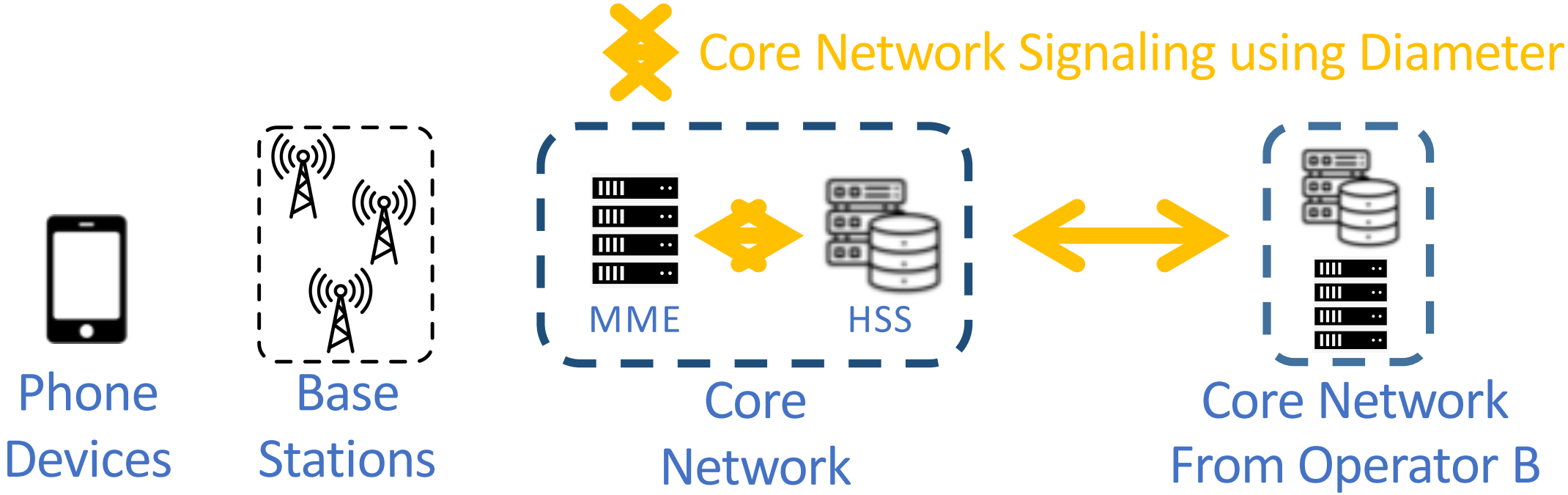
Base Stations

Core Network

- Wireless Coverage
- Device Mobility Management
- User Database

Cellular network: The only large-scale infrastructure for “anywhere, anytime” services

Signaling Messages in Cellular Core



Signaling messages are exchanged between Core Network components for session management, mobility support, etc.

Threats in Core Network Messaging

Vulnerability

It is assumed that LTE components running Diameter are from a trustworthy “closed community”

Diameter attacks: An attacker compromises a core component and forges Diameter messages.

Various news and tech reports on Diameter attacks and compromised nodes

Due to improper trust model, the forged message is accepted to incur damages

Outline

D3: Detect and mitigate Diameter DoS attacks on the device side, without any infrastructure support

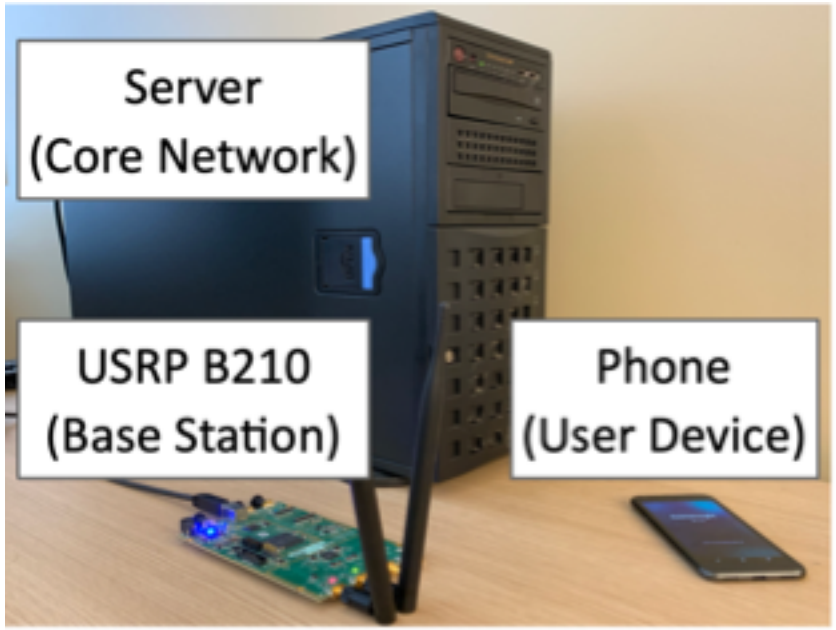
This talk:

1. Can we prototype and validate Diameter attacks?
2. Is a defense solution on the device side possible?
3. How to design and implement D3?

Prototyping Diameter Attacks

Testbed for Prototyping Attacks

We build an SDR-based 4G LTE testbed



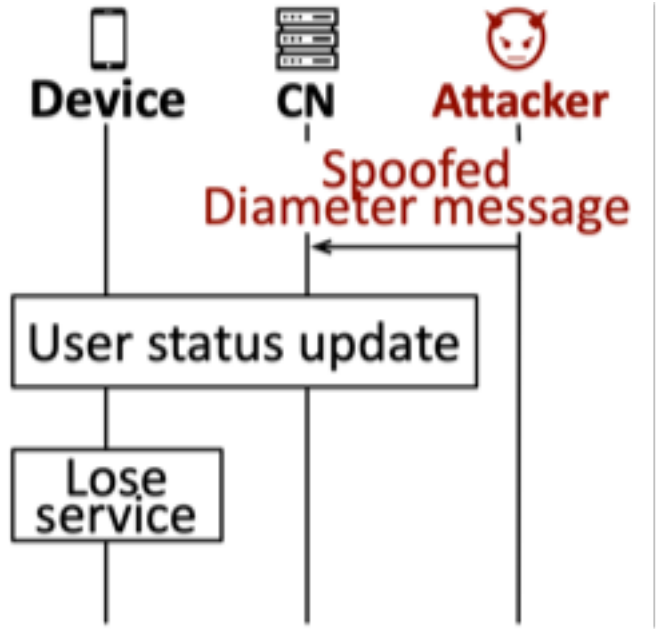
Purposes of the prototype

- Validate typical Diameter attacks
- Understand the attack severity
- Gain insights for our solutions

Prototyping Diameter Attacks

We implement an attacker process that sends 4 typical malicious Diameter messages for attacks

- IDR: Insert Subscriber Data Request
- PUR: Purge Request
- ULR: Update Location Request
- CLR: Clear Location Request

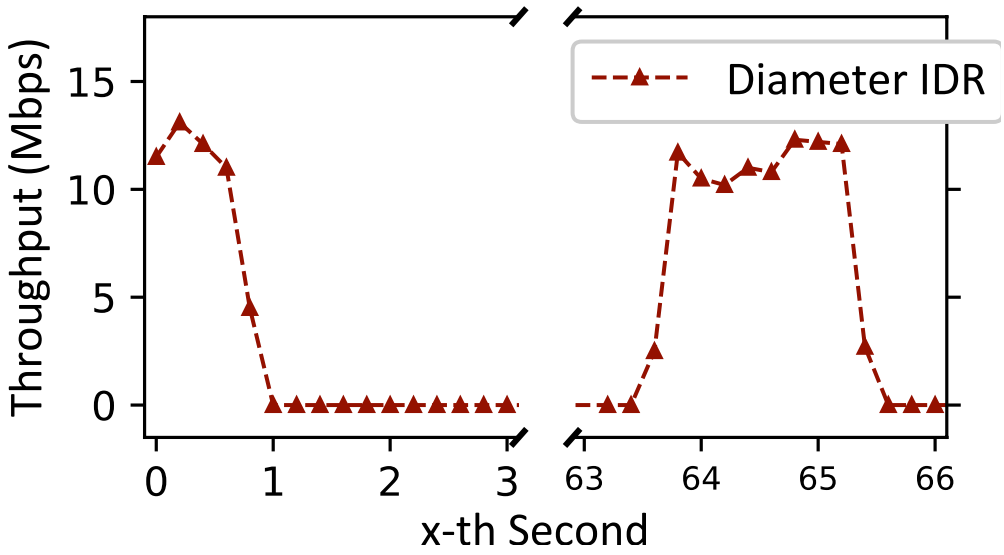


IDR Attack and Its Damages

IDR: A message for updating user subscription

An attacker can send a malicious IDR message to disable certain user service in subscription

Consequently, the victim loses certain service, e.g., data access

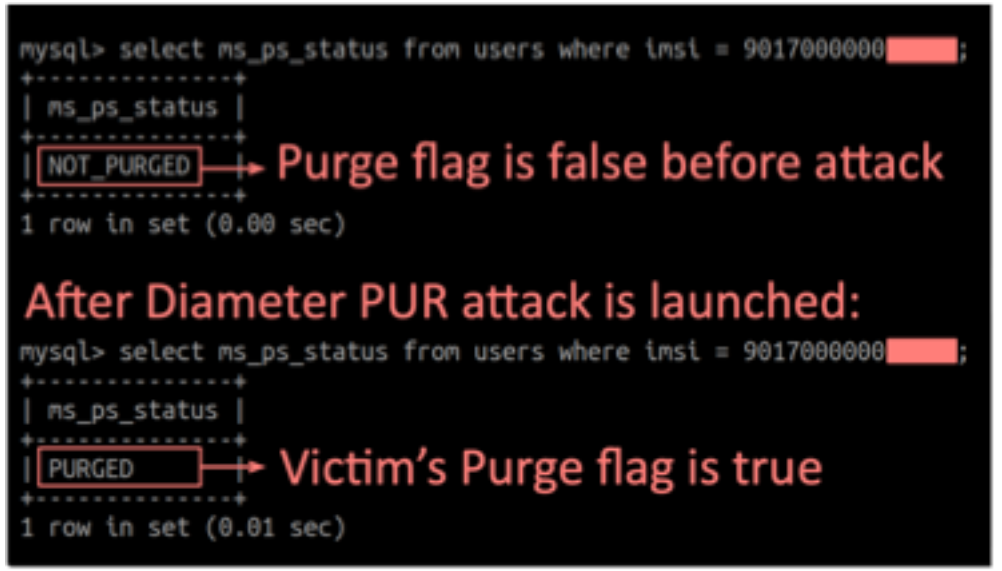


PUR Attack and Its Damages

PUR: A message that indicates a device is no longer being served (Purged)

An attacker can send a malicious PUR message to purge a victim device in the database

Any incoming call or text message is blocked given the purged status



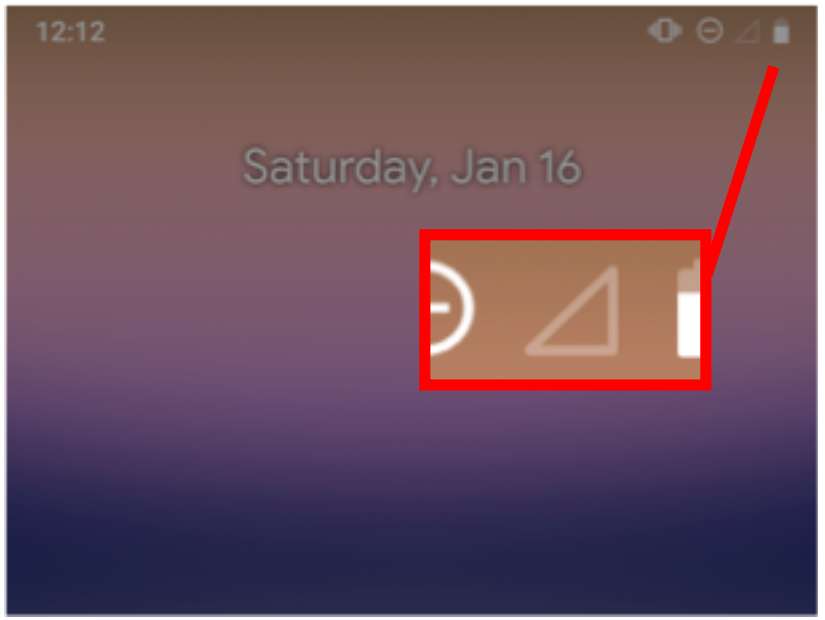
ULR/CLR Attacks and Damages

ULR: An MME notifies the HSS that it is serving a user

CLR: An HSS notifies the MME to stop serving a user

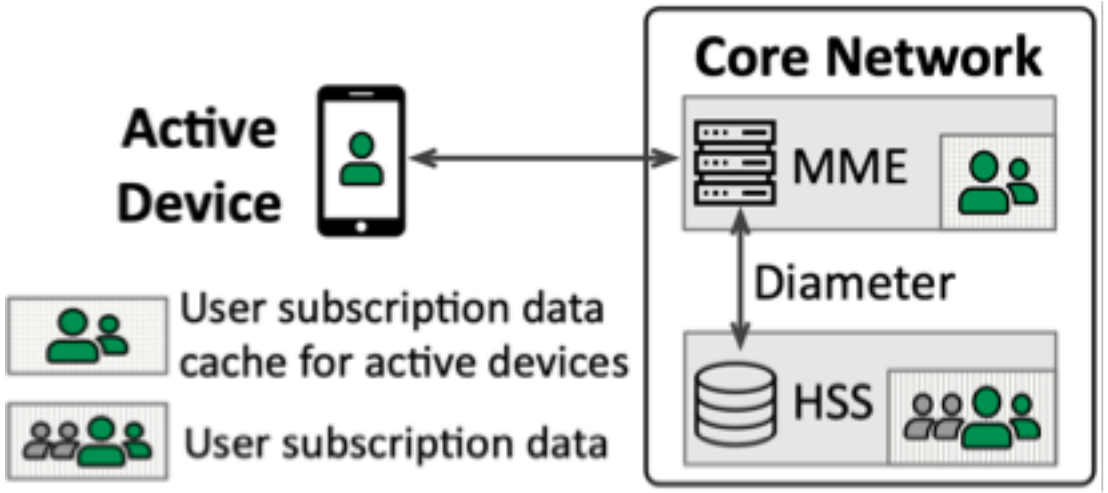
An attacker can send a malicious ULR that triggers a CLR from HSS to the victim's serving MME

Consequently, the victim is disconnected and loses all services



Insights: Causes of DoS Damage

The cellular core manages the user subscription data with two copies in MME and HSS



Diameter DoS attacks essentially cause inconsistency among network nodes

Insights for Detection Methods

+ The damages can be observed from end devices

- The attacks appear as legitimate service loss
  → Domain knowledge to distinguish between them
- The Diameter attacks can be repeatedly launched
  → Fast mitigation after detection is necessary

Device-Centric Solution

Why Device-Centric?

- Some attacks are easier to detect on the device side
- Cost-effective without expensive infrastructure update
- Scalable, easy to apply patches for new attacks, …

Complementary to infrastructure-side solutions

- The device can notify the network to block future attacks
- Some Diameter attacks are only detectable by infrastructure

Device-Centric Solutions: Roadblocks

Challenge 1: How to distinguish between Diameter attacks and normal service loss?

Idea: Analyze cellular-level logs on device side for differences

Study 3GPP standards on how network reacts upon a Diameter message

Device-Centric Solutions: Roadblocks

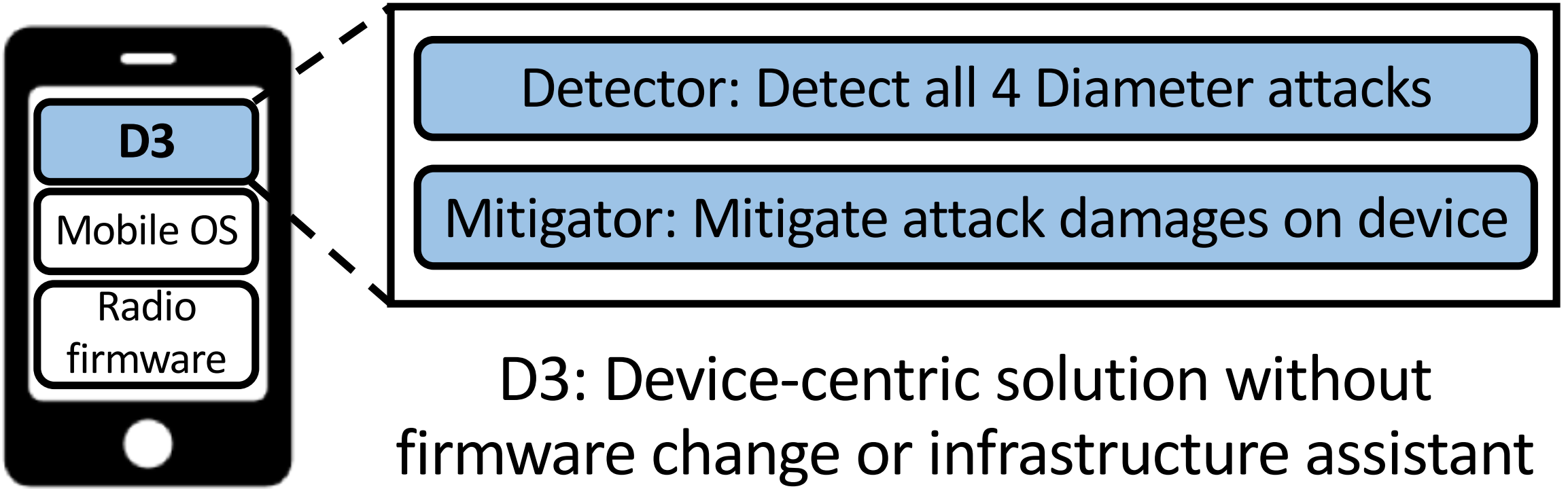
Challenge 2: How to access NAS signaling messages from closed-source cellular networks?

Idea: Device-side tools for cellular data collection & analysis

Use tools such as QXDM or MobileInsight to collect cellular signaling messages and write data analyzer

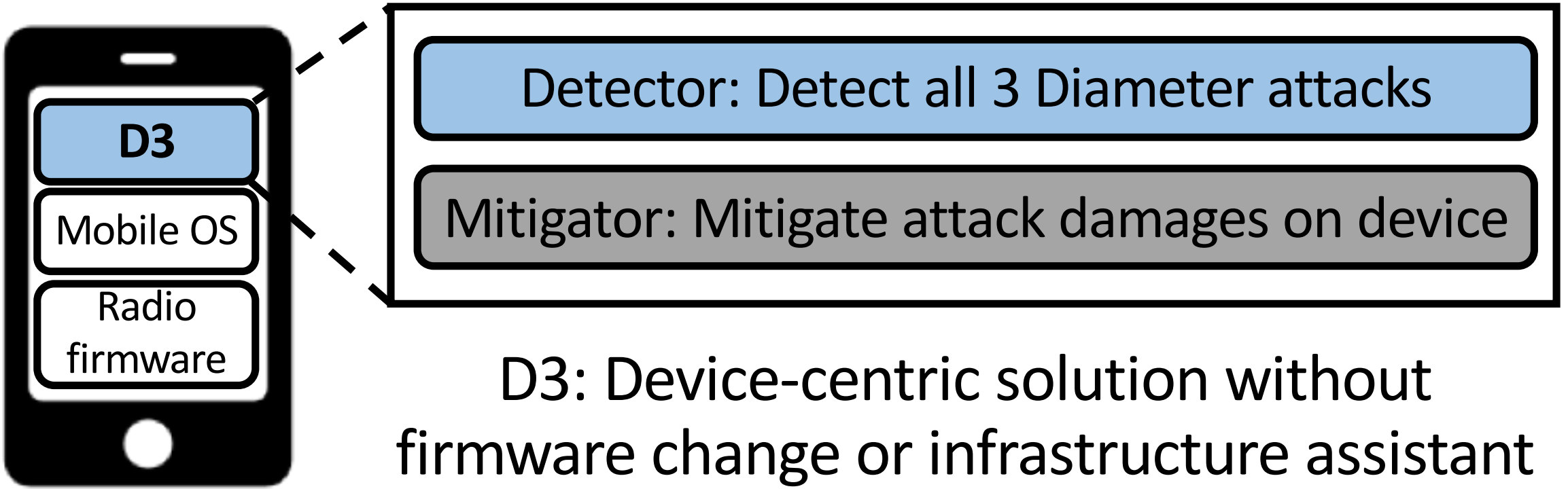
D3: A Device-Centric Defense for Diameter Attacks

D3 Overview



D3: Device-centric solution without firmware change or infrastructure assistant

D3 Overview

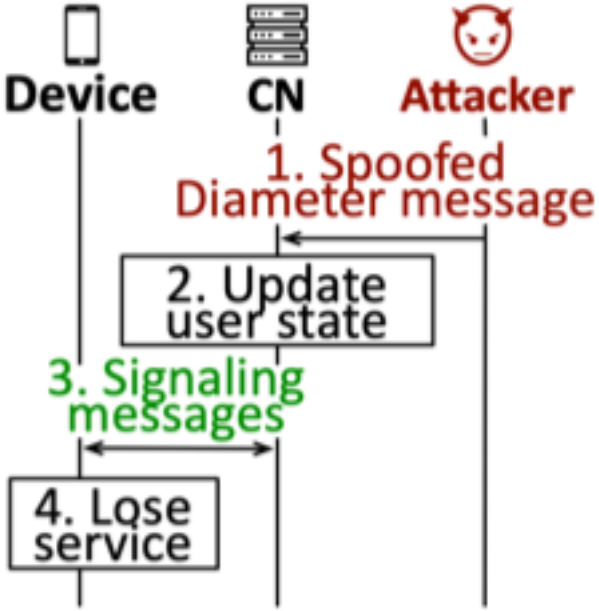


D3: Device-centric solution without firmware change or infrastructure assistant

Key Idea of D3 Detection

Signaling messages (NAS) are different during a Diameter attack and normal service loses

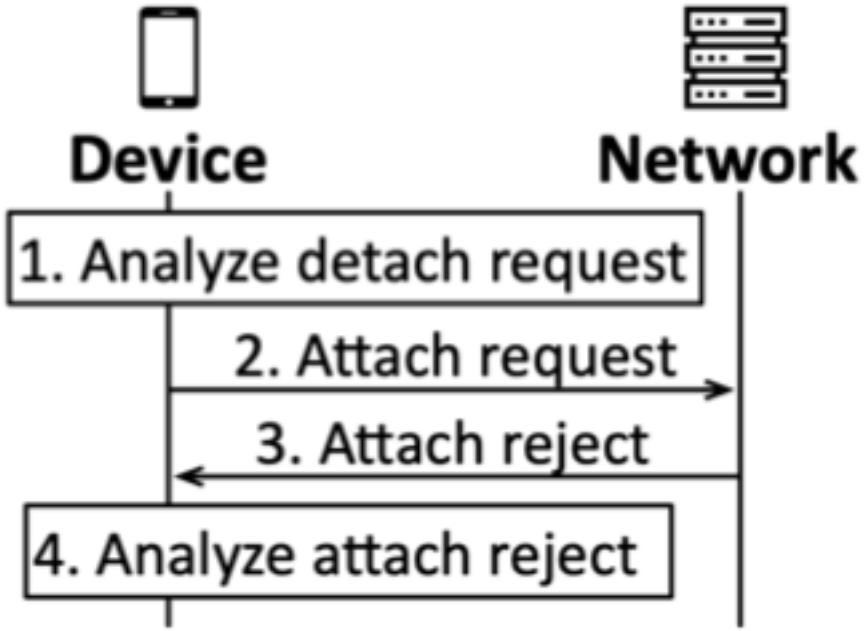
- D3 passively analyzes the signaling message exchanges
- If necessary, D3 proactively sends messages to confirm the attacks



D3 Detector: Detecting IDR Attack

To detect IDR attack, D3 analyzes detach request caused by the attack

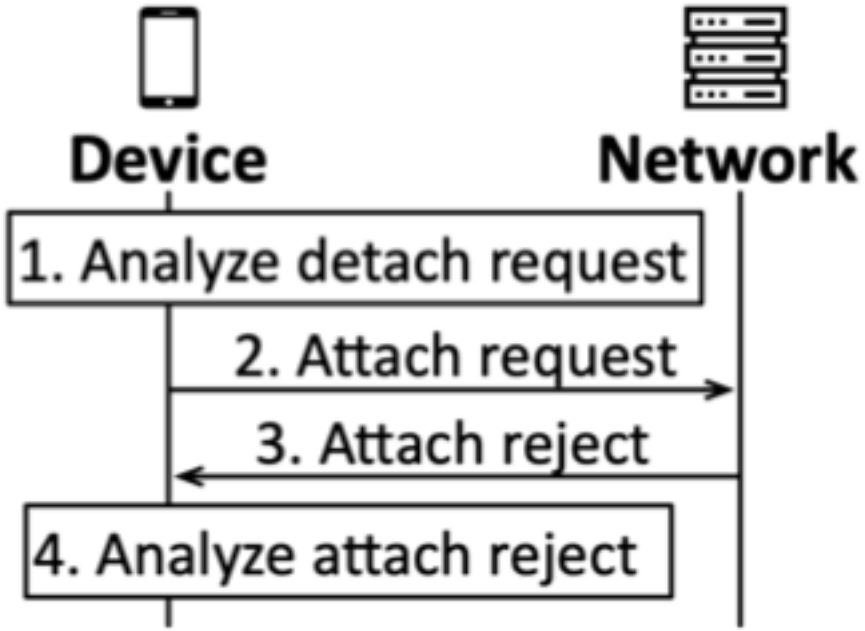
- A detach request itself indicates an abnormal behavior
  - A detach request caused by IDR attack includes “no re-attach”



D3 Detector: Detecting IDR Attack

It then actively sends an attach request and analyzes reject message

- The attach reject will include subscription issue for detach
  - The device can check whether the issue matches its subscription



D3 Detector: Detecting PUR Attack

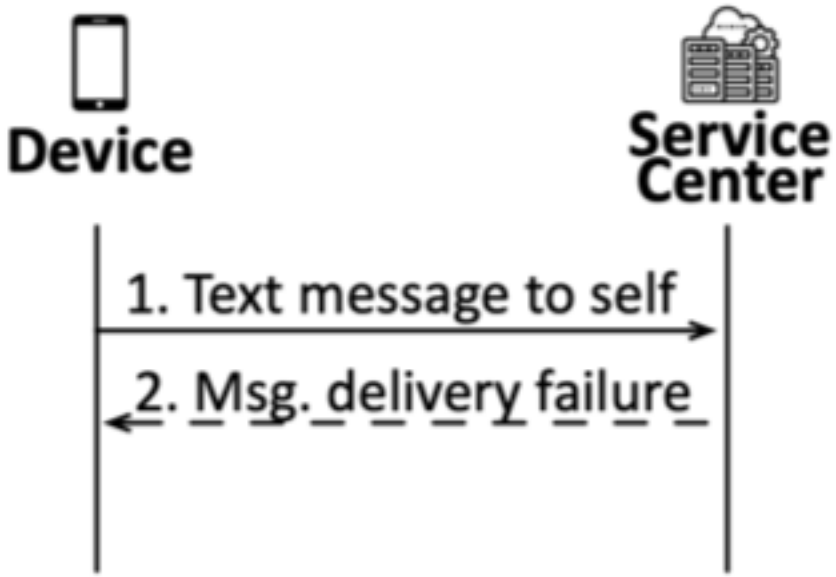
PUR attacks cannot be detected by passive monitoring

- PUR attack only blocks *incoming* texting and calls
- The core network blocks them without notification
- The outgoing texting and calls are not affected

D3 Detector: Detecting PUR Attack

D3 actively triggers incoming texting to detect PUR attack

- D3 periodically sends texts to itself
  - The overhead depends on the texting message periodicity
- If an incoming text is blocked while the network connection is normal, D3 detects a potential PUR attack



D3 Detector: Detect ULR/CLR Attacks

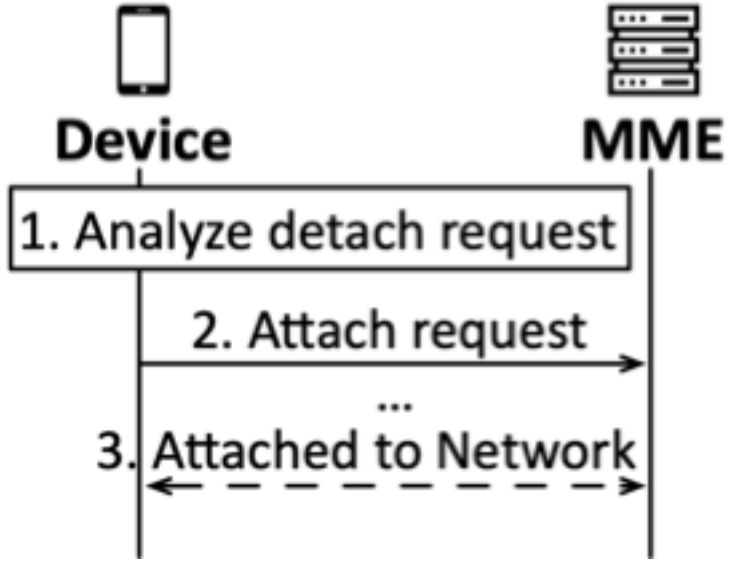
D3 detects (and mitigates) ULR/CLR attacks by initiating an attach request following the detach

Since a ULR eventually triggers a CLR, detecting a CLR attack can effectively detect a ULR attack

D3 Detector: Detect ULR/CLR Attacks

D3 detects (and mitigates) ULR/CLR attacks by initiating an attach request following the detach

- Send attach request regardless of the detach request type
- Under CLR attack, the attach request helps re-gain services



Discussion on D3 for 5G

D3 applies to attacks against 5G core network signaling

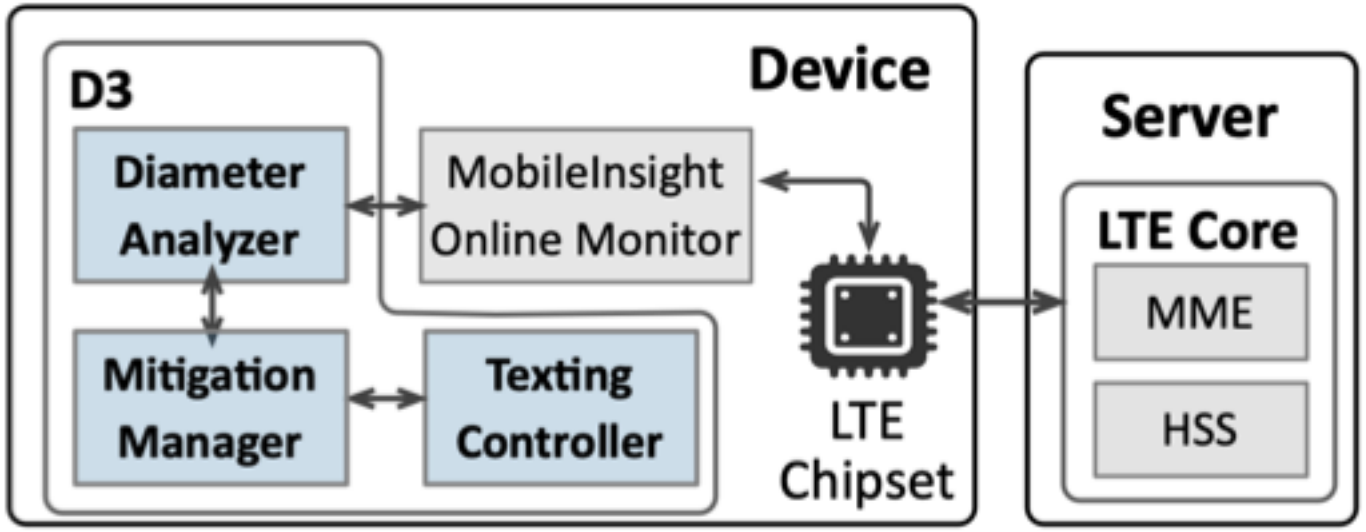
- 5G fist phase: reuses 4G core network
- 5G second phase: replaces Diameter with more secure protocol, but still uses the same trust model
  - The attacks are still available from compromised nodes
  - Device-centric solution is still necessary and applicable
  - 4G NAS is inherited by 5G; D3 applies with modification

Evaluation

- Does D3 detect Diameter attacks from normal service loss?
- Can D3 mitigate the Diameter attacks?
- What is the overhead of D3?

D3 Implementation

Implement D3 on off-the-shelf Android phones



- The prototype works as a standalone user-space daemon
- Interact with MobileInsight Monitor to analyze cellular logs

Detection Results

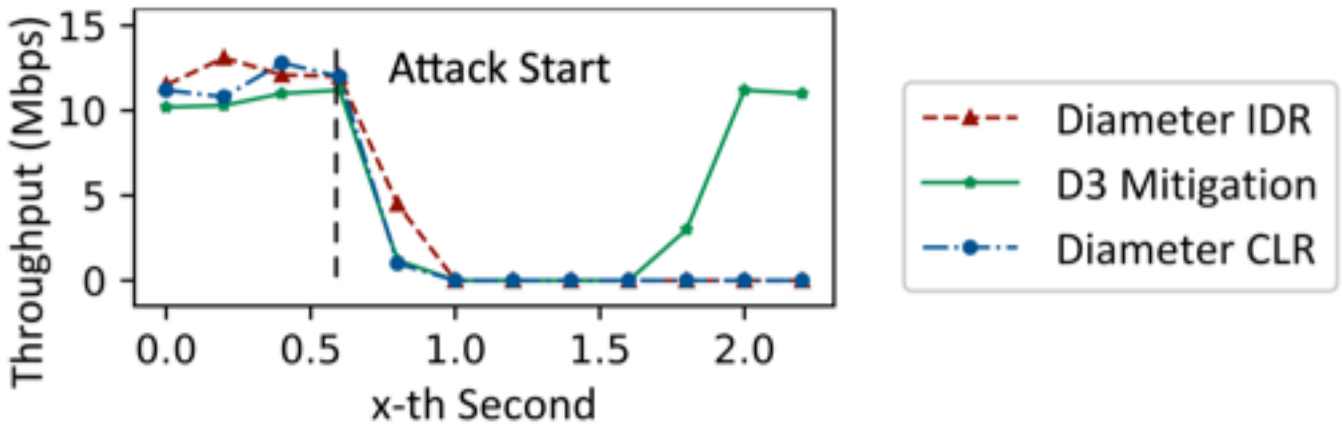
D3 can detect all 4 Diameter attacks from normal service loss

- We mix Diameter attacks with conditions that can cause device DoS: bad signal, network error, and device error
- D3 achieves perfect precision and recall for the detection

Even if D3 misclassifies a normal service loss as Diameter attack, its mitigation does not incur extra damage

Mitigation Results

D3 can mitigate the damages of 4 Diameter attacks



The effectiveness and difficulty of D3 mitigation depend on core network implementation

D3 Overhead

Small overhead!

- Memory usage: Extra 1%
- CPU usage: Extra 4.9%

D3 components are mostly passive
NAS messages are infrequent

Summary

- We validate that Diameter attacks incur serious damages
- D3: Device-centric solution for detection and mitigation
  - Accurately detect all 4 Diameter attacks
  - Mitigate the attack damages on the device side
- Its solution idea is applicable to both 4G and 5G

Thank you!

For more information:
http://metro.cs.ucla.edu/d3.html