Real Threats to Your Data Bills:
Security Loopholes and Defenses in Mobile Data Charging

Chunyi Peng
Chi-Yu Li, Hongyi Wang, Guan-Hua Tu, Songwu Lu
Mobile Data Services, Everywhere
Certainly, No Free Lunch

- Mobile data bills: pay for usage
- Essential to carriers and users
  - $400-500B revenue
  - Monetary rights of billions of users

Mobile data service revenues worldwide from 2010 to 2015 (in billion U.S. dollars)

Source: http://www.statista.com/
Volume-based Mobile Data Charging

- Various data plans
  - Volume-capped, e.g., $20/300MB
  - Per-use, e.g., $0.0195/KB for roaming
  - ...
  - Single line or shared plans
  - Prepaid or postpaid
  - ...

- The core: charged by usage volume
Are our data bills CORRECT?

We pay for what we use;
We do not pay for what we do not use.
Overcharges and Undercharges [CCS’12]

Flaws in Mobile Networks Allow Users to Surf the Internet for Free (via DNS tunneling)

Your carrier may be charging you for data you didn't receive

By Aaron Souppouris (http://www.theverge.com/users/AaronSoup) on September 20, 2012 08:15 am  Email (mailto:aaron@theverge.com) @AaronsisSocial

When your wireless carrier charges you for the amount of data you used on your cell
Now, are they CORRECT?
This Talk

- Real threats to mobile data bills
  - Free uplink data access at other’s cost
  - Overcharges while victims do nothing
    - In a much more covet way
  - No sophisticated attacks needed: readily launched

- Security breach against Authentication, Authorization and Accounting (AAA)
  - How they work?
  - How they fail?

- Defense solutions
Three Requirements

- Mobile data charging: collect how much data is actually used by whom at his/her consent

<table>
<thead>
<tr>
<th>Authentication</th>
<th>Authorization</th>
<th>Accounting</th>
</tr>
</thead>
<tbody>
<tr>
<td>The user being billed = Who transfers data.</td>
<td>The user agrees to use data and pay it.</td>
<td>Volume should be accurate.</td>
</tr>
</tbody>
</table>
No extra capability needed at the attacker
- No comprise or access to operator networks
- No malware or remote access to victim phones
- Commodity phone and server (optional)
  - E.g, an rooted Android phone

All proof-of-concept attacks ready to launch NOW
- Responsible: victims = our own phones
Current Mobile Data Charging

4G Mobile Network

(1a) User authentication

(1b) bearer setup (IP allocation)

(2) Data transfer

(3) Accounting: Volume used by whom
(1a) User authentication via AKA

Bearer setup request

P-GW

U.IP 10.0.0.1

(1b) IP allocation
Bearer (GTP) established

U.IP 10.0.0.1

P-GW

Data-plane

Billing based on packet.srcIP

U’s bill

IP address is indeed authenticated.
(not during data transfer)

Authentication bypass for charging
(IP spoofing)
Authentication Bypass

Free-Uplink-Attack

Cause: No cross-layer secure binding

Authentication bypass for charging (IP spoofing)

U’s bill

X’s Proxy

X

X.GTP

X.IP

U

X.GTP

X.IP

P-GW

U.IP

X.GTP

X.IP

P-GW

U.IP

X’s Proxy

Causes:

No cross-layer secure binding

Authentication bypass for charging (IP spoofing)
In Real Networks

- Two US carriers: OP-1 and OP-2

<table>
<thead>
<tr>
<th></th>
<th>OP-1</th>
<th>OP-2</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP spoofing is feasible</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Free-uplink-attack is viable</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Maximum spoofing MSB</td>
<td>24 (all)</td>
<td>32 (all)</td>
</tr>
<tr>
<td>Fully spoofable?</td>
<td>No</td>
<td>OP-1: fewer spoofable addresses</td>
</tr>
</tbody>
</table>

- More findings: 4G/3G/2G, geo locations
Authorization

Uplink via authentication

Filter established

Filtering

Downlink via implicit mapping
Authorization Frauds

Close the app
(TCP: half-open, UDP: still open)

Filter: still valid (stateful)

Authorization: one-time;
Only in the core

U.IP

MMS Server X

PGW

CCS'14
Authorization Frauds

No proper authorization for downlink traffic

Causes:
- Network-based authorization;
- IP-push model

Cloak-and-dagger attacks:
- via MMS
- via IP Spoofing

More covet and threatening:
Nothing done at the victim

Can’t say NO

Dest. IP given

U’s bill

P-GW
In Real Networks

- US-1: via IP spoofing
- US-2: via MMS
- Attacks (overcharge)
  - Last 80 minutes (no sign of limit)
  - ~ 120MB charged (no sign of limit)
Packets can be lost after being charged

Accounting: Volume = local view @ P-GW

Accounting: In parallel with data
Accounting Inflation

Causes:
(1) Open-loop accounting arch.
(2) Independent packet delivery

More covet:
no data received at victim

Hit-but-no-touch Attack via TTL

TTL = 0 (dropped)
TTL >= 0
TTL = n

P-GW
In Real Networks

- **US-1 and US-2 both suffer**
  - **US-1**: TTL = 26, 27, 28
  - **US-2**: TTL = 18

![Graph showing volume and TTL for OP-I and OP-II](image)
How to defend?
Key Issues

Packet: source and destination

Packet: connectionless, no state

Packet: independent over hops

Charging: who is authenticated entity? (control plane vs. data plane)

Charging: what is the state of connection packets serves (@phone vs. @network)

Charging: Is it delivered? (at the end vs. in the middle)
## Basic Ideas

<table>
<thead>
<tr>
<th>Authentication</th>
<th>Authorization</th>
<th>Accounting</th>
</tr>
</thead>
<tbody>
<tr>
<td>The user being billed = Who transfers data.</td>
<td>The user agrees to use data and pay it.</td>
<td>Volume should be accurate.</td>
</tr>
</tbody>
</table>

### Loopholes

- **Authen. bypass** (No secure binding)
- **Authorization frauds** (No deauthorization)
- **Account. inaccuracy** (Local view @core)

### Proposed defense

- **Cross-layer secure binding in data plane**
- **Explicit de-deauthorization in the control plane**
- **Feedback from end/network + de-deauthorization**
Defense Framework

- Standard compatible

Authenticated, Verified ID

Runtime Access Control

Accounting Correction

Fraud Detector

Event Alerter

Event Alerter & Volume Corrector

Mischarging Handler

Secure Binding

Always implicit (de) author.

Explicit de-authorization

P-GW
Prototype and Evaluation

➤ Gateway = PC (out of carrier network)
➤ Test: all except secure binding
  ▪ All attacks + other attacks in [CCS’12, NDSS’14]
➤ Results: effective
Latest Update

- Positive response from US carriers
  - All these vulnerabilities are verified officially

- Work with US carriers to fix the issues
  - Nationwide upgrade (Nov 2014)
  - Initial fix in place
Summary

- Systematic security analysis of AAA for mobile data charging

- Uncover vulnerabilities and real threats
  - No sophisticated attacks needed

- Simple and effective defense proposed

- Immediate upgrade in carrier networks