TOWARDS A SECURE ZERO-RATING FRAMEWORK WITH THREE PARTIES

Authors: Zhiheng Liu, Zhen Zhang, Yinzhi Cao†, Zhaohan Xi, Shihao Jing and Humberto La Roche ‡
Lehigh University, †Johns Hopkins University/Lehigh University, ‡Cisco System
Hi Zhen,
Give me some data ...
2G...
2G...
2G...
Loading zhza16@lehigh.edu...

PuTTY Fatal Error

Network error: Connection timed out

2G...
Is that possible …

Zero-rating Services
Yes, Let’s fool the ISP…

Zero-rating Services
Yes, let's fool the ISP… Launch free-riding attacks

Zero-rating Services
Threat Model of Free-riding Attacks
Threat Model of Free-riding Attacks

Clients
malicious

ISP

Content Providers
Threat Model of Free-riding Attacks

- Clients
  - malicious

- ISP
  - ISP is benign/victim

- Content Providers
Threat Model of Free-riding Attacks

- Clients (malicious)
- ISP (benign/victim)
- Content Providers
- Zero-rated CPs are benign/victim
Threat Model of Free-riding Attacks

Clients

malicious

ISP is benign/victim

Attacker can masquerade zero-rating CP

Content Providers

Zero-rated CPs are benign/victim

ISP is benign/victim

malicious
Outline

- Introduction
- Free-riding Attacks
- System Design
- Formal Security Analysis
- Implementation
- Evaluation
- Conclusion
Request Masquerade Attack on Industry System

- Masquerade request domain
  - HTTP: “Host” field [1]
  - HTTPs: “SNI” field


08/15/2018  @Zhen Zhang (zhangzhen.dev@gmail.com)
Request Masquerade Attack on Industry System

- Masquerade request domain
  - HTTP: "Host" field [1]
  - HTTPs: "SNI" field

Masquerade request domain
- HTTP: “Host” field [1]
- HTTPs: “SNI” field

Request

srcIP, dstIP ...

<data>

SNI/Host: www.youtube.com

Request Masquerade Attack on Industry System

- Masquerade request domain
  - HTTP: “Host” field [1]
  - HTTPs: “SNI” field


08/15/2018 @Zhen Zhang (zhangzhen.dev@gmail.com)
Request Masquerade Attack on Industry System

- Masquerade request domain
  - HTTP: “Host” field [1]
  - HTTPs: “SNI” field


08/15/2018 @Zhen Zhang (zhangzhen.dev@gmail.com)
Response Modification Attack on Industry System

- Inject non-zero-rated content

Client

Request
- srcIP, dstIP ...
- <data>
  - SNI/Host: www.zero-rated.com

ISP Network

Zero-rated domain list

Zero-rated CP

Response
- srcIP, dstIP ...
- <data>
Response Modification Attack on Industry System

- Inject non-zero-rated content

![Diagram showing the process of injecting non-zero-rated content via an ISP network and zero-rated CP.]
Prototype Zero-Rating Systems

- Network Cookies [1]
  - A malicious user can abuse the cookie.

- IP Whitelist-based Method [2]
  - An attacker at the server side can abuse source IP address.

Attacks on Network Cookies

- Network Cookies [1]
  - A malicious user can abuse the cookie.

---


Attacks on Network Cookies

- Network Cookies [1]
  - A malicious user can abuse the cookie.

Attacks on Network Cookies

- Network Cookies [1]
  - A malicious user can abuse the cookie.


Attacks on IP whitelist based system

- Facebook Zero [2]
  - An attacker at the server side can abuse source IP address.

---


Attacks on IP whitelist based system

- Facebook Zero [2]
  - An attacker at the server side can abuse source IP address.


08/15/2018 @Zhen Zhang (zhangzhen.dev@gmail.com)
Attacks on IP whitelist based system

- Facebook Zero [2]
  - An attacker at the server side can abuse source IP address.

---


Attacks on IP whitelist based system

- Facebook Zero [2]
  - An attacker at the server side can abuse source IP address.


Attacks on IP whitelist based system

- Facebook Zero [2]
  - An attacker at the server side can abuse source IP address.

## Attacks on Zero-Rating Systems

<table>
<thead>
<tr>
<th>T-Mobile</th>
<th>China Mobile</th>
<th>China Unicom</th>
<th>United WiFi</th>
<th>ORD WiFi</th>
<th>Network Cookies [1]</th>
<th>IP Whitelist</th>
</tr>
</thead>
<tbody>
<tr>
<td>Req-Mas</td>
<td>✗</td>
<td>✗</td>
<td>N/A</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>Res-Mod</td>
<td>✗</td>
<td>✗</td>
<td>N/A</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>Req-Mas</td>
<td>✗</td>
<td>N/A</td>
<td>✗</td>
<td>N/A</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>Res-Mod</td>
<td>✗</td>
<td>N/A</td>
<td>✗</td>
<td>N/A</td>
<td>✗</td>
<td>✗</td>
</tr>
</tbody>
</table>

![Unencrypted Traffic](lock_unencrypted.png) ![Encrypted Traffic](lock_encrypted.png) | Unencrypted Traffic; Encrypted Traffic; Req-Mas: Request Masquerade; Res-Mod: Response Modification

Impacts of free-riding attacks

- A major U.S. network carrier lost over 7 millions in a month [1]
- China Mobile lost over 0.5 million/month in one province.
  - Filtering abnormal users, i.e., those consuming over 3 GB per month zero rating traffic
  - Inspecting unencrypted data manually
  - Results: found 71TB free-riding traffic

Outline

▪ Introduction
▪ Free-riding Attacks
▪ **System Design**
▪ Formal Security Analysis
▪ Implementation
▪ Evaluation
▪ Conclusion
System Design: Overview

Client

ISP
Assistant

ISP
Network

Content
Provider

Server
Agent
System Design: Overview

Client

ISP Assistant

Control Plane

Server Agent

ISP Network

Content Provider
System Design: Overview

Client

ISP Network

ISP Assistant

Control Plane

Server Agent

Content Provider
System Design: Overview

ISP Assistant | Control Plane | Server Agent

ISP Network

Content Provider

Mirrored traffic

Client
System Design: Overview

Client

ISP Network

ISP Assistant

Server Agent

Content Provider

Mirror/redirect

Mirrored traffic

Control Plane

08/15/2018
@Zhen Zhang (zhangzhen.dev@gmail.com)
System Design: Overview

ISP Assistant
Control Plane
ISP Network
Server Agent
Mirrored traffic

If blocking mode
Mirror/redirect

Client
System Design: ISP Assistant

- Blocking/Non-Blocking Mode
- Accept hash values and match

ZFREE ISP Assistant

- Integrity Check
- Hash Engine
- Packet Parser
- ISPHashDB
- CPHashDB
- Ctrl Plane Interface
System Design: ISP Assistant

- Blocking/Non-Blocking Mode
- Accept hash values and match

ZFREED ISP Assistant

- Integrity Check
- ISPHashDB
- CPHashDB
- Hash Engine
- Packet Parser
- Ctrl Plane Interface
- ZFREE Control Plane
- ZFREE Server Agents

08/15/2018
@Zhen Zhang (zhangzhen.dev@gmail.com)
System Design: ISP Assistant

- Blocking/Non-Blocking Mode
- Accept hash values and match
System Design: ISP Assistant

- Blocking/Non-Blocking Mode
- Accept hash values and match
System Design: ISP Assistant

- Blocking/Non-Blocking Mode
- Accept hash values and match

ZFREE ISP Assistant

Integrity Check

ISPHashDB

CPHashDB

Hash Engine

Packet Parser

Ctrl Plane Interface

ZFREE Control Plane

ZFREE Server Agents

ISP Network

Mirrored or redirected traffic
System Design: ISP Assistant

- Blocking/Non-Blocking Mode
- Accept hash values and match

If Blocking Mode: send packets back
System Design: ISP Assistant

- Blocking/Non-Blocking Mode
- Accept hash values and match

If Blocking Mode: send packets back
System Design: Server Agent

- Get network traffic through port mirror
- Real-time/Batch hash report
System Design: Server Agent

- Get network traffic through port mirror
- Real-time/Batch hash report
System Design: Server Agent

- Get network traffic through port mirror
- Real-time/Batch hash report
System Design: Server Agent

- Get network traffic through port mirror
- Real-time/Batch hash report
System Design: Server Agent

- Get network traffic through port mirror
- Real-time/Batch hash report
System Design: Server Agent

- Get network traffic through port mirror
- Real-time/Batch hash report
System Design: Server Agent

- Get network traffic through port mirror
- Real-time/Batch hash report
Outline

- Introduction
- Free-riding Attacks
- System Design
- Formal Security Analysis
- Implementation
- Evaluation
- Conclusion
Formal Security Analysis

- Using ProVerif

<table>
<thead>
<tr>
<th>Goals</th>
<th>Network Cookies[1]</th>
<th>IP Whitelist</th>
<th>ZFree</th>
</tr>
</thead>
<tbody>
<tr>
<td>Packet Integrity</td>
<td>✗</td>
<td>✗</td>
<td>✓</td>
</tr>
<tr>
<td>CP Authenticity</td>
<td>✗</td>
<td>✗</td>
<td>✓</td>
</tr>
<tr>
<td>Data Secrecy</td>
<td>✗</td>
<td>✓</td>
<td>✗</td>
</tr>
</tbody>
</table>


Audio/Video: Unencrypted/Encrypted data plane communication
Outline

- Introduction
- Free-riding Attacks
- System Design
- Formal Security Analysis
- Implementation
- Evaluation
- Conclusion
Implementation

- ZFree Prototype: 1,890 Lines of Code (LoC):
  - 1,100 LoC for ISP assistant
  - 790 LoC for Server Agent
- LTE network (ns3)
- WiFi network (Mininet)
- Formal verification code: 1,680 LoC
Outline

▪ Introduction
▪ Free-riding Attacks
▪ System Design
▪ Formal Security Analysis
▪ Implementation
▪ Evaluation
▪ Conclusion
Evaluation: Environment Setup

- Airplane WiFi: Mininet-WiFi
- 120 User Equipments (UEs)
- Two Access Points (AP)
- 30 Mbps
Evaluation: Environment Setup

- LTE network: ns3
- 1,200 UEs, two base stations (BSs)
- UE moving at speed 10-120km/h
Evaluation: Environment Setup

- LTE network: ns3
- 1,200 UEs, two base stations (BSs)
- UE moving at speed 10-120km/h
Evaluation: Page Loading Time Overhead is Ignorable

- Metric: Loading Time
- Content Provider as Network Proxy
- Top 500 Alexa websites
Evaluation: Transmission Overhead is Small
Evaluation: ZFree is Scalable

- Cellular Network:
  Bandwidth 150Mbps
Evaluation: ZFree is Durable
Evaluation: ZFree is Secure

- ZFree is robust against:
  - Request Masquerade attack
  - Response Modification attack
  - TCP retransmission-based attacks [1]

Outline

- Introduction
- Free-riding Attacks
- System Design
- Formal Security Analysis
- Implementation
- Evaluation
- Conclusion
Conclusion

- We launch free-riding attacks against real-world zero-rating services.
- We propose and implement ZFree, a secure, backward compatible, scalable zero-rating framework.
- We formally prove that ZFree is secure.
- Our evaluation results show that ZFree incurs ignorable overhead and is scalable.
Thank You! Questions?

- Source Code: https://github.com/zfree2018/ZFREE
- Online Demo: http://www.zfree.org