Header Enrichment or ISP Enrichment?
Emerging Privacy Threats in Mobile Networks

Narseo Vallina-Rodriguez, ICSI
Srikanth Sundaresan, ICSI
Christian Kreibich, ICSI / LastLine
Vern Paxson, ICSI / UC Berkeley

ACM HotMiddlebox 2015. London
“In the mobile space delivering the right ad to the right person is difficult because there is no common standard for identity and addressability. We think we’re in a position to solve that”

–Colson Hillier, VP of Verizon’s Precision Market Insight division.
HTTP Header Enrichment

(a.k.a Header Injection)

IETF Working Group SFC
Service Functioning Chaining

https://datatracker.ietf.org/wg/sfc/documents/
HTTP Header Enrichment

• Technique that allows ISP-enforced proxies to extend/inject HTTP headers for:
  ‣ Performance Enhancement
  ‣ Load Balancing
  ‣ Access Control
  ‣ Content Customization
  ‣ Analytics
  ‣ Advertising and user-tracking
How does HTTP Header Enrichment work?
How does HTTP Header Enrichment work?

GET /index.html HTTP/1.1
Host: www.example.com
x-acr: 486E03F2A285E07F5A981152DB80BB4932022388EC34B22434928;ncc=310410;type=Dyna
How does HTTP Header Enrichment work?

GET /index.html HTTP/1.1
Host: www.example.com
x-acr: 486E03F2A285E07F5A981152DB80BB4932022388EC34B22434928;ncc=310410;type=Dyna
User Implications

- HTTP Header Enrichment may become a privacy threat for mobile users:
  - ISPs may **leak** sensitive user and device data
  - ISPs may enable **user-tracking** (unique IDs)
Why does it matter?

• User sensitive data may be **collected** and **combined** with other metadata by **any** online service if not removed by the egress point

• IETF GW SFC leaves this decision up to the ISP
Inappropriate use of HTTP Header Enrichment affects millions of mobile subscribers all over the world.
Paper Contributions

- Identification, analysis and characterization of HTTP Header Enrichment:
  - 299 Mobile ISPs from 112 countries
  - 16-month period
- Data collection: Netalyzr for Android traces
- Discussion of user implications and solutions
Method and Data Collection
How does HTTP Header Enrichment work?

Mobile ISP Network

ISP Proxy

Internet

example.com

GET /index.html HTTP/1.1
Host: www.example.com

GET /index.html HTTP/1.1
Host: www.example.com
x-acr: 486E03F2A285E07F5A981152DB80BB4932022388EC34B22434928;ncc=310410;type=Dyna
Netalyzr: Proxy Artifacts Detection

We control both end-points and generated traffic: we can identify modifications!
Method Limitations

• We cannot identify when HTTP Header Injection occurs to selected destinations (e.g., ISP partners)

• Crowd-sourcing data collection: discrete sampling
Results
HTTP Header Analysis

We defined 3 categories:

- ✓ Privacy-compromising headers
- ✓ Tracking headers
- ● Operational headers

Header Enrichment or ISP Enrichment? Emerging Privacy Threats in Mobile Networks

Narseo Vallina-Rodriguez*, Srikanth Sundaresan*, Christian Kreibich*,†, Vern Paxson*‡

*ICSI, †Lastline, ‡UC Berkeley
{narseo,srikanth}@icsi.berkeley.edu, {christian,vern}@icir.org
Privacy-compromising headers

**Definition:** HTTP headers leaking sensitive information that identify uniquely:

- the device (e.g., **IMEI**)
- the user (e.g., **IMSI/MSISDN**)

Identified in **5 mobile operators**
# Privacy-compromising headers

<table>
<thead>
<tr>
<th>Header</th>
<th>Value</th>
<th>Provider (Country)</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>x-up-calling-line-id</td>
<td>Vodacom (ZA)</td>
<td>Phone #</td>
<td></td>
</tr>
<tr>
<td>msisdn</td>
<td>Orange (JO)</td>
<td></td>
<td>MSISDN</td>
</tr>
<tr>
<td>x-nokia-msisdn</td>
<td>Smart (PH)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>x-up-3gpp-imeisv</td>
<td>Vodacom (ZA)</td>
<td>IMEI</td>
<td></td>
</tr>
</tbody>
</table>

**x-up-3gpp-imeisv:** 35858805517XXXXXXXX
2 Tracking headers

**Definition:** Operator-generated unique identifier for *advertising* purposes

- They are immutable
- They do not directly reveal sensitive information about users but enable user-tracking

Identified in **6 mobile operators**
## Tracking headers

<table>
<thead>
<tr>
<th>Header</th>
<th>Company</th>
</tr>
</thead>
<tbody>
<tr>
<td>x-acr</td>
<td>AT&amp;T (US)</td>
</tr>
<tr>
<td>x-amobee</td>
<td>Airtel (IN), Singtel (SG)</td>
</tr>
<tr>
<td>x-uidh</td>
<td>Verizon (US)</td>
</tr>
<tr>
<td>x-vf-acr</td>
<td>Vodacom (ZA), Vodafone (NL)</td>
</tr>
</tbody>
</table>

x-acr: 486E03D […]D359D; ncc=310410; type=Dyna
2 Tracking headers

Date

- x-amobee-1
- x-acr
- x-amobee-2
- x-uidh
- x-vf-acr
- x-vf-acr

Header injected
Header not injected

Airtel (IN)
AT&T (US)
Singtel (SG)
Verizon (US)
Vodacom (ZA)
Vodafone (NL)
### Operational headers

**Definition:** HTTP headers for operational purposes. They contain information such as:

- Mobile operator (**MCC/MNC** codes) and 3GPP technology
- 3GPP Gateway, manufacturer (**Nokia/BlueCoat**), software version and even its location
- Handset’s private IP address

Identified in **24 operators**
Use-case: **x-forwarded-for** header [RFC 7239]
- Reports the internal IP address of proxied traffic
- Used for load-balancing and abusive access

Flip-side:
- **De-anonymizes** traffic
- It may not tell the truth!

Final Remarks
What can users do?

- Tech-savvy users may use **VPNs**
- “**Do-Not-Track**” header is useless
Be aware and complain

http://amibeingtracked.com
This problem also requires non-technical solutions
This is an increasing concern!

- Evidence of **JavaScript injection** for advertising
- New **3rd party services** providing advertising services for ISPs
- No evidence of header injection in **HTTPS** traffic (**yet**)