Attacking Mobile Broadband Modems Like A Criminal Would

Andreas Lindh, @addelindh, Black Hat USA 2014
whoami

- Security Analyst with I Secure Sweden
- Technical generalist
- I like web
- Not really an expert on anything
Agenda

• Introduction
• Target overview
• Attacks + demos
• Summary
Introduction
What’s it about?

Source: http://www.smbc-comics.com
This is what it’s about

- Practical attacks
- Likely to happen
- Easy to execute
- Great potential for paying off
Why USB modems?

- Very popular
  - ~130 million devices shipped in 2013
- Few vendors
  - Not that many models
  - Shared code between models
Target overview
Previous research

- Nikita Tarakanov & Oleg Kupreev
  - From China With Love (Black Hat EU 2013)

- Rahul Sasi
  - SMS to Meterpreter – Fuzzing USB Modems (Nullcon Goa 2013)
Scope

• Devices from the two biggest vendors*
  – Huawei
  – ZTE

• Focus on one device from each
  – Huawei E3276
  – ZTE MF821D

• Identify common attack surface

*Combined market share of more than 80% in 2011 (www.strategyanalytics.com)
In a nutshell

- Runs embedded Linux
- Mobile capabilities
  - GSM, 3G, 4G, SMS
- Web interface
  - Part of carrier branding
- No authentication
  - Single-user device
Network topology

192.168.x.0/24

Public IP

192.168.x.1

192.168.x.0/24

192.168.x.x

WWW

192.168.x.x
Attacks

or

“What would Robert Hackerman do?”
Ground rules

- **Objectives**
  1. Make money
  2. Steal information
  3. Gain persistence

- **Pre-requisites**
  1. Remote attacks only
  2. See #1
Out of scope (but possible)

- Disconnect the device
- Lock out PIN and PUK
- Permanently break the application

```
'; if((NetStat_roam!='2')&&!((roamstatus_roam=='1')&&(2==service_status_roam))&&!((roam_status_info=='1')))
  if(!confirm(On_roam[lang_index])) { flag = true; }
  if(flag == true) {
    alert("The page at 192.168.0.1 says:
    You need to restart the device, input PUK code to unlock it!"
    top.global_set_cookie("disconnectWaiting", "true", 3600000,
    top.global_set_cookie("always_on_to_roam", "false", 3600000,
    file=4&node=AutoManual&value=1&rd=4&node=AutoManual&value=1&rd=
    document.netConnect.action = "goform/SetNetworkSelectionMode?
    /alert("after"); } } function initpage() { get_pin_status(); initTranslation(); }
```

- Permanently brick the device
Attacking configuration
DNS poisoning
DNS poisoning

```xml
<?xml version="1.0" encoding="UTF-8"?>
<request>
  
  <SetDefault>0</SetDefault>
  
  <Profile>
    <Index/>
    <IsValid>1</IsValid>
    <Name>malicious</Name>
    <ApnIsStatic>1</ApnIsStatic>
    <ApnName>internet.telenor.se</ApnName>
    <DialupNum>*99#</DialupNum>
    <Username/>
    <Password/>
    <AuthMode>0</AuthMode>
    <IpIsStatic>0</IpIsStatic>
    <IpAddress/>
    
    <DnsIsStatic>0</DnsIsStatic>
    <PrimaryDns> </PrimaryDns>
    <SecondaryDns> </SecondaryDns>
    <ReadOnly>0</ReadOnly>
  </Profile>

</request>
```
DNS poisoning

- CSRF to add a new profile
- Static DNS servers
- Read Only & Set Default
- Remove original profile
- Send user to ad-networks, malware sites, spoofed websites, etc.
DNS poisoning - bonus attack

- Trigger firmware update
- Spoof update server
  - Downloads are over HTTP
  - No code signing
- Potentially get user to install backdoored firmware...
SMS MitM

SMS Settings

SMS report: ○ Enabled ○ Disabled

<?xml version="1.0" encoding="UTF-8"?>
<request>
    <SaveMode>0</SaveMode>
    <Validity>10752</Validity>
    <Sca>+46708000708</Sca>
    <UseSReport>0</UseSReport>
    <SendType>1</SendType>
    <Priority></Priority>
</request>
SMS MitM

• Replace the Service Center Address
• Set up rogue SMSC
• MitM all outgoing text messages
Abusing functionality
CSRF to SMS

- CSRF to make the modem send SMS
  - Send to premium rate number
- Potentially identify the user
  - Look up phone number
    - Twin cards
- Useful in targeted phishing attacks
Demo

Let’s go phishing!
Getting persistent
Getting persistent

• Multiple XSS vulnerabilities
• Configuration parameters

```
data_roam_option=1';alert(1);/\&SubmitRoam=Apply
```

```
function initTranslation2()
{
    var roam_status_info = '1';alert(1);/\';
}
```

• Configuration is persistent...
Getting persistent

• The web interface is where you go to connect to the Internet
  – Huawei Hilink opens main page automatically
  – ZTE creates a desktop shortcut

• The main page sets everything up
  – Loads an iframe for user interaction
  – It also loads the chosen language
Getting persistent

• Language is a configuration parameter loaded by the main page

```javascript
function change_lang_cookie_before_mlang_js()
{
    var xml_lang = 'en';
    setCookie('lang', xml_lang, 60*24*20);
}
```

• It is injectable...

```text
GET /goform/web_upd_xml?file=4&node=Language&string=en&rd=
```
Getting persistent

• Execute code every time the user connects to the Internet
• Interact with injected code
• Command channel
  – Poll remote server (BeEF style)
  – Out of band over SMS
Demo

SMS hooking
Summary
What to expect

• Attacks on configuration
  – Network
  – Mobile

• Abuse of functionality
  – Outbound & inbound SMS

• Injection attacks
  – Getting persistent
  – Stealing information
Getting it fixed

• ZTE is “working on it”
  – I have no details
  – ZTE does not seem to have a product security team 😞

• Huawei is fixing their entire product line
  – Nice++
  – Huawei has a product security team 😊

• Sounds pretty good though, right?
The update model is broken

• Vendors cannot push fixes directly to end-users
  – Branding complicates things
• Vendor -> Carrier -> User
  – Carriers might not make the fix available
  – Users might not install the fix
• Most existing devices will probably never get patched
Summary: analysis

- Web is easy
- Web is hard!
- How about the Internet of Things?
The OWASP Internet of Things Top 10 2014 (tentative) is as follows:

1. Insecure Web Interface
2. Insufficient Authentication/Authorization
3. Insecure Network Services
Don’t forget...

Marcus J. Carey @marcusjcarey · Jun 7
Risk associated with a lot of the "trending" security research is ridiculously small. Just ignore the stuff we can fix. #nothingtoseehere

Andreas Lindh @addelindh · Jun 7
@marcusjcarey 100% agree - stunt hacking sells tickets, real bad guys pick low-hanging fruit. pic.twitter.com/H8VMVNNCwC
Thank you for listening!

Andreas Lindh, @addelindh, Black Hat USA 2014