(U) I hunt TR-069 admins

PWNING ISPS LIKE A BOSS

Shahar Tal
no ISPs were harmed during the making of this presentation

corporate legal wouldn't let us
I know what you’ve been thinking: "My presentation at DefCon could use Taylor Swift’s keen insight on security."

Today’s your lucky day.
obligatory whoami

• Shahar Tal (@jifa)
• Father, husband, geek
• 10 years with IDF
Agenda

• Intro to TR-069
• Why you should care
• Landscape walkthrough
• Top kek pwnage
• Conclusion
Residential Gateway Security

• It sucks.

• Pedro Joaquin (Routerpwn), Jacob Holcomb (“SO HOpelessly broken”), Zachary Cutlip (“rooting SOHO”), devtty0 (everything)
TR-069 in 69 seconds

CPE WAN Management Protocol (CWMP/TR-069)

- 2004: v1.0
- 2013: v1.4 (amendment 5)
TR-069 Provisioning Session

SOAP RPC
(XML over HTTP)

Always* initiates session
ACS can issue “Connection Request”

Inform(reason)
<empty>
GetParameterValues(<key>*)
SetParameterValues(<key,value>*
<empty>

Dual authentication mechanism
TR-069 Example RPC (ACS → CPE)

```xml
<soapenv:Envelope ...
    ...
    <soapenv:Body>
        <cwmp:SetParameterValues>
            <ParameterList ...
                <Name>InternetGatewayDevice.ManagementServer.URL</Name>
                <Value>http://acs.supersecureisp.com/cwmp/</Value>
            </ParameterList>
        ...
    </cwmp:SetParameterValues>
</soapenv:Body>
</soapenv:Envelope>
```
Growing trend to adopt TR-069
  - Endorsed by Home Gateway Initiative, Digital Video Broadcasting, WiMax Forum

(2011) Estimated 147M TR-069 enabled devices online
  - 70% Gateways

According to zmap, 7547 is open on 1.12% of IPv4
Good Guy ACS

- Provision devices ("zero-touch configuration")
- Tech Support remote management
- Monitor for faults, errors or malicious activity
- Diagnostics and Performance
- Replace/fix faulty configuration
- Deploy upgraded firmware
Trust Issues

• Who do you trust to **run code** on your devices?
• Silently?
• Remotely?
• With elevated permissions?
• I *might* trust heavily protected updates from Apple / Microsoft / Google with this, but what about my ISP?
Remote Management

Turn Remote Management On

Remote Management Help
Using the Remote Management menu, you can allow a user on the Internet to configure, upgrade and check the status of your router.

IMPORTANT: Be sure to change the router's default password to a very secure one.

Allow Remote Access
For security, you should restrict access to as few external IP addresses as practical.

Click Only This Computer to allow access by only one IP address.

Click IP Address Range to allow access from a range of IP addresses on the Internet, enter a beginning and ending IP address to define the allowed range.

Click Everyone to allow access by everyone on the Internet.
TR-069 Configuration

TR-069 Client Configuration

Inform Status: [Enable/Disable]
Inform Interval: 3600
ACS URL: https://acs.[redacted]8443/d
ACS Username: [redacted]
ACS Password: [redacted]

Connection Request Authentication [on/off]
Connection Request User Name: [redacted]
Connection Request Password: [redacted]
TR-069 Status

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Serial Number</td>
<td>4494F000</td>
</tr>
<tr>
<td>TR069:</td>
<td>enable</td>
</tr>
<tr>
<td>ACS URL:</td>
<td><a href="https://acs...c/TR069">https://acs...c/TR069</a></td>
</tr>
<tr>
<td>ACS Username:</td>
<td></td>
</tr>
<tr>
<td>Periodic Inform Enable:</td>
<td>enable</td>
</tr>
<tr>
<td>Periodic Inform Interval:</td>
<td>900002</td>
</tr>
<tr>
<td>Periodic Inform Time(y-m-d T h:min:s):</td>
<td>0000-00-00T00:00:00</td>
</tr>
<tr>
<td>Connection Request Username:</td>
<td></td>
</tr>
<tr>
<td>CPE Port for ACS Access:</td>
<td>30005</td>
</tr>
</tbody>
</table>
TR-069 Architecture

Figure 1 – Positioning in TR-069 Architecture

SINGLE-POINT-OF-PWNAGE

Photo credit: https://www.etsy.com/shop/sharpwriter
I don't always want indiscriminate surveillance over all customers of a service provider.

But when I do, I pwn the ACS.
Scumbag ACS

• What would an attacker do if he was in control of an ACS?
• Get private data
  • SSID, hostnames & MAC addresses, usernames, VoIP
  • Get complete configuration incl. passwords (vendor-specific)
• Set every parameter
  • DNS servers
  • Wi-Fi (add new hidden SSID, remove password)
  • PPP (replace WAN service with attacker controlled tunnel)
• Download
  • Configuration, firmware, logs
• Upload
  • Configuration, firmware
Previous Work?

• Luka Perkov ("ISP’s black box" @ 29c3, UKNOF24)
• A brief survey of CWMP security (3SLabs)
  • http://blog.3slabs.com/2012/12/a-brief-survey-of-cwmp-security.html

• That’s about it.
  • (Apologies if my google fu wasn’t strong enough to find you)
Niche Market

- Service Provider world
- TR-069 community?

there doesn't seem to be anything here
TR-069 Community

ADB, Affinegy, Agile ACS, Alvarion, Arris, AVSystem, Axiros, Calix, Cisco, Comtrend, Consona, Dimark, Draytek, Fine Point Technologies, Friendly Tech, GIP, Incognito Software, Intraway, Iskratel, iWedia, Jungo, Juniper Bridge, Mobigen, Motive, Netgem Communications, Netmania, OneAccess, Pace, ProSyst, Ronankii Infotech, Sigma Systems, Tata Elxsi, Tilgin, Wi-tribe, Wind River, Works Systems
VigorACS SI
Auto Configuration Servers

30 Days Free Trial!!!
much ACS vendors

very TR-069

many features

such 1999 look & feel

wow
I got TR-069 problems
I’m so excited,
And I wish I could hide it,
Because someone’s about to lose control of their infrastructure,
And you’re not going to like it
How do you find ACSs ITW?

• Hack a single router. QED.

• Scanning
  • zmap/masscan FTW
  • 7547 and friends
  • UPnP endpoints

• Public datasets
  • Internet Census 2012
  • DNS Census 2013

• lmgtfy
  • lmstfy
ACS Authentication Drill Down

• **SSL** is RECOMMENDED
• 2nd option: shared secret
• Shared secret = HTTP auth (basic/digest)

**QUANTUM Capabilities – NSA**

(TS//SI//REL) NSA QUANTUM has the greatest success against <yahoo>, <facebook>, and Static IP Addresses. New QUANTUM realms are often changing, so check the GO QUANTUM wiki page or the QUANTUM SpySpace page to get more up-to-date news.

NSA QUANTUM is capable of targeting the following realms:

- IPv4_public
- alibabaForumUser
- doubleclickID
- emailAddr
- rocketmail
- hi5Uid
- hotmailCID
- linkedin
- mail
- mailruMrcu
- msnMailToken64
- qq
- facebook
- simbarUuid
- twitter
- yahoo
- yahoolBcookie
- ymail
- youtube
- WatcherID
Stealing the Secret

- Router interfaces try to protect ACS passwords.
- But... allow you to change the ACS URL.

ACS can even enforce HTTP Basic auth
  - Base64 encoded "username:password"
SSL Certificate Validation

If TLS 1.2 (or a later version) is used, the CPE MUST authenticate the ACS using the ACS-provided certificate. Authentication of the ACS requires that the CPE MUST validate the certificate against a root certificate, and that the CPE MUST ensure that the value of the CN (Common Name) component of the Subject field in the certificate exactly matches the host portion of the ACS URL known to the CPE (even if the host

AND THEN THEY SAID WE ACTUALLY NEED

A VALID CERTIFICATE
Field Test

Certificate Information

This CA Root certificate is not trusted. Install this certificate in the Trusted Root Authorities store.

Issued to: i-hunt-tr069-admins.com
Issued by: i-hunt-tr069-admins.com
Valid from 31/05/2014 to 28/05/2016

YOU CLAIM TO VALIDATE SSL CERTIFICATES
THE FACT YOU ACCEPTED MY SELF-SIGNED CERTIFICATE DETERMINED THAT WAS A LIE
Recap

- TR-069 is very powerful
- ACS makes a very lucrative, accessible target
- A LOT of implementations are just not serious enough

I know it all ends tomorrow;
So it has to be today;
For the first time in forever;
I have a Oday.
OpenACS

• Open source (Java)
• Start auditing
• 3 days later: RCE
• Reflection + Native File Upload = CVE-2014-2840
GenieACS

- Open source (Node.js, Redis, MongoDB)
- Start auditing
- 2 days later: RCE
- Non-Global regex - CVE-2014-4956
- Running as root

```javascript
output = input.replace(/\[[\]\\^$\.\?\+\(\)\]/, "\$&")
```

GET /devices?query="./;require('util').log('lolwut');/*" HTTP/1.1
PWNAGE

> be scanning ipv4 for GenieACS
> detect instance in middle-eastern ISP
> nbi exposed
> picard_facepalm.png
> OP delivers (vulnerability report)
> ISP support center not thrilled with Israeli calling about “vulnerable infrastructure”

> 8/10 would report again
Undisclosed Vendor

- Massive global install base incl. major providers
- Internal API auth bypass, 2xSQLi, DoS
  - CVE-2014-{4916,4917,4918,4957}
- Can write arbitrary files to any location
  - Including C:\Inetpub 😊 ➔ RCE
- Tested vulnerable provider (with permission)

```
+----------+
| count(*) |
+----------+
| 509158   |
+----------+
```
What can I do?

- Audit your TR-069 settings
  - Ensure SSL & proper cert validation
  - Unsatisfied? disable TR-069
    - (If you can)
- Add home security layer
  - Another router with NAT/FW capabilities
  - Open source firmware alternatives
- Ask your provider about their TR-069 configuration!
Fixing the Problem

• There is no easy fix.
  • Bad implementations are out there
  • TR-069 has to mature

• **Awareness** is key
  • Security community
    • That’s you guys
  • ACS vendors
    • Write better software, put money in secure coding
    • Show your security stance (bug bounties?)

• **Service Providers**
  • Protect your customers, it’s your responsibility

"Only the dead have seen the end of cyberwar."

-Taylor Swift
Future Directions

• TR-069 client pwnage
  • Stay tuned for CCC

InfoSec Taylor Swift
@SwiftOnSecurity

I’m sorry, I can’t hear you over my Thought Leadership.
Thank you!

Hit me up on @jifa or shahartal@checkpoint.com
- @swiftonsecurity
- https://www.iol.unh.edu/sites/default/files/knowledgebase/hnc/TR-069_Crash_Course.pdf TR-069 Crash Course (University of New Hampshire Interoperability Laboratory)
- http://internetcensus2012.bitbucket.org/ Internet Census 2012 (anonymous researcher)
- http://www.team-cymru.com/ReadingRoom/Whitepapers/SOHOPharming.html SOHO Pharming (Team Cymru)