



(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



InfoSec Taylor Swift

@SwiftOnSecurity



Following

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.

Reply Retweet Favorite More

RETWEETS

8

FAVORITES

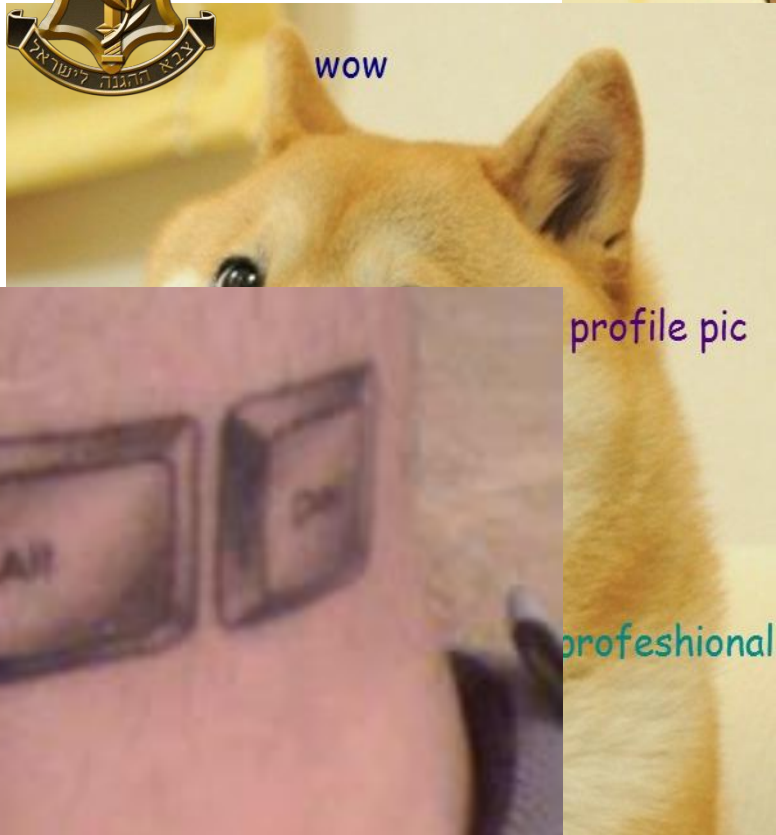
23



4:14 AM - 4 Aug 2014

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)

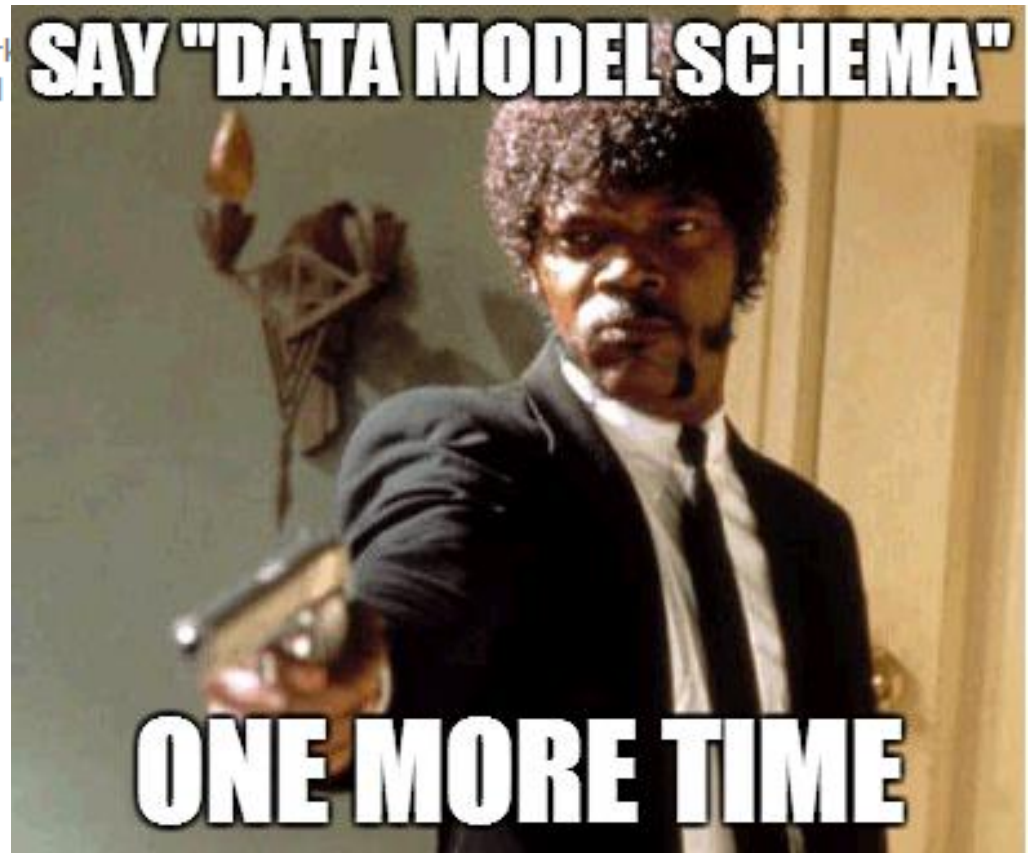
TR-069 in 69 seconds



We develop multi-service broadband packet network management. Our work enables home, business and backbone networks.

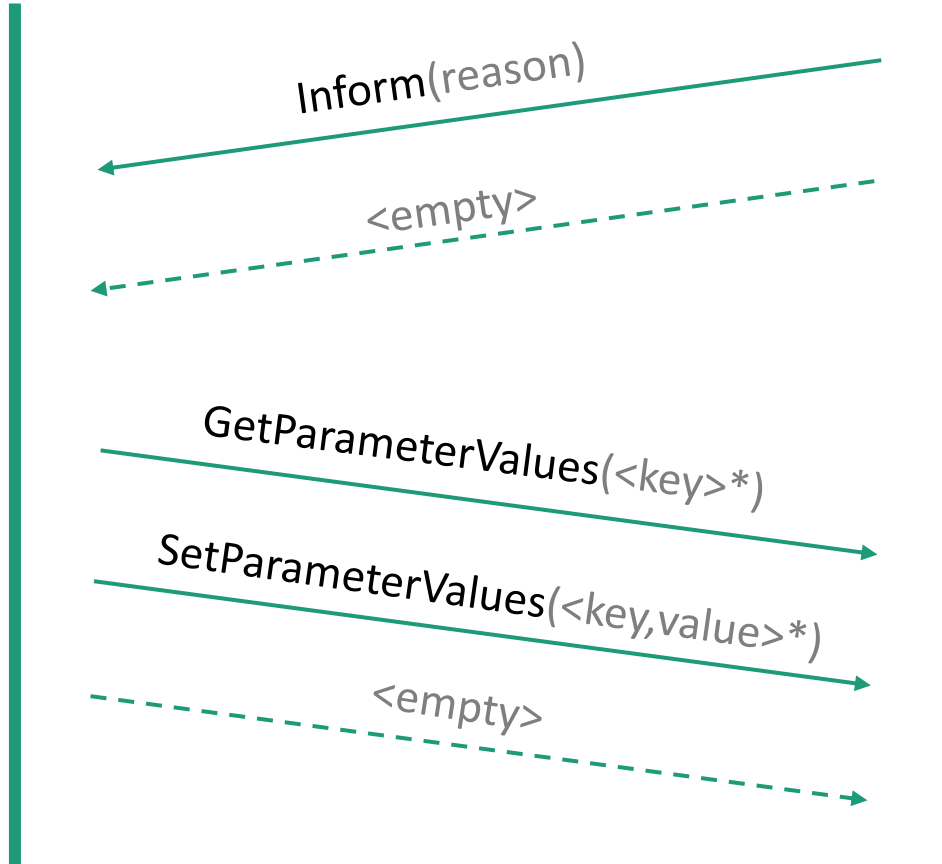
CPE WAN Management Protocol (CWMP/TR-069)

- 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"



Dual authentication mechanism

TR-069 Example RPC (ACS→CPE)

```
<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>
```

TR-who?



Port	Service	Hit Rate (%)
80	HTTP	1.77
7547	CWMP	1.12
443	HTTPS	0.93
21	FTP	0.77
23	Telnet	0.71
22	SSH	0.57
25	SMTP	0.43
3479	2-Wire RPC	0.42
8080	HTTP-alt/proxy	0.38
53	DNS	0.38

- 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?





- Firewall Rules
- Services
- Schedule
- E-mail

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

```
<TR>
  <TD vAlign=top><IMG height=7 alt="" src="redbull.gif" width=7 align=top vspace=6></TD>
  <TD><A href="USB_settings.htm" target=formframe><font color="#ff0000">USB Settings</font></A></TD></TR>
<!--
<TR>
  <TD vAlign=top><IMG height=7 alt="" src="redbull.gif" width=7 align=top vspace=6></TD>
  <TD><A href="TR069_tr069.htm" target=formframe><font color="#ff0000">TR069</font></A></TD></TR>
//-->
<TR>
  <TD vAlign=top>
  <TD><A href="start.htm" target=_top>Standard Mode</A></TD></TR>
```

- Wireless Settings
- Remote Management
- Static Routes
- UPnP
- USB Settings
- Standard Mode
- Logout

<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

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: Disable Enable

Inform Interval: 

ACS URL:

ACS Username:

ACS Password: 

Connection Request Authentication

Connection Request User Name:

Connection Request Password: 

Apply

Cancel

TR-069 Status

Device Serial Number:	4494F0 [REDACTED]
TR069:	enable
ACS URL:	https://acs [REDACTED] /TR069
ACS Username:	[REDACTED]
Periodic Inform Enable:	enable
Periodic Inform Interval:	900002
Periodic Inform Time(y-m-d T h:min:s):	0000-00-00T00:00:00
Connection Request Username:	[REDACTED]
CPE Port for ACS Access:	30005

TR-069 Archite

Figure 1 – Positioning in t



SINGLE-POINT-OF-PWNAGE

APT APT APT APT APT APT APT APT CYBER APT CYBER



Scumbag ACS



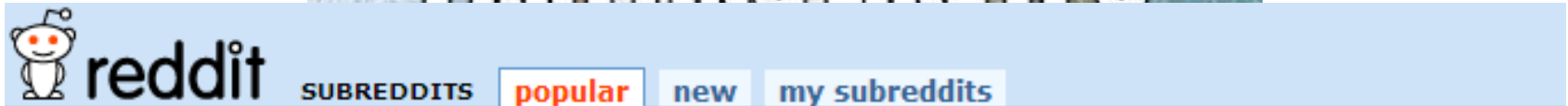
- What would an attacker do if he was in control of an ACS?
- Get private data
 - SSID, hostnames & MAC addresses, usernames, VoIP
 - Get complete configuration incl. passwords (vendor-specific)
- Set every parameter
 - DNS servers
 - Wi-Fi (add new hidden SSID, remove password)
 - PPP (replace WAN service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

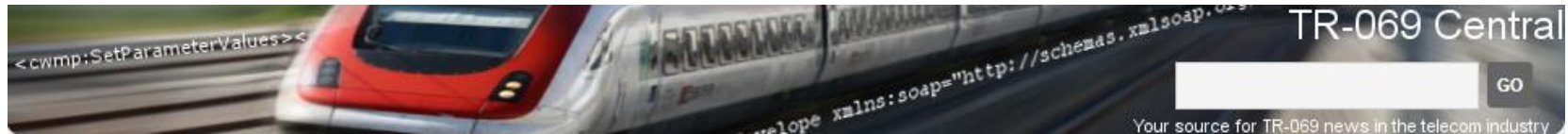


click the subscribe or unsubscribe buttons to choose which subreddits appear on your front page.

there doesn't seem to be anything here



TR-069 Community

A screenshot of a Twitter profile card for TR-069 Central. The profile picture is a purple square with a white egg shape inside. The name is "TR-069 Central" and the handle is "@TR069Central". It shows "FOLLOWS YOU" in a grey box. Below the profile information, there are three tabs: "TWEETS" with 53, "FOLLOWING" with 23, and "FOLLOWERS" with 16. To the right of these tabs is a gear icon and a blue "Following" button.

TWEETS	FOLLOWING	FOLLOWERS
53	23	16

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

DrayTek
Australia

VigorACS SI

Auto Configuration Servers



30 Days Free Trial!!!

i-LAN
www.i-lan.com.au

Produced by
I-Lan Technology





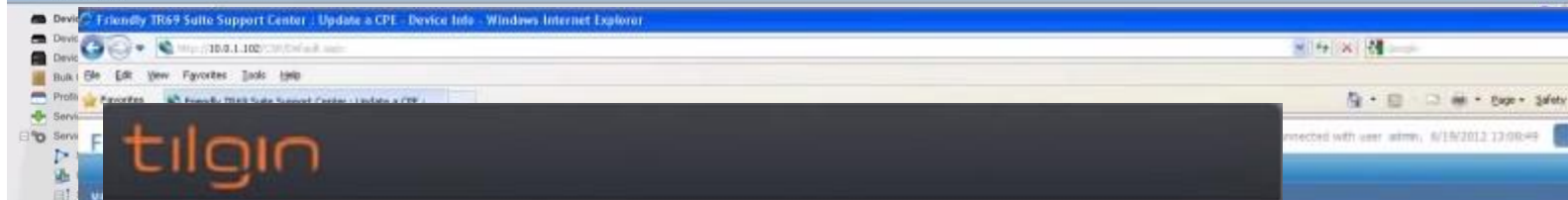
much ACS vendors

very TR-069

many features

such 1999 look & feel

WOW



<input checked="" type="checkbox"/>	Group	Serial number	IP address	Software
<input checked="" type="checkbox"/>	Triple-play	V60200000000-0010024001 *	77.68.153.46	HG13xxx CS5000-02_03_00_60
<input checked="" type="checkbox"/>	Triple-play	V60200000000-0010024002 *	77.68.146.205	HG13xxx CS5000-02_03_00_60
<input checked="" type="checkbox"/>	Triple-play	V60200000000-0010024003 *	77.68.145.154	HG13xxx CS5000-02_03_00_60
<input checked="" type="checkbox"/>	Triple-play	V60200000000-0010024004 *	77.68.145.241	HG13xxx CS5000-02_03_00_60
<input checked="" type="checkbox"/>	Triple-play	V60200000000-0010024005 *	77.68.145.195	HG13xxx CS5000-02_03_00_60
<input checked="" type="checkbox"/>	Triple-play	V60200000000-0010024006 *	77.68.162.152	HG13xxx CS5000-02_03_00_60
<input checked="" type="checkbox"/>	Triple-play	V60200000000-0010024007 *	77.68.130.142	HG13xxx CS5000-02_03_00_60
<input checked="" type="checkbox"/>	Triple-play	V60200000000-0010024008 *	77.68.130.142	HG13xxx CS5000-02_03_00_60
<input checked="" type="checkbox"/>	Triple-play	V60200000000-0010024009 *	77.68.221.47	HG13xxx CS5000-02_03_00_60
<input checked="" type="checkbox"/>	Triple-play	V60200000000-0010024010 *	77.68.160.13	HG13xxx CS5000-02_03_00_60
<input checked="" type="checkbox"/>	Triple-play	V60200000000-0010024011 *	77.68.128.168	HG13xxx CS5000-02_03_00_60
<input checked="" type="checkbox"/>	Triple-play	V60200000000-0010024012 *	77.68.146.6	HG13xxx CS5000-02_03_00_60
<input checked="" type="checkbox"/>	Triple-play	V60200000000-0010024013 *	77.68.152.96	HG13xxx CS5000-02_03_00_60
<input checked="" type="checkbox"/>	Triple-play	V60200000000-0010024014 *	77.68.134.39	HG13xxx CS5000-02_03_00_60
<input checked="" type="checkbox"/>	Triple-play	V60200000000-0010024015 *	77.68.147.105	HG13xxx CS5000-02_03_00_60
<input checked="" type="checkbox"/>	Triple-play	V60200000000-0010024016 *	77.68.128.135	HG13xxx CS5000-02_03_00_60
<input checked="" type="checkbox"/>	Triple-play	V60200000000-0010024017 *	77.68.162.249	HG13xxx CS5000-02_03_00_60
<input checked="" type="checkbox"/>	Triple-play	V60200000000-0010024018 *	77.68.130.246	HG13xxx CS5000-02_03_00_60
<input checked="" type="checkbox"/>	Triple-play	V60200000000-0010024019 *	77.68.156.2	HG13xxx CS5000-02_03_00_60
<input checked="" type="checkbox"/>	Triple-play	V60200000000-0010024020 *	77.68.165.196	HG13xxx CS5000-02_03_00_60

Voice quality [Back](#) [Delete](#) [Clear](#) [Report](#) [Export](#) [Save](#)

[Note] Changes in monitored parameters or devices will clear all existing data

Details

Name:

Description:

Scope:

Collect:

Raise a: Priority:

Monitored devices

Name:

Me: [Delete](#)

Monitored devices

[Add selected device\(s\)](#)

[Back](#) [Delete](#) [Clear](#) [Report](#) [Export](#) [Save](#)

I got TR-069 problems

**Insecure
Configuration**



**Insecure
Implementation**





InfoSec Taylor Swift

@SwiftOnSecurity



Following

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

[↩ Reply](#) [↻ Retweet](#) [★ Favorite](#) [⋮ More](#)

RETWEETS

25

FAVORITES

21



6:12 PM - 31 Jul 2014

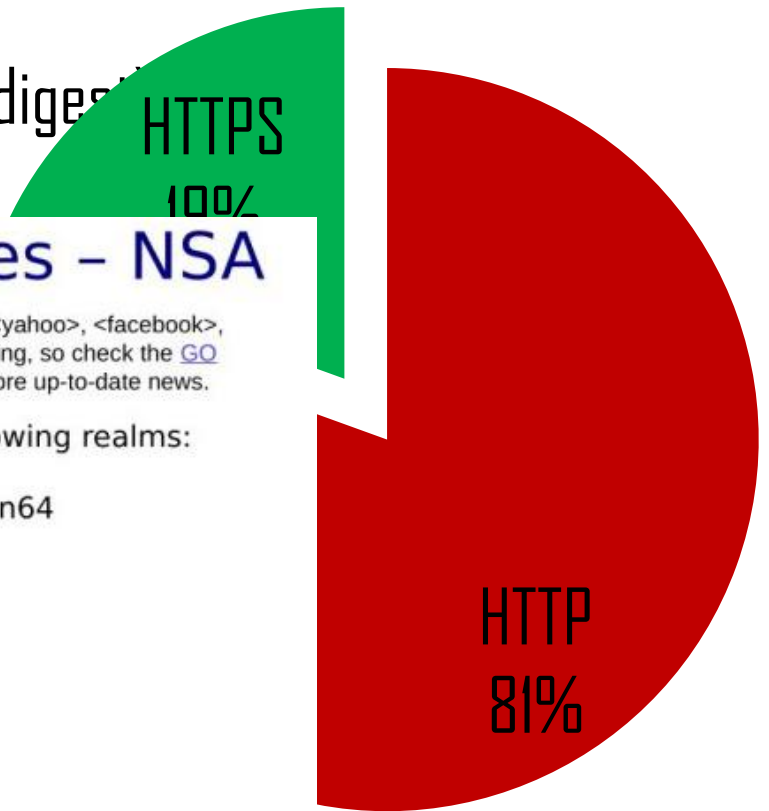
How do you find ACSs ITW?

- Hack a single router. QED.
- Scanning
 - zmap/masscan FTW
 - 7547 and friends
 - UPnP endpoints
- Public datasets
 - Internet Census 2012
 - DNS Census 2013
- **lmg**tfy
 - **lmst**fy



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
- mailruMrcu
- yahooBcookie
- gmail
- youTube
- WatcherID
- msnMailToken64
- WatcherID
- mailruMrcu
- msnMailToken64
- qq
- facebook
- simbarUuid
- twitter
- yahoo
- yahooBcookie
- gmail
- youTube
- WatcherID



Stealing the Secret

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

TR-069 Configuration

TR-069 Client Configuration

Inform Status: Disable Enable

Inform Interval:

ACS URL:

ACS Username:

ACS Password:

Connection Request Authentication

Connection Request User Name:

Connection Request Password:

- 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



Field Test



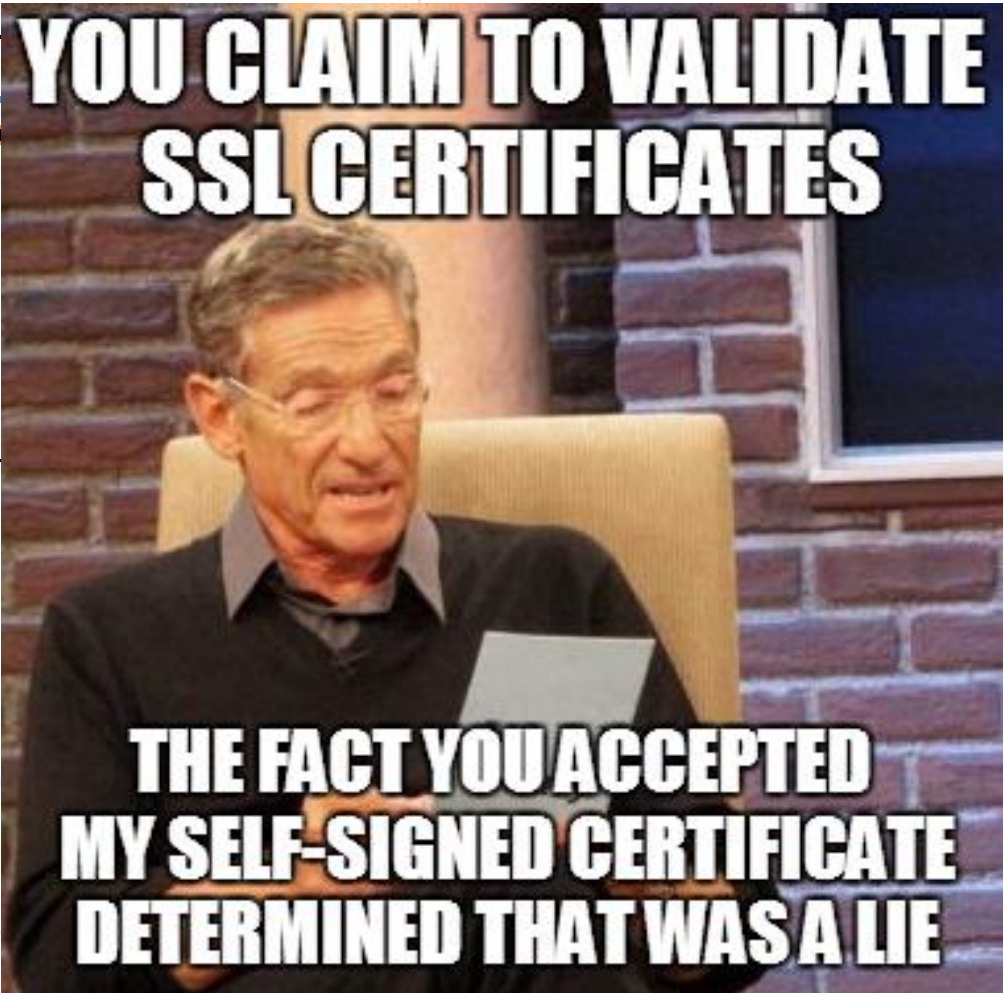
Certificate Information

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** 28/05/20



Recap

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



InfoSec Taylor Swift
@SwiftOnSecurity



Following

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

↩ Reply ↻ Retweet ★ Favorite ⋮ More

RETWEETS

FAVORITES



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

```
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

Showing 7314 devices

Serial number	Product class	Software version	MAC	IP	WLAN SSID	Last inform
78...	963...		78:5...	...	T79280D	9 months ago
78...	963...		78:5...	20.250	T780765	8 months ago
78...	963...		78:5...	20.235	T781675	8 months ago
78...	963...		78:5...	13		about 2 hours
78...	963...		78:5...	20.230	T7AD38D	8 months ago
78...	963...		78:5...	53		12 minutes ago
78...	963...		78:5...	39	9065	about 12 hours
78...	963...		78:5...	215		● less than 20
78...	963...		78:5...	121		● 2 minutes ago
78...	963...		78:5...	37	6520	about 2 hours
78...	963...		78:5...	5.165	4432	4 months ago
78...	963...		78:5...	20.93		7 months ago

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!

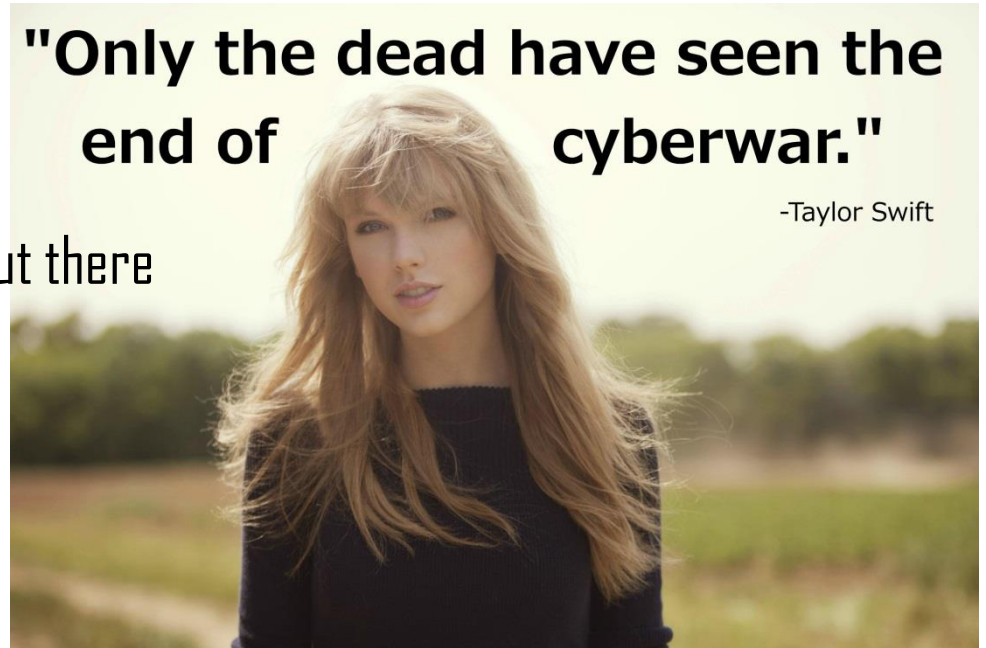


Fixing the Problem

- 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



Following

I'm sorry, I can't hear you over my Thought Leadership.

Reply Retweet Favorited More

RETWEETS
50

FAVORITES
44



6:03 PM - 8 Aug 2014

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)
- <https://community.rapid7.com/servlet/JiveServlet/download/2150-1-16596/SecurityFlawsUPnP.pdf> Whitepaper: Security Flaws in Universal Plug and Play: Unplug, Don't Play. (Rapid7)
- <http://internetcensus2012.bitbucket.org/> Internet Census 2012 (anonymous researcher)
- <http://www.team-cymru.com/ReadingRoom/Whitepapers/SOHOPharming.html> SOHO Pharming (Team Cymru)