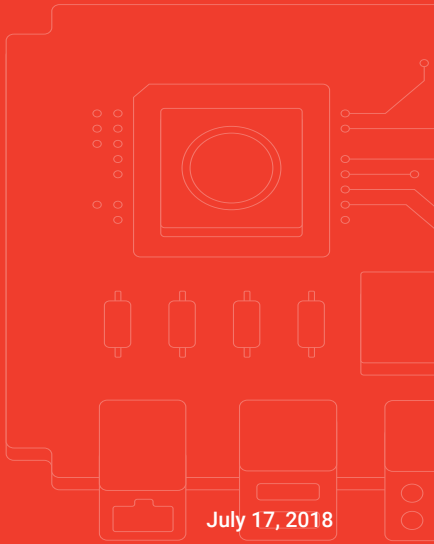
FSec IoT Hacking Summer School 2018

ISP's black box

Luka Perkov



sartura

July 17, 2018

About Sartura

- Programming, integration and consulting services in Open Source, telco, silicon vendor and the embedded manufacturers industries
- Developing solutions based on Linux, OpenWrt, and Yocto platforms
- Past CWMP-related talks:
  - ISP's black box, Chaos Communication Congress (29c3) 2012, Hamburg, Germany
  - Inside TR-069, UK Network Operators' Forum 2013, UKNOF24, Newark, England

Terminology

- *CPE* - Customer Premises Equipment
- *CWMP* - CPE WAN Management Protocol
- *ACS* - Auto Configuration Server
- *provisioning* - the process of CPE configuration

Why CWMP?

- How to effectively manage 10k, 100k, 1 million or more CPEs?
- How to handle the situation of different CPE vendors?
- How to define fine-grained access to certain information?

2004

First publication of TR-069

2011

Ovum report - 147 million TR-069-enabled devices online

2016

Mirai botnet - Deutsche Telekom outage

2018

Latest TR-069 specification (Issue 1 Amendment 6)

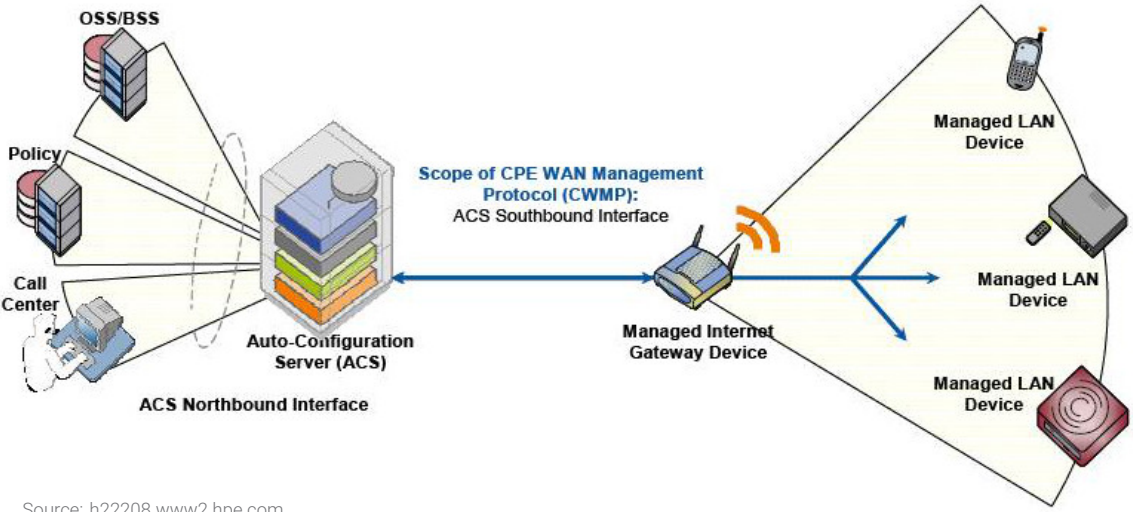
TR-069 (CWMP)

- *CWMP (CPE WAN Management Protocol)*
  - Sometimes referred to as ***TR-069*** (TR-069 Amendment 6) or ***TR-181***
- Technical specification of the Broadband Forum
- Application layer protocol for remote management of CPE

- Standardized, text-based protocol
- Enabling communication between ***Auto Configuration Servers (ACS)*** and CPE
- Offering management capabilities for a wide range of devices
- 2011 statistic by Ovum - around 147 million TR-069-enabled devices online (70 % of them residential gateways)

- Bidirectional SOAP/HTTP based protocol
- Communication in XML
- Around 20 TR-* schemas and data model definitions
- A lot of objects and parameters

- Two main units of a CWMP-based system:
  - ACS located in ISP-s data center
  - Client implemented in CPE
- Connection between CPE and ACS not permanent
  - Established at specific points in time
- Session always initialized by the device
- *Provisioning* - process of CPE configuration
  - ACS can re-provision CPE at any time after initial connection



Source: h22208.www2.hpe.com

Basic provisioning steps

1. CPE sends inform message
2. ACS replies with inform response message
3. CPE sends empty message saying that it has nothing more to report
4. ACS starts provisioning process
5. At some point CPE will receive all the data and ACS will send an empty message
6. CPE will reply with an empty message and provisioning is completed

CWMP functionalities

- Reboot, factory reset, flashing firmware
- Saving and restoring configuration
- Creating or deleting objects
- get or set parameter values
- get or set parameter attributes

Enables viewing and/or changing:

- Credentials for PPP, SIP, and other services
- Configuration for services such as DNS, DHCP
- Wireless settings
- Routing
- Firewall
- QoS

CWMP components

- *HTTP* - used for exchanging SOAP messages between a CPE and ACS
- *SOAP* - Standardized XML-based syntax used to encode remote procedures
- *RPC methods* - CPE parameters that are accessible by the ACS
  - Mechanisms which enable ACS to read and write CPE configuration parameters
  - Most common RPC methods: parameter values, parameter attributes, objects, file transfers, system

Publicized attacks

- 2016 - Mirai botnet
  - Attack on Deutsche Telekom
  - Vulnerability in RomPager server on port 7547
  - Not a TR-069 vulnerability but an implementation vulnerability
- 2016 - NewNTPServer feature used to execute arbitrary commands (ISP Eir's D1000 modem)

Identification of CPE devices

- SOAP (CWMP) message contains several mandatory parameters:
  - `Device.WANDevice. . . 1.ExternalIPAddress`
  - Used to obtain IP address of the management interface
- Checking user authenticity:
  1. Checking sole text of SOAP message
     - Easily faked
  2. Checking IP address of the IP packet

Transport security

- CWMP uses HTTP to transfer information between client and server
  - All HTTP vulnerabilities apply to CWMP
  - The TR-069 specification recommends use of HTTPS
- Important security steps:
  - Checking and validation of the server's certificate prevents false introductions
  - Public keys safely saved on the router
  - No user influence; complete security lies on the ISP

DoS attacks using protocol specifics

- ACS: two interfaces to two different network segments:
  - Southbound interface - facing CPEs
  - Northbound interface - facing ISP's data center and CRM
- Upon receiving inform message from CPE on southbound interface, ACS starts collecting provisioning information on northbound interface (time-consuming)
- New requests can be still continuously sent to the southbound interface, e.g. delivering a payload using a simple curl command:

```
$ curl -v -X POST -d "@payload.xml" http://user:pass@address:port/path/
```

Sartura FOSS CWMP implementations

- *freecwmp*
  - Open Source CWMP client
  - Only GPL licensed TR-069 client working with OpenWrt out of the box
- *freeacs-ng*
  - Stable and flexible ACS licensed under GPL
  - SCGI server using AMQP for message transfer
  - Enables creating complex provisioning rules

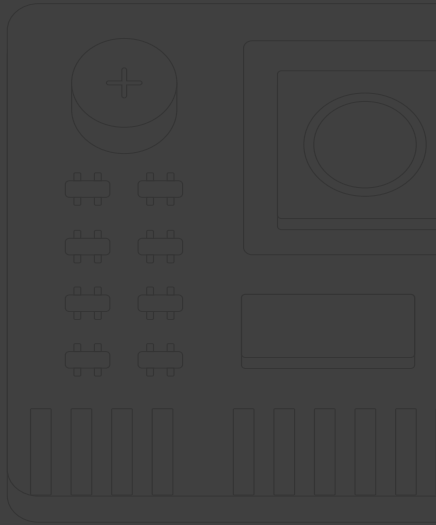
- *mod_cwmp*
  - Modular extension to Nginx HTTP server
  - Preventing protocol-based attacks in CWMP by doing deep message inspection
- *Rocket CWMP*
  - Successor to freecwmp
  - Carrier-grade solution to fill CWMP client market gap
  - Plugin-based

Conclusion

- Time-to-market brings low-quality products
- Devices running antiquated firmware
- Protocol designed in 90s with the 90s mindset
- Managing around 147 million devices
- The industry and the community does not seem to care

FSec IoT Hacking Summer School 2018

ISP's black box



info@sartura.hr · www.sartura.hr