Back to the Basics: Security of Software Downloads for Smart Objects

Alberto Bartoli, Andrea De Lorenzo, Eric Medvet, Fabiano Tarlao
University of Trieste

Internet of Things

Smart objects

Distributed sensing

"Whenever an appliance is described as being smart, it is vulnerable"

Hyppoponen's Law

LILY HAY NEWMAN SECURITY 04.01.17 07:00 AM

SECURITY NEWS THIS WEEK: YES, EVEN INTERNET-CONNECTED DISHWASHERS CAN GET HACKED

Why Light Bulbs May Be the Next Hacker Target

ANDY GREENBERG SECURITY 08.13.18 07:00 AM

HOW HACKED WATER HEATERS COULD TRIGGER MASS BLACKOUTS

FUTURE TENSE

The Ransomware Attack That Locked Hotel Guests Out of Their Rooms

This is a good demonstration of why electronic systems need physical backups.

By JOSEPHINE WOLFF FEB 01, 2017 • 2:09 PM

NEWS

465,000 Abbott pacemakers vulnerable to hacking, need a firmware fix

The FDA and Homeland Security issued alerts about vulnerabilities in Abbott (formerly St. Jude Medical) pacemakers and a firmware update to close those security holes.

Over a dozen vulnerabilities uncovered in BMW vehicles

Tencent's Keen Security Lab found a number of serious bugs which could be exploited by attackers to remotely attack a number of BMW models.

By Charlie Osborne for Zero Day | May 23, 2018 -- 10:10 GMT (11:10 BST) | Topic: Security

OUT IN THE COLD Netatmo smart heating outage leaves customers 'FREEZING' – because they can't turn temperature up

> The failure of the Netatmo Smart Thermostat was the result of a server outage, which put the Netatmo smartphone app out of action

Smart dildos and vibrators keep getting hacked – but Tor could be the answer to safer connected sex

Connected sex toys are gathering huge amounts of data about our most intimate moments. Problem is, they're always getting hacked. Welcome to the emerging field of Onion Dildonics

Agreed solution:

Update the software!

How to update?

- Keeping software up to date is crucial
- How to do it?
- Distributing software over web protocol is most common solution
- But… basic web protocol (HTTP) does not provide **any guarantee** of server **authentication** and **message integrity**
- Our study: is software actually distributed securely over HTTPS?

Threat model

Attacker goal: to alter the downloaded software

The attacker can:

- passively observe traffic sent to the server
- modify the traffic sent by server (e.g.: links in a page)

Assumptions

- No download authenticity or integrity verification
- Attacker cannot corrupt or control user platform
- Attacker cannot corrupt or control server infrastructure
- HTTPS is unbreakable

How difficult is it?

- At local scale: not so difficult
  - The attacker can easily set up a fraudulent Wi-Fi access point

- At global scale: harder, but not impossible
  - Security purpose: “NSA Plans to Infect `Millions’ of Computers with Malware”
  - BGP manipulation: “Hacker Redirects Traffic From 19 Internet Providers to Steal Bitcoins”
  - Script Injection: “How a banner ad of H&R Block appeared on apple.com without Apple’s OK”

Methodology

We analyzed almost 200 *web-based software download enviremontents*: web pages which allow to download an executable resource.

Crucial element for security: protocol for downloading

- HTTPS is ok
- HTTP is very easy to attack
- Depends on how the user obtains the link

Security Level

Configuration	Security Label
HTTP only	Insecure
HTTPS only	Secure
HTTPS, HTTP redirect to HTTPS	Partly Secure
HTTPS, HTTP	Partly Secure
Executable not publicly available	Unknown

Data collection

We collected data in May 2018

- 194 download environments of 163 brands
- 14 macro categories (IP cams, smart meters, networks, ...)
- Results based on several search queries in web engine to emulate user behaviour

Search queries

For each category:

- We identified of the main productors through Wikipedia and Amazon
- We setup a search query combining productor names with:
  - “Software”
  - “Firmware”
  - “Driver”
  - “Upgrade”
  - “Download”
  - “Install”
- We considered the first result page

Categories: brands and environments (1/2)

Category	Brands	Environments
Smart meters (energy)	8	10-5
Smart meters (gas)	8	8-6
Webcam	11	17-0
IP cameras (outdoor)	6	9-0
IP cameras (consumer)	11	12-0
IP cameras (best)	15	16-7
Electronics	38	52-7

Categories: brands and environments (2/2)

Category	Brands	Environments
Telecoms	4	4-1
Network (consumer)	8	10-0
Network (enterprise)	13	14-0
Energy meter	9	9-5
Smart thermostat	7	7-3
Industrial thermostat	2	2-1
ICS firmware	23	24-0

Categories: security level (1/2)

Category	Secure	Partly secure	Insecure
Smart meters (energy)	0-0	5-5	0-0
Smart meters (gas)	0-0	1-1	1-1
Webcam	0-1	12-12	4-3
IP cameras (outdoor)	0-0	7-4	2-5
IP cameras (consumer)	0-0	3-2	6-7
IP cameras (best)	0-0	6-5	2-3
Electronics	0-0	28-24	12-14

Categories: security level (2/2)

Category	Secure	Partly secure	Insecure
Telecoms	0-0	2-1	0-1
Network (consumer)	0-0	7-5	3-4
Network (enterprise)	0-0	12-10	2-4
Energy meter	0-0	3-3	1-1
Smart thermostat	0-0	0-0	2-0
Industrial thermostat	0-0	1-1	0-0
ICS firmware	1-0	17-13	6-10

Results

Security level	Percentage
Secure	0.6%-1.3%
Partly Secure	65.4%-54.1%
Insecure	25.8%-34.6%
Unknown	8.2%-10.1%

Strict transport security

It exists a prevention policy: HSTS

- Optional security enhancement
- Specified by a dedicated HTTP header
- Prevent browsers to receive non-HTTPS transactions

Strict Transport Security for HTTPS download pages

Category	HST	No HST
Smart meters (energy)	4	6
Webcam	7	4
IP cameras	4	19
Electronics	9	24
Telecoms	1	2
Network	3	16
Energy meter	0	5
Smart thermostat	0	3
Industrial thermostat	0	2
ICS firmware	4	13

Conclusions

Distributing software updates for smart objects will be crucial for society

- We analyzed hundreds of websites spreading software updates
- We discovered that the most part of them are insecure