



Security Aspects for IoT Projects

Guido Bertoni and Filippo Melzani

IoT, Internet of.. What?

What can go wrong?

The Mirai botnet explained: How teen scammers and CCTV cameras almost brought down the internet

Mirai took advantage of insecure IoT devices in a simple but clever way. It scanned big blocks of the internet for open Telnet ports, then attempted to log in default passwords. In this way, it was able to amass a botnet army.



October 2016



Smart lamps

IoT worm can hack Philips Hue lightbulbs, spread across cities

Easy chain reaction hack would spread across Paris, boffins say

The software nasty, detailed in a paper titled *IoT Goes Nuclear: Creating a ZigBee Chain Reaction* [[PDF](#)], exploits hardcoded symmetric encryption keys to control devices over Zigbee wireless networks. This allows the malware to compromise a single light globe from up to 400 metres away.

Shodan.io


Shodan Developers Monitor View All...

SHODAN port:1883 MQTT 🔍 🏠 Explore Downloads Reports Pricing Enterprise Access

Exploits Maps Share Search Download Results Create Report

TOTAL RESULTS
75,175

TOP COUNTRIES



China	20,167
United States	12,428
Germany	5,074
Korea, Republic of	3,146
Japan	2,637

TOP ORGANIZATIONS

Hangzhou Alibaba Advertising C...	7,793
Amazon.com	6,938
Digital Ocean	2,069
Microsoft Azure	1,757
Tencent cloud computing	960

TOP PRODUCTS

MQTT	48,585
Mosquitto	26,590

New Service: Keep track of what you have connected to the Internet. Check out [Shodan Monitor](#)

[REDACTED] MQTT Connection Code: 0
Added on 2019-09-16 13:05:24 GMT
🇨🇭 Switzerland, Chiasso
Topics:

[REDACTED] MQTT Connection Code: 0
Added on 2019-09-16 13:05:35 GMT
🇦🇪 United Arab Emirates, Dubai
Topics:
\$SYS/broker/version
\$SYS/broker/timestamp
\$SYS/broker/uptime
\$SYS/broker/clients/total
\$SYS/broker/clients/inactive
\$SYS/broker/clients/disconnected
\$SYS/broker/clients/active
\$SYS/broker/clients/connected
\$SYS/broker/clients/expired
\$SYS/broker/clients/maximum
\$S...

[REDACTED] MQTT Connection Code: 5
Added on 2019-09-16 13:04:28 GMT
🇨🇳 China
Topics:

116.002.70.104 [View Raw Data](#)

Country	Germany
Organization	
ISP	
Last Update	2019-09-16T13:00:44.257666
Hostnames	

Vulnerabilities

Note: the device may not be impacted by all of these issues. The vulnerabilities are implied based on the software and version.

CVE-2019-0220	A vulnerability was found in Apache HTTP Server 2.4.0 to 2.4.38. When the path component of a request URL contains multiple consecutive slashes ('/'), directives such as LocationMatch and RewriteRule must account for duplicates in regular expressions while other aspects of the servers processing will implicitly collapse them.
CVE-2017-3169	In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod_ssl may dereference a NULL pointer when third-party modules call ap_hook_process_connection() during an HTTP request to an HTTPS port.
CVE-2017-7679	In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod_mime can read one byte past the end of a buffer when sending a malicious Content-Type response header.

Ports

21	22	80	1883	8086	8888
----	----	----	------	------	------

Services

21	220 (vsFTPD 3.0.3)
tcp	530 Login incorrect.
ftp	530 Please login with USER and PASS.
	211-Features:
	EPRT
	EPSV
	MDTM
	PASV
	REST STREAM
	SIZE
	TVFS
	211 End

22	OpenSSH Version: 7.6p1 Ubuntu-4ubuntu0.3
tcp	SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ubuntu0.3
ssh	Key type: ssh-ed25519

CVE-2019-0220	A vulnerability was found in Apache HTTP Server 2.4.0 to 2.4.38. When the path component of a request URL contains multiple consecutive slashes (/), directives such as LocationMatch and RewriteRule must account for duplicates in regular expressions while other aspects of the servers processing will implicitly collapse them.
CVE-2017-3169	In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod_ssl may dereference a NULL pointer when third-party modules call ap_hook_process_connection() during an HTTP request to an HTTPS port.
CVE-2017-7679	In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod_mime can read one byte past the end of a buffer when sending a malicious Content-Type response header.
CVE-2019-0196	A vulnerability was found in Apache HTTP Server 2.4.17 to 2.4.38. Using fuzzed network input, the http/2 request handling could be made to access freed memory in string comparison when determining the method of a request and thus process the request incorrectly.
CVE-2017-7659	A maliciously constructed HTTP/2 request could cause mod_http2 in Apache HTTP Server 2.4.24, 2.4.25 to dereference a NULL pointer and crash the server process.
CVE-2017-9788	In Apache httpd before 2.2.34 and 2.4.x before 2.4.27, the value placeholder in [Proxy-]Authorization headers of type 'Digest' was not initialized or reset before or between successive key=value assignments by mod_auth_digest. Providing an initial key with no '=' assignment could reflect the stale value of uninitialized pool memory used by the prior request, leading to leakage of potentially confidential information, and a segfault in other cases resulting in denial of service.
CVE-2017-9798	Apache httpd allows remote attackers to read secret data from process memory if the Limit directive can be set in a user's .htaccess file, or if httpd.conf has certain misconfigurations, aka Optionsbleed. This affects the Apache HTTP Server through 2.2.34 and 2.4.x through 2.4.27. The attacker sends an unauthenticated OPTIONS HTTP request when attempting to read secret data. This is a use-after-free issue and thus secret data is not always sent, and the specific data depends on many factors including configuration. Exploitation with .htaccess can be blocked with a patch to the ap_limit_section function in server/core.c.
CVE-2019-0211	In Apache HTTP Server 2.4 releases 2.4.17 to 2.4.38, with MPM event, worker or prefork, code executing in less-privileged child processes or threads (including scripts executed by an in-process scripting interpreter) could execute arbitrary code with the privileges of the parent process (usually root) by manipulating the scoreboard. Non-Unix systems are not affected.
CVE-2017-15710	In Apache httpd 2.0.23 to 2.0.65, 2.2.0 to 2.2.34, and 2.4.0 to 2.4.29, mod_authnz_ldap, if configured with AuthLDAPCharsetConfig, uses the Accept-Language header value to lookup the right charset encoding when verifying the user's credentials. If the header value is not present in the charset conversion table, a fallback mechanism is used to truncate it to a two characters value to allow a quick retry (for example, 'en-US' is truncated to 'en'). A header value of less than two characters forces an out of bound write of one NUL byte to a memory location that is not part of the string. In the worst case, quite unlikely, the process would crash which could be used as a Denial of Service attack. In the more likely case, this memory is already reserved for future use and the issue has no effect at all.
CVE-2018-11763	In Apache HTTP Server 2.4.17 to 2.4.34, by sending continuous, large SETTINGS frames a client can occupy a connection, server thread and CPU time without any connection timeout coming to effect. This affects only HTTP/2 connections. A possible mitigation is to not enable the h2 protocol.
CVE-2018-1283	In Apache httpd 2.4.0 to 2.4.29, when mod_session is configured to forward its session data to CGI applications (SessionEnv on, not the default), a remote user may influence their content by using a "Session" header. This comes from the "HTTP_SESSION" variable name used by mod_session to forward its data to CGIs, since the prefix "HTTP_" is also used by the Apache HTTP Server to pass HTTP header fields, per CGI specifications.
CVE-2017-3167	In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, use of the ap_get_basic_auth_pw() by third-party modules outside of the authentication phase may lead to authentication requirements being bypassed.
CVE-2018-1312	In Apache httpd 2.2.0 to 2.4.29, when generating an HTTP Digest authentication challenge, the nonce sent to prevent reply attacks was not correctly generated using a pseudo-random seed. In a cluster of servers using a common Digest authentication configuration, HTTP requests could be replayed across servers by an attacker without detection.
CVE-2017-7668	The HTTP strict parsing changes added in Apache httpd 2.2.32 and 2.4.24 introduced a bug in token list parsing, which allows ap_find_token() to search past the end of its input string. By maliciously crafting a sequence of request headers, an attacker may be able to cause a segmentation fault, or to force ap_find_token() to return an incorrect value.
CVE-2018-1333	By specially crafting HTTP/2 requests, workers would be allocated 60 seconds longer than necessary, leading to worker exhaustion and a denial of service. Fixed in Apache HTTP Server 2.4.34 (Affected 2.4.18-2.4.30,2.4.33).
CVE-2018-17199	In Apache HTTP Server 2.4 release 2.4.37 and prior, mod_session checks the session expiry time before decoding the session. This causes session expiry time to be ignored for mod_session_cookie sessions since the expiry time is loaded when the session is decoded.
CVE-2019-0197	A vulnerability was found in Apache HTTP Server 2.4.34 to 2.4.38. When HTTP/2 was enabled for a http: host or H2Upgrade was enabled for h2 on a https: host, an Upgrade request from http/1.1 to http/2 that was not the first request on a connection could lead to a misconfiguration and crash. Server that never enabled the h2 protocol or that only enabled it for https: and did not set "H2Upgrade on" are unaffected by this issue.
CVE-2017-15715	In Apache httpd 2.4.0 to 2.4.29, the expression specified in <FilesMatch> could match '\$' to a newline character in a malicious filename, rather than matching only the end of the filename. This could be exploited in environments where uploads of some files are externally blocked, but only by matching the trailing portion of the filename.

New 'unpatchable' iPhone exploit could allow permanent jailbreaking on hundreds of millions of devices

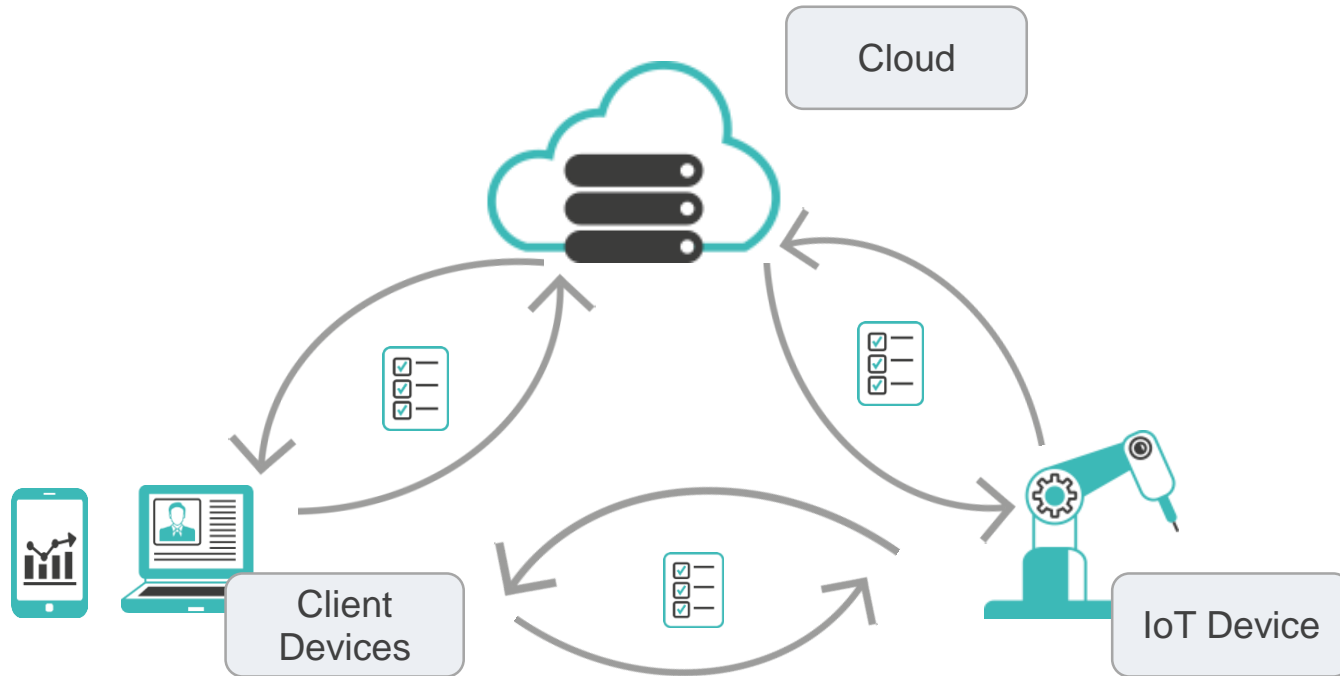
All devices from the iPhone 4S to the iPhone X are impacted

By Chaim Gartenberg | @cgartenberg | Sep 27, 2019, 11:23am EDT



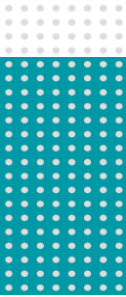
If you take anything away from this, it should be that you are no less safe today from the reveal of Checkm8 than you were yesterday, or the day before, or four years ago. Malware can't exploit it at all, **and if you maintain physical security of your iPhone 5S and newer**, then your passcode —and your data —remains safe.

The big picture



Cryptography

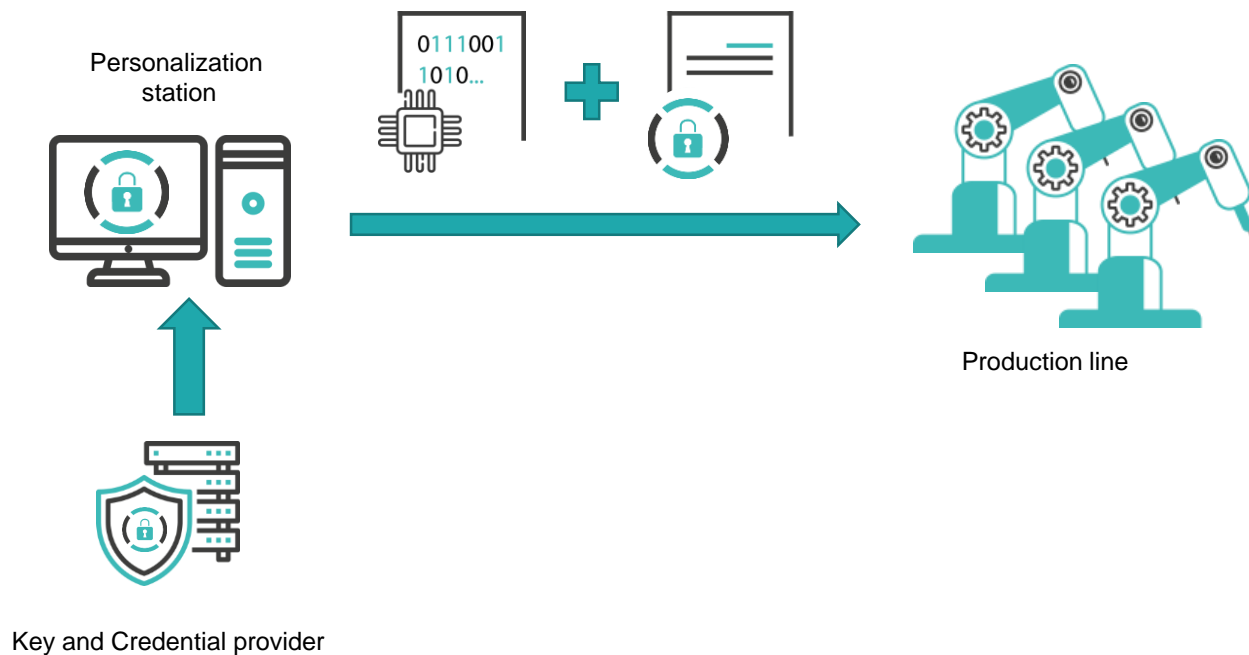
- Secure communications
 - Provides entity authentication, confidentiality and integrity of data
 - Standards protocol exists, but sometimes not well fitting
- Platform security
 - Protection of infrastructure, like enabling authenticated upgrades



Application requirements

- No user interaction
- Metrics:
 1. Cost
 2. Cost
 3. Cost
 4. Execution time
 5. Power consumption
 6. Security

Secure provisioning



Conclusion

- Time-to-market requires reuse
- Threat analysis is a fundamental step
 - Many projects fall in a scenario already formalized
 - Don't reinvent the wheel
- Cryptography is a functional tool for:
 - Secure communication
 - Infrastructure security

We are
hiring!



+ Stage &
Thesis

Brings strong Security to your IoT system

Need more details? We would love to get in touch!

hello@securitypattern.com