



SVEUČILIŠTE U ZAGREBU



Fakultet
elektrotehnike i
računarstva

Diplomski studij

Sigurnost komunikacija

Ak. godina 2023/2024

Sigurnost u Internetu stvari



Creative Commons



- **slobodno smijete:**

- **dijeliti** — umnožavati, distribuirati i javnosti priopćavati djelo
- **remiksirati** — prerađivati djelo



- **pod sljedećim uvjetima:**

- **imenovanje.** Morate priznati i označiti autorstvo djela na način kako je specificirao autor ili davatelj licence (ali ne način koji bi sugerirao da Vi ili Vaše korištenje njegova djela imate njegovu izravnu podršku).
- **nekomercijalno.** Ovo djelo ne smijete koristiti u komercijalne svrhe.
- **dijeli pod istim uvjetima.** Ako ovo djelo izmijenite, preoblikujete ili stvarate koristeći ga, prerađu možete distribuirati samo pod licencom koja je ista ili slična ovoj.



U slučaju daljnjeg korištenja ili distribuiranja morate drugima jasno dati do znanja licencne uvjete ovog djela. Najbolji način da to učinite je linkom na ovu internetsku stranicu. Od svakog od gornjih uvjeta moguće je odstupiti, ako dobijete dopuštenje nositelja autorskog prava. Ništa u ovoj licenci ne narušava ili ograničava autorova moralna prava.

Tekst licencije preuzet je s <http://creativecommons.org/>.

Zanimljivosti...

- MIRAI botnet – kraj 2016.
 - ◆ Zloćudni kôd koji cilja uređaje IoT (tipično kamere)
 - ◆ telnet/web – lista *default* imena i lozinki -> *bruteforce* -> zaraza
 - ◆ “2016 Dyn cyberattack”
 - ◆ <https://github.com/jgamblin/Mirai-Source-Code>
- Automobili
 - ◆ Jeep 2015 - pristup CAN-u kroz *firmware update*
 - ◆ Provaljivanje alarmnih sustava - Calamp i Viper SmartStart
 - ◆ Stealing a Tesla in seconds:
<https://www.youtube.com/watch?v=aVIYuPzmJoY>
 - ◆ Puno novijih primjera – CAN hacking:
 - ◆ <https://medium.com/@yogeshojha/car-hacking-101-practical-guide-to-exploiting-can-bus-using-instrument-cluster-simulator-part-i-cd88d3eb4a53>

Zanimljivosti...

- Medicinski uređaji
 - Pacemaker – sučelje za provjeru stanja
 - ◆ Medtronic – ažuriranja nisu digitalno potpisana
 - ◆ Moguće mijenjati otkucaje srca, pokrenuti defibrilator
 - ◆ Inzulinske pumpe – Medtronic
 - ◆ Utjecati na doze inzulina korištenjem uređaja SDR
 - ◆ <https://www.csoonline.com/article/566025/hacking-pacemakers-insulin-pumps-and-patients-vital-signs-in-real-time.html>
- Brodovi
 - Ranjivosti u opremi Moxa – manipuliranje firmwareom koji se koristi za IP-serijsku pretvorbu
 - Upadi putem phishinga, nesigurnog WiFi-a, USB stickova....
 - NMEA 0183/2000 – poznate ranjivosti i manipuliranje porukama
 - <https://pdfs.semanticscholar.org/635e/5df799b87fc7d8f0d3a2f8cb3a7d454bb23d.pdf>
 - Balastni tankovi i kontrola pumpi - <https://threatpost.com/hacker-capsize-ship-sea/142077/>

Još zanimljivosti...

- Smart Locks Used by Airbnb Get Bricked by Software Update
 - <https://gizmodo.com/smart-locks-used-by-airbnb-get-bricked-by-software-upda-1797839523>
- Sustavi SCADA (*Supervisory Control and Data Acquisition*) / ICS
 - ◆ Industrija 4.0, elektrane... - automatizacija –
 - ◆ Sve više uređaja IoT -> Industrial IoT (IIoT)
 - ◆ *December 2015 Ukraine power grid cyberattack*
 - ◆ Energetski sektori – SAD, UK
 - ◆ Finska – sustavi grijanja

I još zanimljivosti...

- Stuxnet
 - Crv dizajniran za napad na sustave SCADA
 - Konkretnije, za iranski nuklearni program
 - Nakon ulaska u mrežu tražio je specifični Siemensov PLC
 - Odnosno radnu stanicu koja konfigurira taj PLC
 - Nakon pronalaska, mijenja konfiguraciju vrtnje centrifuga tako da ih ošteti
 - Cijena izrade Stuxneta?
 - *An Unprecedented Look at Stuxnet, the World's First Digital Weapon*
 - <https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/>
 - Dokumentarni film Zero Days:
 - <https://www.imdb.com/title/tt5446858/>

Problemi sigurnosti i privatnosti u IoT

- Uzroci loše sigurnosti u IoT (vrijede i općenito)
 - Fokus je na funkcionalnosti uređaja / sustava
 - Fokus je na sučeljima prema korisnicima
 - (a ne prema drugim uređajima ili oblaku)
 - Pokušava se skratiti vrijeme razvoja kako bi proizvodi čim prije izašli na tržište (konkurencija)
- Što je s podacima korisnika?
 - Uređaji IoT ih prikupljaju
 - Prenose se u "oblak" i obrađuju
 - Curenje podataka?

Složaj tehnologija u IoT...

- Napadači “poznaju” tehnologije i imaju alate
 - Automatizirani alati za napad na pojedine slojeve / tehnologije
 - Poznate ranjivosti za većinu slojeva u složaju
- Razvijatelji nisu sigurnosni stručnjaci
 - Ne postoje specifična gotova rješenja / alati
 - Ne postoje metodologije implementacije sigurnosti
 - Kao npr. za web
- Što se događa?
 - Razvijatelji razviju komponente i integriraju ih u sustav
 - Ostaje velika “površina napada” preko cijelog složaja
 - Iskusnim napadačima nije problem pronaći i iskoristiti ranjivost



OWASP

- *Open Web Application Security Project*
- Top 10
 - ◆ Web, mobilne aplikacije, IoT



- Smjernice za razvoj sigurnih aplikacija/usluga
 - ◆ i testiranje nesigurnih aplikacija/usluga
- Alati – npr. ZAP
- *Application Security Verification Standard (OWASP ASVS)*
 - ◆ “kuharica” za izradu sigurnih (web) aplikacija
 - ◆ Donekle primjenjivo i na ostale domene!

OWASP Top 10 IoT – 2014

- I1 Nesigurna sučelja weba** (*Insecure Web Interface*)
- I2 Nedovoljna autentifikacija / autorizacija** (*Insufficient Authentication/Authorization*)
- I3 Nesigurne mrežne usluge** (*Insecure Network Services*)
- I4 Nedostatak šifriranja u transportu** (*Lack of Transport Encryption*)
- I5 Privatnost** (*Privacy Concerns*)
- I6 Nesigurna sučelja u oblaku** (*Insecure Cloud Interface*)
- I7 Nesigurna mobilna sučelja** (*Insecure Mobile Interface*)
- I8 Konfiguracija sigurnosnih postavki** (*Insufficient Security Configurability*)
- I9 Nesigurni software/firmware** (*Insecure Software/Firmware*)
- I10 Loša fizička sigurnost** (*Poor Physical Security*)

OWASP Top 10 IoT 2018

- I1 Loše lozinke** - *Weak Guessable, or Hardcoded Passwords*
- I2 Nesigurne mrežne usluge** - *Insecure Network Services*
- I3 Nesigurna sučelja** - *Insecure Ecosystem Interfaces*
- I4 Nesigurni mehanizmi nadogradnji** - *Lack of Secure Update Mechanism*
- I5 Zastarjele komponente** - *Use of Insecure or Outdated Components*
- I6 Loša privatnost** - *Insufficient Privacy Protection*
- I7 Nedovoljno šifriranje** - *Insecure Data Transfer and Storage*
- I8 Nedostatak upravljanja** - *Lack of Device Management*
- I9 Loše početne postavke** - *Insecure Default Settings*
- I10 Fizička sigurnost** - *Lack of Physical Hardening*

OWASP IoT Top 10 2014

I1 Insecure Web Interface

I2 Insufficient Authentication/Authorization

I3 Insecure Network Services

I4 Lack of Transport Encryption/Integrity Verification

I5 Privacy Concerns

I6 Insecure Cloud Interface

I7 Insecure Mobile Interface

I8 Insufficient Security Configurability

I9 Insecure Software/Firmware

I10 Poor Physical Security

OWASP IoT Top 10 2018 Mapping

I3 Insecure Ecosystem Interfaces

I1 Weak, Guessable, or Hardcoded Passwords

I3 Insecure Ecosystem Interfaces

I9 Insecure Default Settings

I2 Insecure Network Services

I7 Insecure Data Transfer and Storage

I6 Insufficient Privacy Protection

I3 Insecure Ecosystem Interfaces

I3 Insecure Ecosystem Interfaces

I9 Insecure Default Settings

I4 Lack of Secure Update Mechanism

I5 Use of Insecure or Outdated Components

I10 Lack of Physical Hardening

[https://www.owasp.org/index.php/OWASP Internet of Things Project#tab=OWASP IoT Top 10 2018 Mapping Project](https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project#tab=OWASP_IoT_Top_10_2018_Mapping_Project)

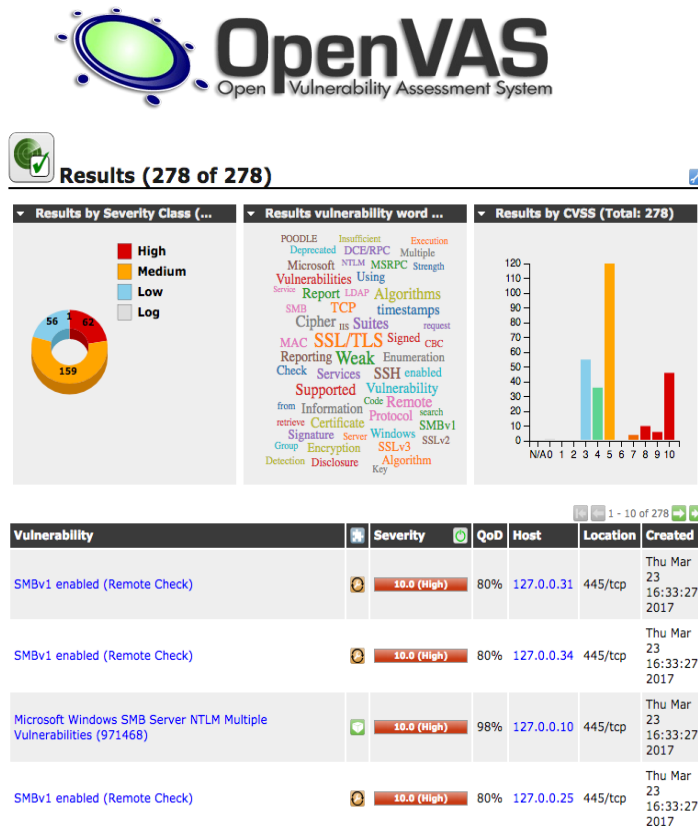
I1 *Weak Guessable, or Hardcoded Passwords*

- Korištenje jednostavnih lozinki
- Statičke lozinke ili tokeni (posebno kod “manjih” uređaja)
- Korištenje slabih i predvidljivih tokena / identifikatora sjednica?
- Osnovne provjere:
 - ◆ Mogu li postaviti jednostavnu lozinku (npr. qwerty)?
 - ◆ Ističe li sjednica nakon nekog vremena?
 - ◆ Mogu li promijeniti default ime i lozinku?
 - ◆ Hoće li me aplikacija “zaključati” nakon n pogrešnih lozinki?
 - ◆ *Mogu li nekako doći do podataka korisnika (Zaboravljena lozinka?)*
 - ◆ Penetracijsko testiranje sučelja “izvana”
 - ◆ a poželjno i kao registrirani korisnik

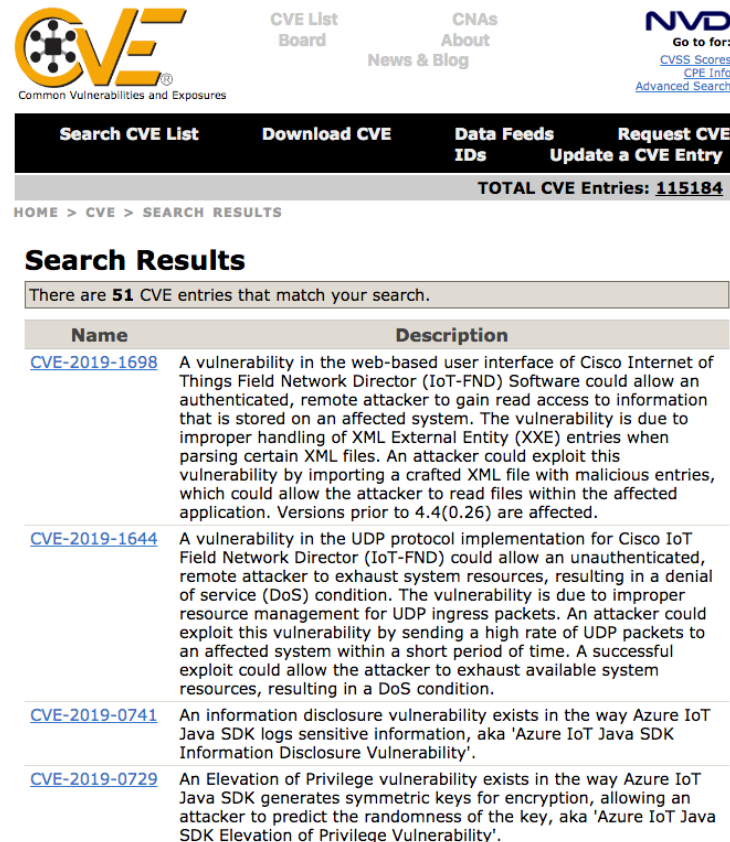
I2 *Insecure Network Services*

- Uz osnovne usluge nužne za funkcioniranje uređaja IoT često su pokrenuti različiti servisi
 - ◆ Jesu li svi servisi doista potrebni?
 - ◆ Ako jesu, je li verzija / implementacija sigurna (CVE liste)?
 - ◆ Jesu li adekvatno zaštićeni (npr. I3)?
- Osnovne provjere:
 - ◆ Skeniranje portova kako bi se utvrdilo što je sve pokretnuto (nmap)
 - ◆ Provjera ranjivosti otvorenih servisa (npr. Nessus, OpenVAS)
 - ◆ *Fuzzing, buffer overflow* -> tipičan cilj: DoS
 - ◆ Posebno paziti na UPnP portove (Universal Plug&Play)

Alati za skeniranje i lista ranjivosti



<http://openvas.org/>



<https://cve.mitre.org/>

I3 *Insecure Ecosystem Interfaces*

- Objedinjene 3 top ranjivosti iz 2014:
 - IoT uređaji tipično komuniciraju s poslužiteljem – nesigurna sučelja weba (ex. I1)
 - Zapravo OWASP web top 10 (prethodno predavanje)
 - Možemo li provaliti sučelje na poslužitelju i doći do podataka s uređaja?
 - Usluge često imaju mobilne aplikacije za pregled podataka i upravljanje uređajima (npr. kamere) (ex .I7)
 - Vrlo slično OWASP top 10 mobilnih ranjivosti (prethodno predavanje)
 - Možemo li preko aplikacije ii sučelja za aplikaciju na uređaju preuzeti kontrolu?
 - Tipično uređaje IoT kontroliramo / agregiramo podatke putem sučelja u oblaku (ex. I6)
 - Ponovno, vrlo slično ex. I1 – poslužitelji weba i njihova sučelja

14 *Lack of Secure Update Mechanism*

- Ažuriranje programske podrške (firmwarea) je uvijek nužno
 - ◆ Pronađene ranjivosti -> zakrpe (npr. napadači - kdiff!)
 - ◆ Lojox malware?
- Problem može biti i “nesigurno” ažuriranje
 - ◆ Autentifikacija poslužitelja - automatizirano ažuriranje sa preuzetog “*update servera*”
 - ◆ NotPetya – Ukrajina, brave s Airbnb...
 - ◆ Prijenos ažuriranja mora biti šifriran a ažuriranje potpisamo
 - ◆ Ažurirani software/firmware ne smije sadržavati “hardkodirane” autentifikacijske podatke! (npr. kako do ključeva iz hardware-a?)
 - ◆ Kako ažurirati ključeve na uređajima IoT?
- Osnovne provjere:
 - ◆ Može li se software/firmware uređaja uopće ažurirati?
 - ◆ Kako se prenose povjerljivi elementi?
 - ◆ Kakvi su mrežni uvjeti?

15 *Use of Insecure or Outdated Components*

- Korištenje zastarjelih ili nesigurnih komponenti
 - Programske knjižnice, radni okviri...
 - Nesigurna dorada funkcija operacijskog sustava
 - Nesigurno sklopovlje?
- Osnovne provjere:
 - ◆ Pobrojati što se sve koristi
 - ◆ Provjeriti je li sve ažurirano
 - ◆ Sličan princip kao i kod ranjivosti weba...

I6 *Insufficient Privacy Protection*

- Uređaji IoT mogu skupljati osobne podatke
 - ◆ Kamere, mikrofoni, medicinski podaci...
- Problem: kompromitacija takvih podataka koje napadači tipično koriste za daljnje napade
 - ◆ *Phishing, spear-phishing*, ucjene, lažno predstavljanje...
- Osnovne provjere
 - ◆ Kakve sve podatke uređaj IoT skuplja (i je li to nužno)?
 - ◆ Što se radi s tim podacima - gdje se i kako obrađuju/šalju?
 - ◆ Jesu li anonimizirani u nekoj mjeri?
 - ◆ Domena GDPR-a
 - ◆ Posljedica zapravo svih ranjivosti I1-I10
- ◆ Npr. Amazon Echo – "prisluškivanje" za poboljšanje usluge?
- ◆ Npr. Web kamere – je li stream šifriran i kako?

17 *Insecure Data Transfer and Storage*

- Česta ranjivost općenito, donekle smanjena posljednjih godina
- Nepostojanje šifriranja prometa na transportnom sloju
 - ◆ Sva komunikacija je lako čitljiva metodama "sniffanja" (npr. Wireshark)
- ◆ Nepostojanje šifriranja podataka "u mirovanju" – novost!
- Potrebno je **ispravno** koristiti infrastrukturu PKI, ključeve i mehanizme
- Osnovne provjere:
 - ◆ Analiza prometa kako bi se utvrdilo je li dio ili sav promet šifriran
 - ◆ Ako se koristi TLS provjeriti da se koristi ispravno
 - ◆ Dosta postojećih problema s neispravnim korištenjem (npr. SSLstrip)
 - ◆ Provjera korištenih algoritama i ključeva – jesu li zastarjeli?
 - ◆ Nove preporuke svakih nekoliko godina
- ◆ ESP32 npr.: <https://hackaday.com/2017/06/20/practical-iot-cryptography-on-the-espressif-esp8266/>
- ◆ Koliko šifriranje opterećuje sam uređaj i njegovu osnovnu namjenu?

I8 *Lack of Device Management*

- Upravljanje i nadzor IoT uređaja
- Znamo li gdje su, u kojem su stanju, rade li ispravno, rade li uopće...
- Problem sa zamjenom / isključivanjem uređaja?
 - Npr. *smart dust* problem
- Problem “*rogue node*” – kako detektirati lažni uređaj?
- Kao *Logging and monitoring* kod web aplikacija
- Potrebno je pokriti čitav životni ciklus uređaja
 - Uključujući isključivanje i zamjenu

19 *Insecure Default Settings*

- Tko je kriv za MIRAI botnet? (korišteni su *default* računi!)
- Može li se mijenjati sigurnosne postavke uređaja?
 - ◆ Mora li ih se mijenjati? (MIRAI!)
 - ◆ Što ako postane **prekompleksno** – korisnici očekuju PnP! (loše)
- Osnovne provjere:
 - ◆ Ako već proizvođač ne forsira jake lozinke, mogu li ih sam forsirati na administratorskom sučelju?
 - ◆ Ima li mogućnosti povećavanja sigurnosti putem sučelja:
 - ◆ Logiranje svih akcija u sustavu (bitno za napade iznutra!)
 - ◆ Upozorenja u slučaju incidenata (mail, SMS, alarm)?
 - ◆ Definiranje korisničkih uloga



- https://www.owasp.org/index.php/Top_10_2014-l8_Insufficient_Security_Configurability

I10 *Lack of Physical Hardening*

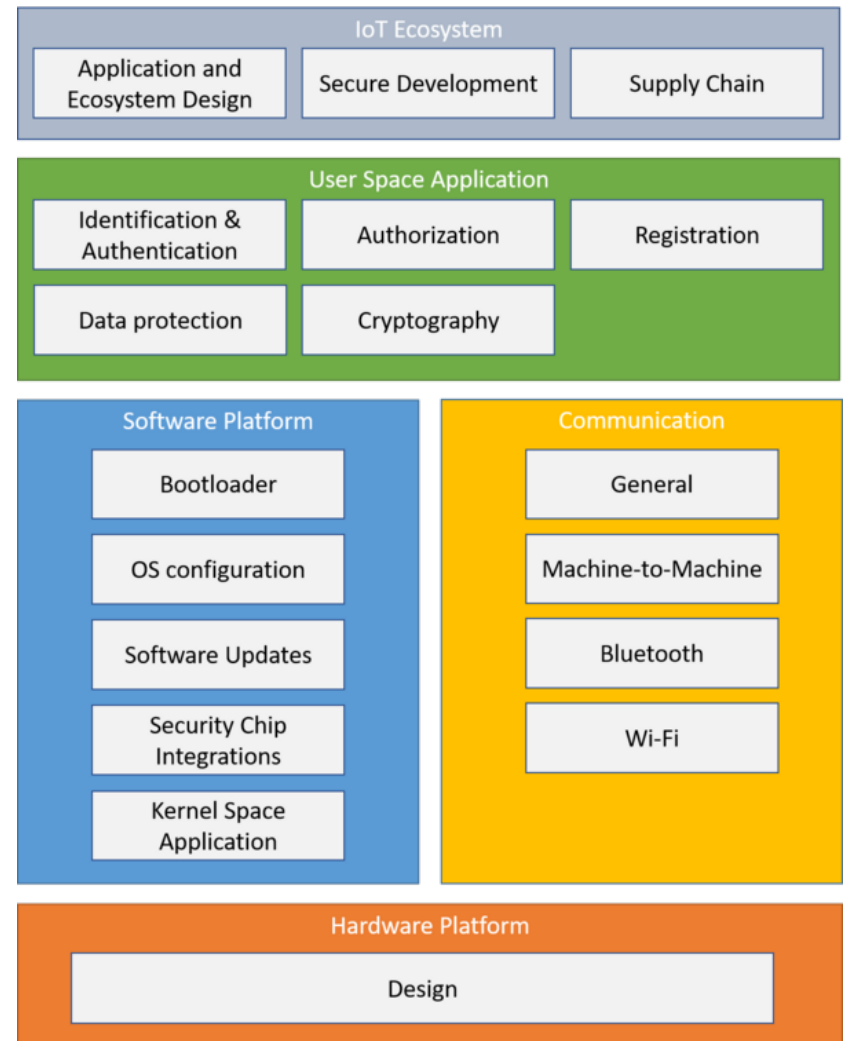
- Što napadač može napraviti ako ima fizički pristup uređaju?
 - ◆ Kako do ključeva/lozinki iz sklopovlja? (prošli slide)
 - ◆ Pristup podacima (npr. očitavanja) pohranjenim na mem. Kartici
 - ◆ Pristup USB i sličnim priključcima (npr. PoisonTap)?
- Osnovne provjere:
 - ◆ Mogu li jednostavno "otvoriti" uređaj? Postoji li detekcija?
 - ◆ Mogu li se spojiti na ulaze (npr. USB) namijenjene konfiguraciji uređaja?
 - ◆ Mogu li programski onemogućiti lokalno spajanje na uređaj?
 - ◆ Jesu li pohranjeni podaci šifrirani?
- https://www.owasp.org/index.php/Top_10_2014-I10_Poor_Physical_Security

Kako se štititi?

- Za razvijatelje:
 - IoT Security Verification Standard
 - Sličan concept kao ASVS za web
 - “Kuharica” sa sigurnosnim zahtjevima za nove aplikacije i sustave
 - “Kuharica” sa smjernicama za verifikaciju postojećih aplikacija i sustava
 - Još u razvoju!
 - <https://github.com/OWASP/IoT-Security-Verification-Standard-ISVS>
- Za pen-testere
 - OWASP IoT Security Testing Guide
 - <https://owasp.org/owasp-istg/index.html>

IoT Security Verification Standard – grupe zahtjeva i razine sigurnosti

- 5 grupa zahtjeva
 - Hardware
 - Software
 - Komunikacija
 - Korisničke aplikacije
 - IoT ekosustav
- Razine sigurnosti
 - Različiti zahtjevi!
 - Level 1 (najniža)
 - Level 2
 - Level 3 (najviša)



IoT Security Verification Standard – sigurnosne razine

- Najniža razina (Level 1)
 - Uređaji koji ne čuvaju podatke korisnika, do kojih nije moguće ostvariti fizički pristup i kod kojih kompromitacija jednog uređaja neće omogućiti napadaču kompromitaciju drugih uređaja. Fokus na softwareske ranjivosti!
 - Npr. Pametna žarulja
- Srednja razina (Level 2, uključuje razinu 1)
 - Fokus i na hardverske ranjivosti, kompromitacija uređaja može ugroziti korisnika ili druge uređaje
 - npr. Pametna brava
- Visoka razina (Level 3, uključuje razine 1 i 2)
 - Uređaji kod kojih je potrebno osigurati obranu u dubinu na razini softwarea i hardwarea (anti-tampering).
 - Npr. vozila, medicinski uređaji, industrijski IoT, brodovi...

Primjer – V4: Communication Requirements

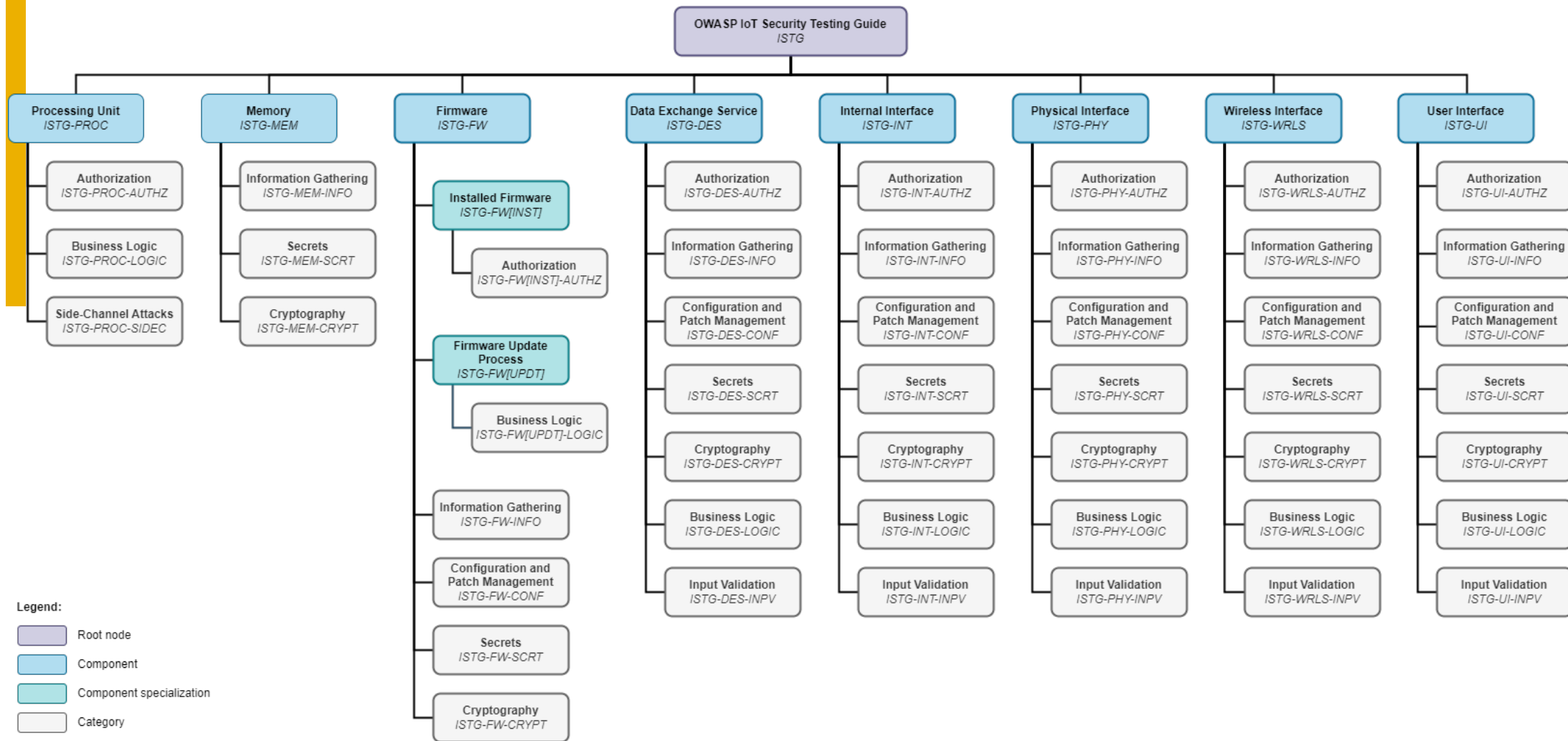
General

#	Description	L1	L2	L3
4.1.1	Verify that communication with other components in the IoT ecosystem (including sensors, gateway and supporting cloud) occurs over a secure channel in which the confidentiality and integrity of data is guaranteed and in which protection against replay attacks is built into the communication protocol.	✓	✓	✓
4.1.2	Verify, using up-to-date TLS testing tools, that only strong cipher suites are enabled, with the strongest cipher suite set as preferred.	✓	✓	✓
4.1.3	Verify that in case TLS is used, the device cryptographically verifies the X.509 certificate.	✓	✓	✓
4.1.4	Verify that either protection or detection of jamming is provided for availability-critical applications.		✓	✓
4.1.6	Verify that the device's TLS implementation uses its own certificate store, pins to the endpoint's certificate or public key, and disallows connections to endpoints with different certificates or keys, even if signed by a trusted CA.		✓	✓
4.1.7	Verify that inter-chip communication is encrypted (e.g. main board to daughter board communication).			✓

Machine-to-Machine

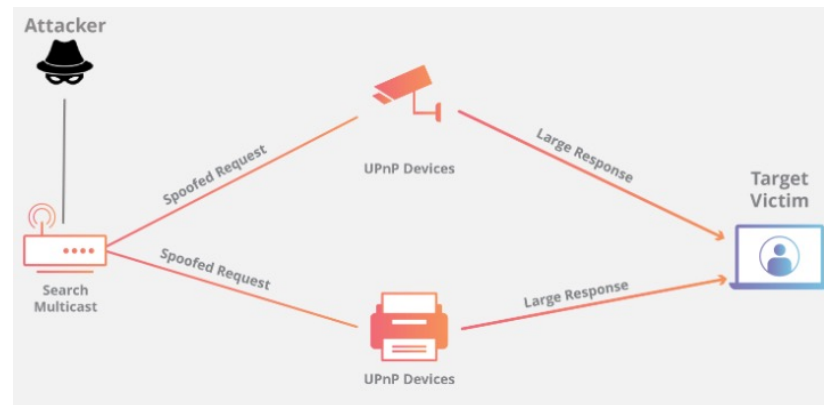
#	Description	L1	L2	L3
4.2.1	Verify that unencrypted communication is limited to data and instructions that are not of a sensitive nature.	✓	✓	✓
4.2.2	Verify that MQTT brokers only allow authorized IoT devices to subscribe to topics and publish messages.	✓	✓	✓
4.2.3	Verify that certificates are favored over native username and passwords to authenticate MQTT transactions.	✓	✓	✓

OWASP IoT Security Testing Guide - komponente



Uređaji IoT kao sredstvo za DDoS? – npr. SSDP DDoS

- "amplification" napad
- UPnP (*Universal Plug'n'Play*) uređaji (PS4, Smart TV, kamere...)
 - Koriste SSDP (Simple Service Discovery Protocol) za objavu slanjem paketa na multicast adresu – koriste UDP!
 - Nakon objave računala ih mogu zatražiti karakteristike / usluge -> pojačanje!



<https://www.cloudflare.com/learning/ddos/ssdp-ddos-attack/>

- Napadač lažira IP adresu žrtve i zatraži karakteristike od velikog broja UPnP uređaja...

Još neki korisni resursi...

- Smjernice GSMA IoT Security
 - ◆ 85 preporuka za siguran dizajn IoT sustava, uređaja...
 - ◆ Ranjivosti, modeli napada i procjena rizika za svaki slučaj
 - ◆ <https://www.gsma.com/iot/iot-security/iot-security-guidelines/>
- SHODAN (<https://www.shodan.io/>)
 - ◆ Google za IoT uređaje
 - ◆ Pretraga uređaja
 - ◆ Pretraga pronađenih ranjivosti
 - ◆ Koristiti kao prvi korak napada (*probe*)?


SHODAN

[Exploits](#)[Maps](#)[Share Search](#)[Download Results](#)[Create Report](#)

TOTAL RESULTS

25

TOP COUNTRIES



Croatia25

TOP CITIES


Zagreb	16
Karlovac	3
Dubrovnik	2

TOP SERVICES

2002	7
Telnet	7
HTTPS	5
264	3
HTTP	1

TOP ORGANIZATIONS


VIPnet d.o.o.	11
Croatian Academic and Research ...	8
T-Mobile Croatia	2
Metronet telekomunikacije d.d.	2
POS LuH d.o.o, za informatičke usl...	1

193.198.162.131
Croatian Academic and Research Network
Added on 2019-04-13 13:14:39 GMT
 Croatia, Zagreb



Studentski centar u Zagrebu
University of Zagreb

Studom
Stjepan Radic
Zagreb, Croatia

Authorized access only !!!

193.198.162.139
Croatian Academic and Research Network
Added on 2019-04-16 20:16:06 GMT
 Croatia, Zagreb

|-----|
|
| Studenski centar
| Sveucilišta u Zagrebu
| ...
|

83.139.115.146 
dh115-146.xnet.hr
VIPnet d.o.o.
Added on 2019-04-17 01:18:41 GMT
 Croatia, Zagreb

HTTP/1.1 200 OK
Date: Wed, 17 Apr 2019 01:18:41 GMT
Server: Apache
Last-Modified: Mon, 02 Sep 2013 12:31:25 GMT
ETag: "90dd04-249-c025c140"
Accept-Ranges: bytes
Content-Length: 585
Content-Type: text/html

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/...

Za one koji žele znati više

- <https://www.iotforall.com/5-worst-iot-hacking-vulnerabilities/>
- https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project#tab=Main
- <https://www.gsma.com/iot/iot-security/iot-security-guidelines/>
- <https://www.shodan.io>