Internet stvari

SVEUČILIŠTE U ZAGREBU
Fakultet elektrotehnike i računarstva

Diplomski studij
Računarstvo
Znanost o mrežama
Programsko inženjerstvo i informacijski sustavi
Računalno inženjerstvo
Informacijska i komunikacijska tehnologija
Automatika i robotika
Informacijsko i komunikacijsko inženjerstvo
Elektrotehnika i informacijska tehnologija
Audiotehnologije i elektroakustika
Elektroenergetika
(Izborni predmet profila)

7. Sigurnosni aspekti, upravljanje uređajima

Ak. god. 2022./2023.

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
- Medicinski uređaji - primjer St. Jude’s
  - Pacemaker – sučelje za provjeru stanja
  - Moguće mijenjati otkucaje srca i isprazniti bateriju…
- 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=aVlYuPzmJoY

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)
  - Stuxnet – crv koji je napadao Siemens PLC-ove
    - iranska nuklearna postrojenja
  - December 2015 Ukraine power grid cyberattack
  - Energetski sektori – SAD, UK
  - Finska – sustavi grijanja

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
  - 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 gotova rješenja / alati
  - Ne postoje metodologije impl. sigurnosti
- 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	OWASP IoT Top 10 2018 Mapping
I1 Insecure Web Interface	I3 Insecure Ecosystem Interfaces
I2 Insufficient Authentication/Authorization	I1 Weak, Guessable, or Hardcoded Passwords I3 Insecure Ecosystem Interfaces I9 Insecure Default Settings
I3 Insecure Network Services	I2 Insecure Network Services
I4 Lack of Transport Encryption/Integrity Verification	I7 Insecure Data Transfer and Storage
I5 Privacy Concerns	I6 Insufficient Privacy Protection
I6 Insecure Cloud Interface	I3 Insecure Ecosystem Interfaces
I7 Insecure Mobile Interface	I3 Insecure Ecosystem Interfaces
I8 Insufficient Security Configurability	I9 Insecure Default Settings
I9 Insecure Software/Firmware	I4 Lack of Secure Update Mechanism I5 Use of Insecure or Outdated Components
I10 Poor Physical Security	I10 Lack of Physical Hardening

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

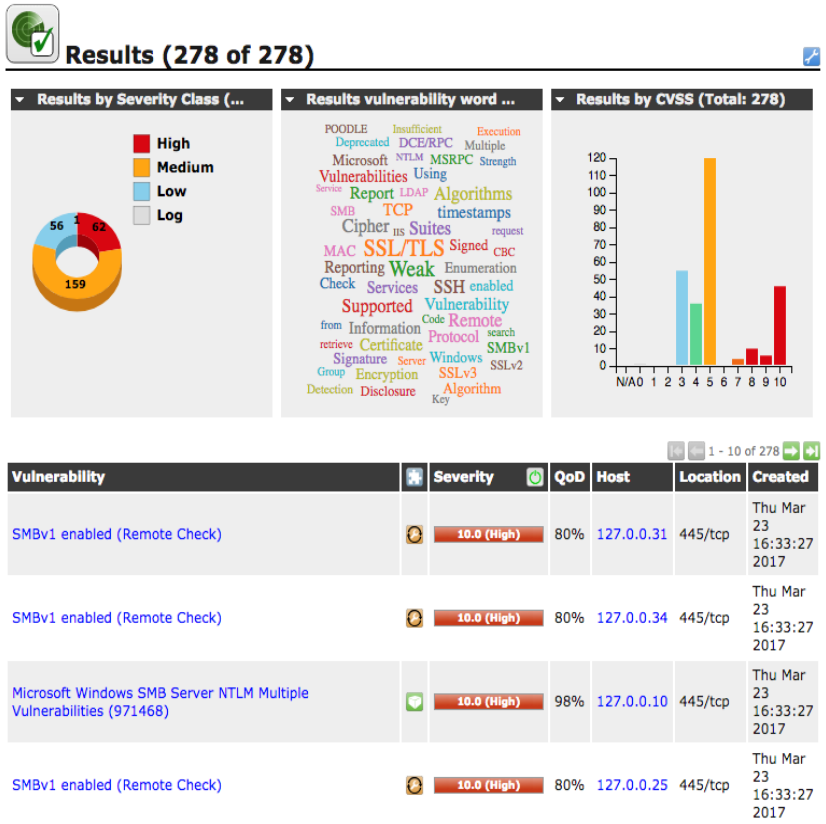
I2 Insecure Network Services

- 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)?

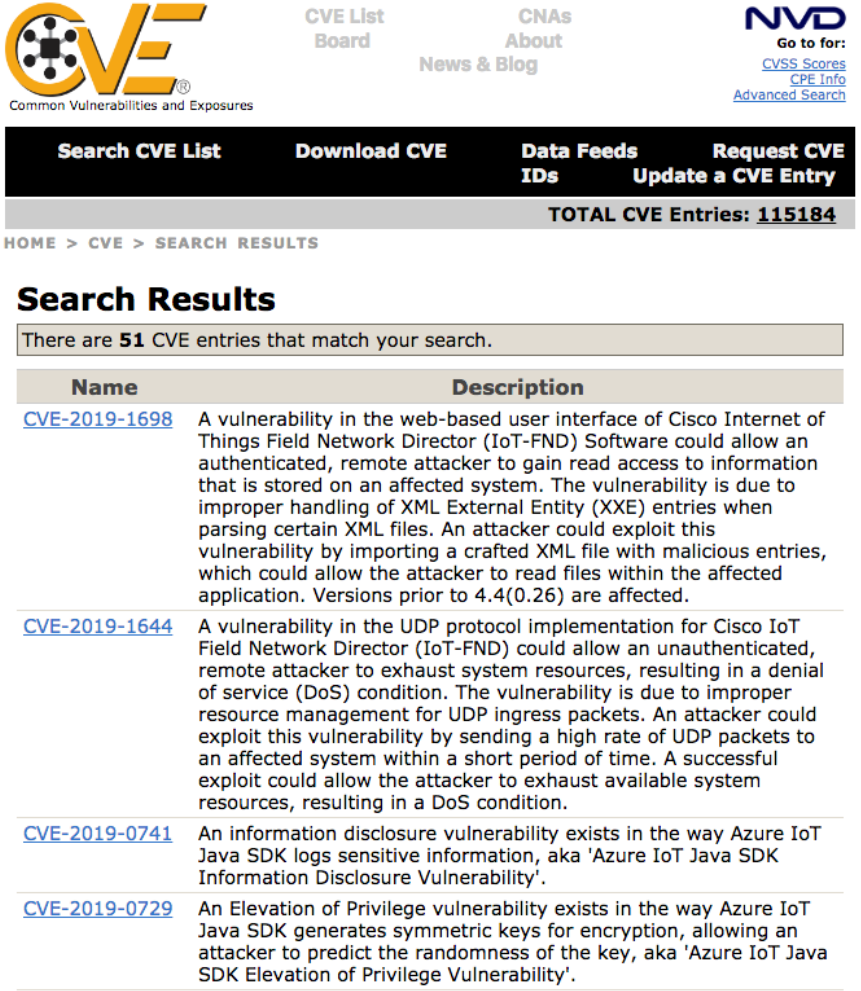
- Osnovne provjere:
  - Skeniranje *portova* kako bi se utvrdilo što je sve pokrenuto (nmap)
  - Provjera ranjivosti otvorenih servisa (npr. Nessus, OpenVAS)
    - Fuzzing, buffer overflow → tipičan cilj: DoS
  - Posebno paziti na UPnP portove (Universal Plug&Play)

Alati za skeniranje i lista ranjivosti

OpenVAS
Open Vulnerability Assessment System



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

I4 Lack of Secure Update Mechanism

- Ažuriranje programske podrške je uvijek nužno
  - Pronađene ranjivosti → zakrpe (npr. napadači - diff!)
- Problem može biti i "nesigurno" ažuriranje
  - Autentifikacija poslužitelja - automatizirano ažuriranje sa preuzetog "update servera"
    - NotPetya – Ukrajina, brave s Airbnb…
  - Prijenos ažuriranja mora biti šifriran
  - Ažurirani software/firmware ne smije sadržavati "hardkodirane" autentifikacijske podatke! (npr. kako do ključeva iz hardvera?)

- Osnovne provjere:
  - Može li se software/firmware uređaja uopće ažurirati?

I5 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?

I7 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
- ESP8266 npr.: https://hackaday.com/2017/06/20/practical-iot-cryptography-on-the-espressif-esp8266/

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

I9 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-I8_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. očitanja) pohranjenim na memorijskoj kartici
  - Pristup USB-u 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

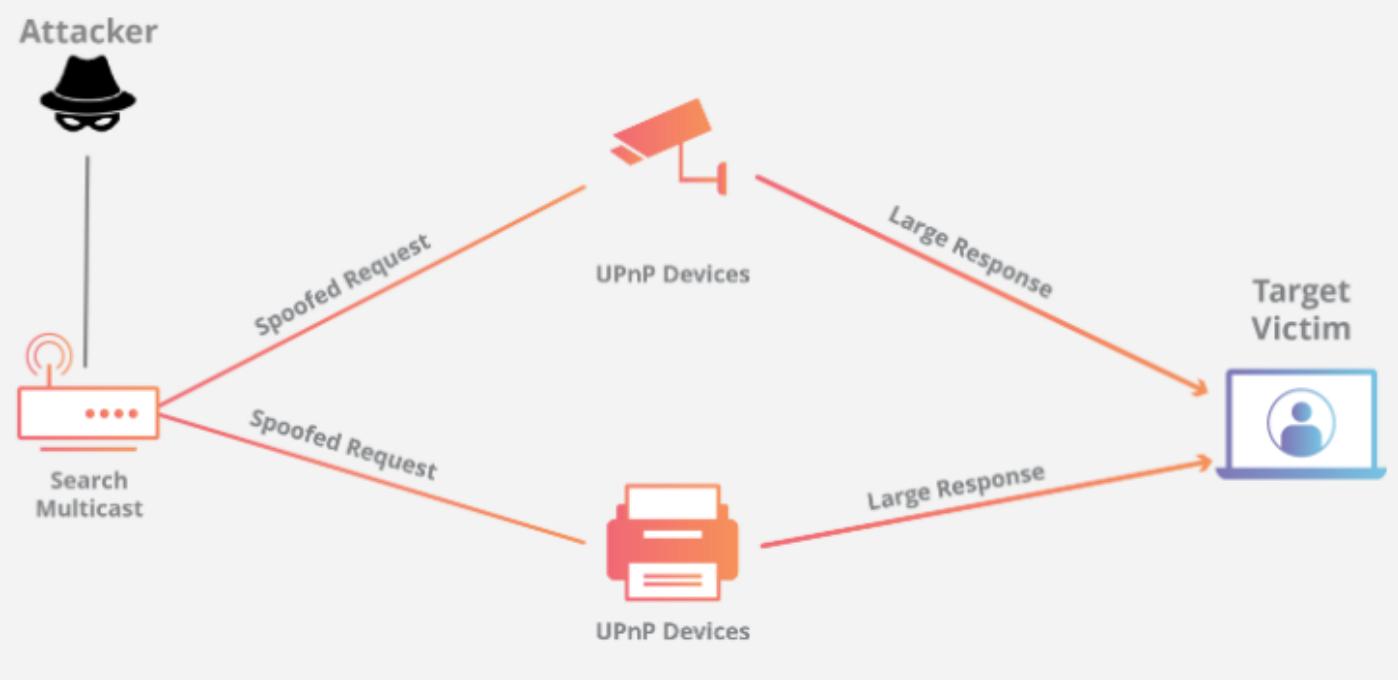
Kako se štititi?

- Shvatiti zašto postoje ranjivosti (…)
- Za svaku ranjivost OWASP ima preporuke (poveznice)
- Smjernice za razvijatelje
  - Kako razvijati, što omogućiti, na što paziti?
- Smjernice za korisnike
  - Kako osigurati uređaj / sustav?
  - *Default* je uobičajeno jednostavan i nesiguran!
  - Tko je kriv u slučaju zlouporaba?

- Sigurnost je složena i traži puno znanja na svim “slojevima”
  - Jedna ranjivost može kompromitirati cijeli sustav!

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



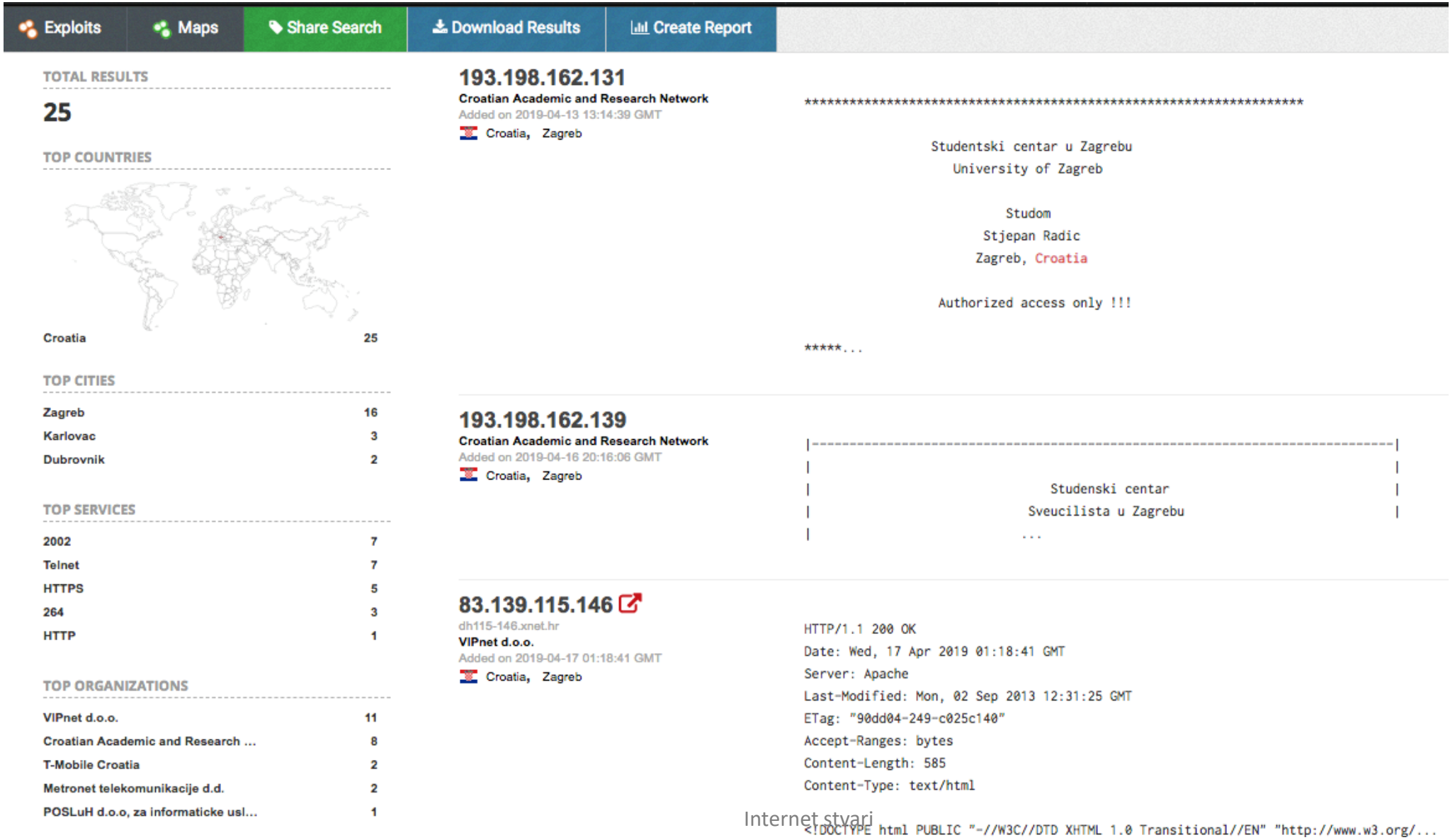
https://www.cloudflare.com/learning/ddos/ssdp-ddos-attack/

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
Croatia 25
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
POSLuH d.o.o, za informaticke 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
Sveucilista 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