Mobile Device Security

Summer Academy in Cyber Security and Privacy 2021

$ whoami

Arti Karahoda

Cyber & Information Security Manager @
Raiffeisen Bank International AG

Researcher for Data Privacy @
Sense Cyber Research Center

- Network & Mobile Security
- Digital Forensics
- Exploit Development & Automation
- Cyber Threat Intelligence

https://artikrh.sh

Content

Mobile Device Security

IN THIS PRESENTATION:

Security approach towards phone devices

Threat landscape in mobile market

Real life scenarios on spyware

Feel free to interrupt at any given time, otherwise you can also write down your questions in the meanwhile so we can discuss them at the end – Q&A Session

So, what exactly is mobile security?

Protection of mobile devices such as smartphones and tablets

1 Security Layers

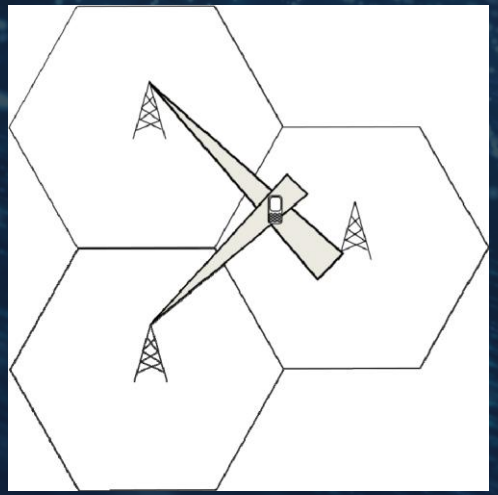
- How can we protect our devices?
- What are today's available methods in terms of security?

Device Security

- Screen locks
  - Password
  - Passcode
  - Pattern
  - Biometric Authentication
    - Fingerprints
    - Facial recognition
    - Voice recognition

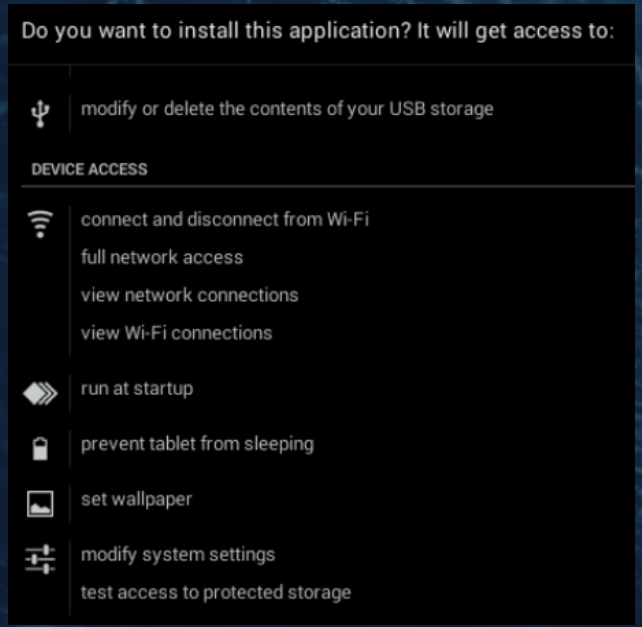
Device Security (cont.)

- Firmware upgrades
- Encryption
  - File-based (Nougat 7.0)
  - Full-disk (Lollipop 5.0)
- Lost devices
  - Lockout settings
  - Find My Device / Find My iPhone
  - International Mobile Equipment Identity



Application Security

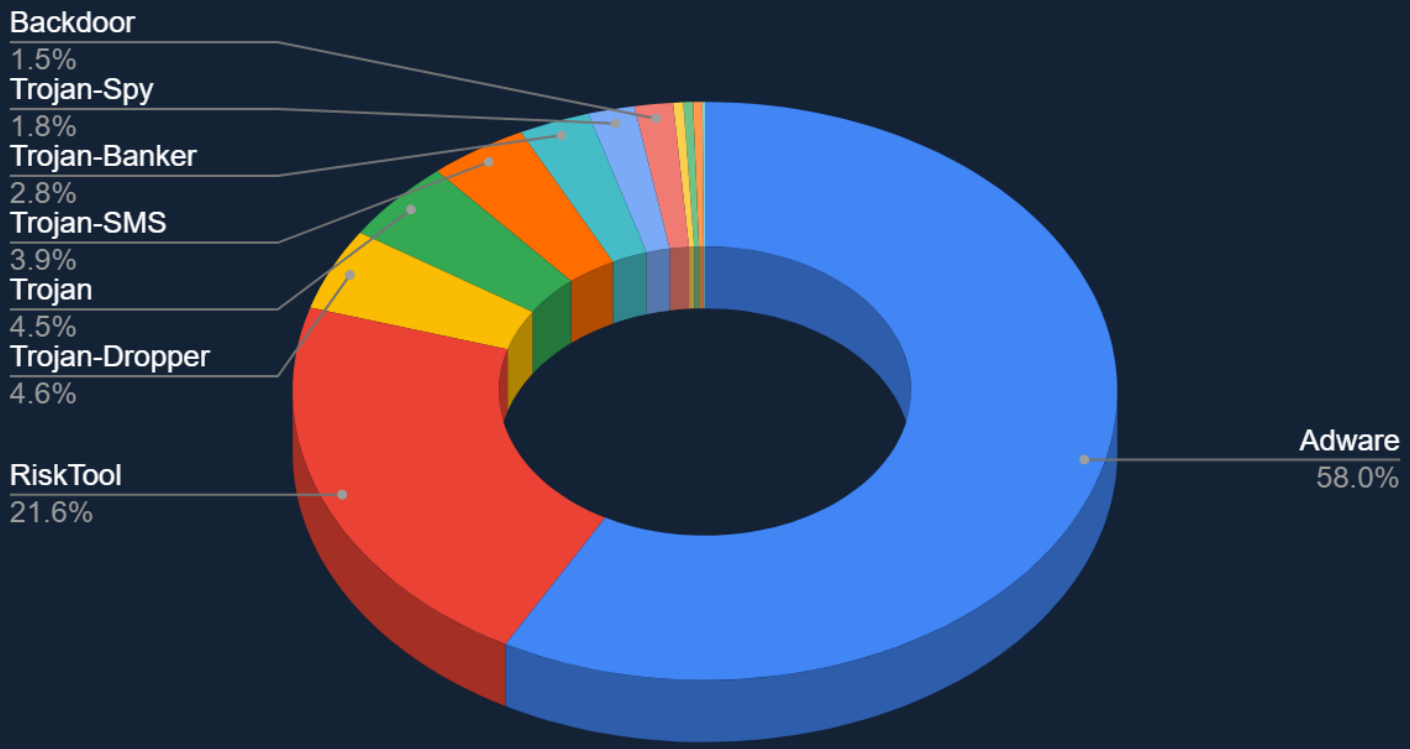
- Permission control
- Storage options
  - Internal (Device)
  - External (SD Card)
- Authentication
- Trusted stores
- Updated apps
- Unusual behaviors
- Tracking



2 Attack Vectors

- What are the current existing threats in our context?
- Why do these attacks occur?
- Who are the malicious actors?

Types of Mobile Malware



Source: FireEye Trends 2020

Common motives

1. **Money** — Bank account compromise, ransomware, billing fraud, unauthorized transactions
2. **Information** — Sensitive data, financial information, chat messages, contacts, government secrets
3. **Vengeance** — Blackmail, account takeover, reputational damage, psyops

Advanced Persistent Threats (APT)

Existing Issues

- Social engineering
- Data leakage through malicious apps
- Unsecured public Wi-Fis
- End-to-End Encryption gaps
- Spyware
- Out of date operating systems

Threat Trends 2021

- Increasing
  - Banking trojans
  - Zero-day attacks
    - Kernel exploits
    - Web-kit exploits
- Decreasing
  - Ransomware
  - Covid-themed malware
    - tousanticovid.apk, coronaalert.apk, coviddetect.apk

Global Statistics Overview

85%

mobile apps today are largely unsecured

4 in 10

mobile devices globally are vulnerable

46%

of organizations had at least one employee download a malicious app

1/3

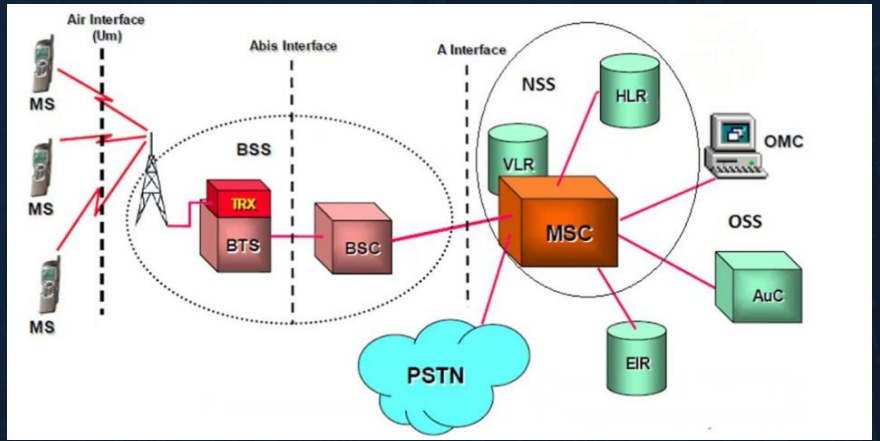
unencrypted communications sent by apps

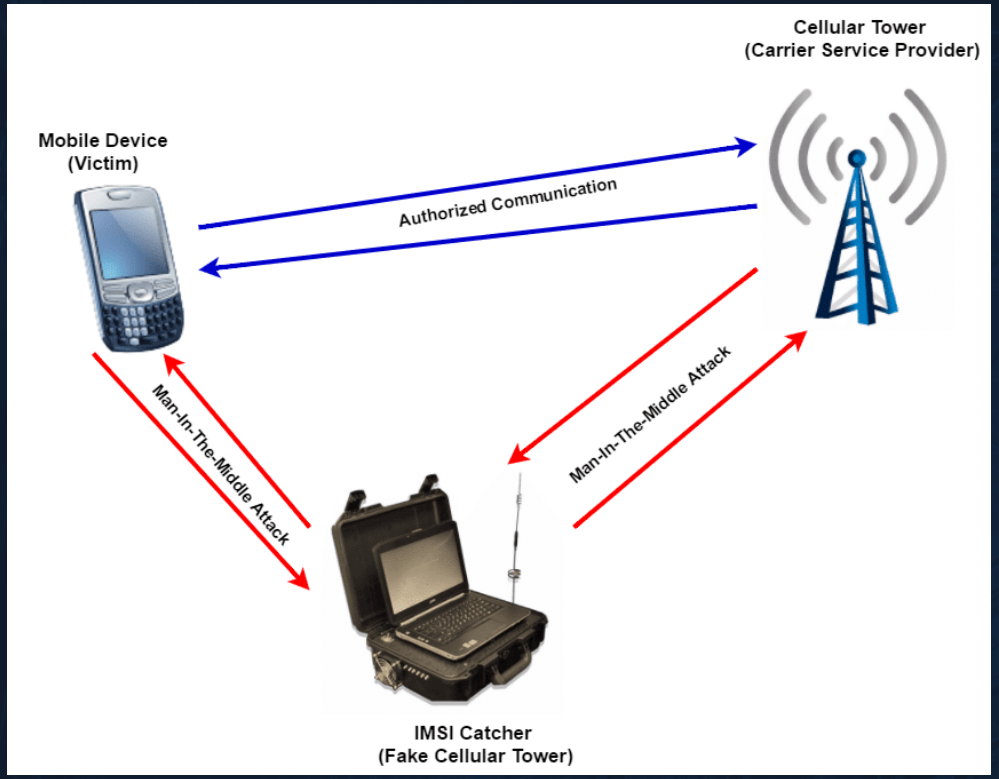
3 Surveillance

- What are some real life examples apropos of intercepting?
- Can we protect ourselves at all?

GSM Interception

- Global System for Mobile Communications (GSM)
- Base Transceiver Station (BTS)
- Cryptographic algorithms
  - A5/1
  - A5/2



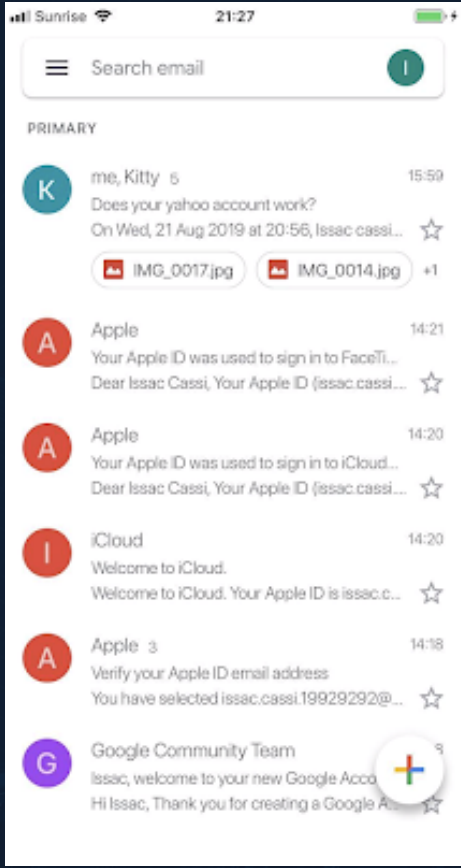

Cellular Tower
(Carrier Service Provider)
Mobile Device
(Victim)
Authorized Communication
Man-In-The-Middle Attack
Man-In-The-Middle Attack
IMSI Catcher
(Fake Cellular Tower)

iOS Spyware

- Scope ranging from iOS 10 to iOS 12 (fixed in 12.1.4)
- Google Project Zero
- Spyware campaign for Uyghur Muslims in China

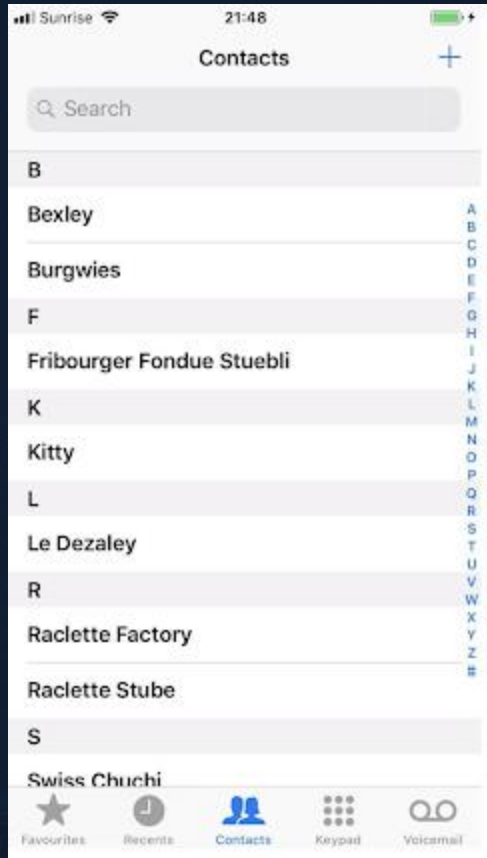
messages database file uploaded by implant

```
$ sqlite3 ChatStorage.sqlite
SQLite version 3.24.0 2018-06-04 14:10:15
Enter ".help" for usage hints.
sqlite> .tables
ZWABLACKLISTITEM          ZWAGROUPMEMBERSCHANGE     ZWAPROFILEPUSHNAME
ZWACHATPROPERTIES         ZWAMEDIAITEM              ZWAVCARDMENTION
ZWACHATPUSHCONFIG         ZWAMESSAGE                ZWAZ1PAYMENTTRANSACTION
ZWACHATSESSION            ZWAMESSAGEDATAITEM        Z_METADATA
ZWAGROUPINFO              ZWAMESSAGEINFO            Z_MODELCACHE
ZWAGROUPMEMBER            ZWAPROFILEPICTUREITEM     Z_PRIMARYKEY
sqlite> select * from ZWACHATSESSION;
...
2|4|6|0|0|272|0|2|0|4|0|0|-5|0||9||588088153.555802||578764AD-682C-42DE-A19
C-8D83C3B60977:ABPerson|447846412085@s.whatsapp.net|||Kitty|
sqlite> select * from ZWAMESSAGE;
...
8|9|4|0|0|0|3|5|0|0|0|2|0|0|8|0|2|-32768||2||||||588088133|588088136.227191
|447846412085@s.whatsapp.net||||3A1A5EF9D85E2656CBFE|Gruuuuezi Issac!|
9|9|4|0|0|0|3|6|0|0|0|0|1|0|8|0|3|-32768||2||2||1||588088153.555802|5880881
53.599606|||||3AE107207900EEC3C115|MEGA HAMMER|447846412085@s.whatsapp.net
```



gmail email database file uploaded by implant

```
$ sqlite3 "./Library/Application
Support/data/issac.cassi.19929292@gmail.com/sqlitedb" "select
hex(item_summary_proto) from items" | xxd -r -p
...
thread-a:r-3850742854413041744Does your yahoo account work??On Wed, 21 Aug
2019 at 20:56, Issac cassi <issac.cassi.19929292@gmail.com> wrote: On Wed,
21 Aug 2019 at 20:49, Issac cassi <issac.cassi.19929292@gmail.com> wro ?
i?-(????-U F?hqx`??G?x?
...
?thread-f:1642479081486697007NYour Apple ID was used to sign in to FaceTime
and iMessage on an iPhone 8.?Dear Issac Cassi, Your Apple ID
(issac.cassi.19929292@gmail.com)
...
```



contacts database file uploaded by implant

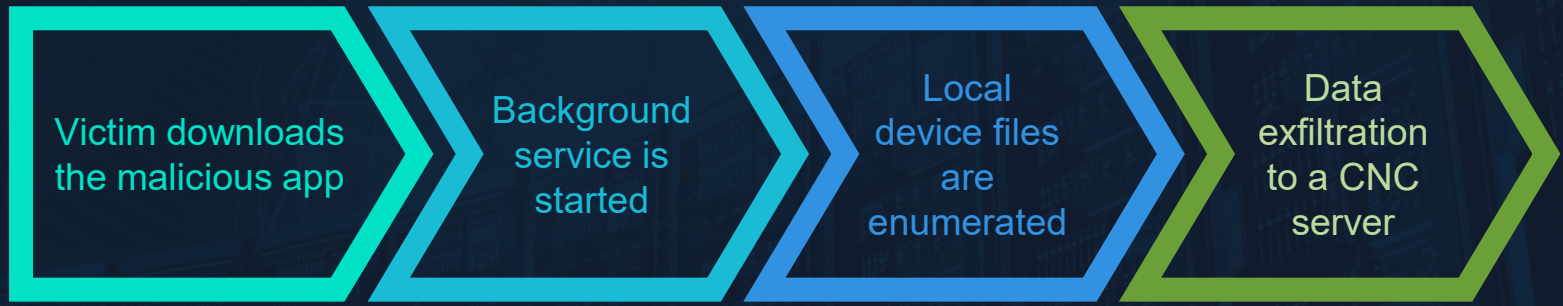
```
$ sqlite3 AddressBook.sqlitedb
sqlite> select First, Organization from ABPerson;
Bexley|
Kitty|
|Le Dezaley
|Swiss Chuchi
|Raclette Stube
|Raclette Factory
|Fribourger Fondue Stuebli
|Burgwies

sqlite> select c16Phone from ABPersonFullTextSearch_content;
07848 795725
07846 412085
+41 44 251 61 29
+41 (0) 44 266 96 66
+41 (0) 44 251 41 30
+41 (0) 44 261 04 10
+41 (0) 44 241 90 76
+41 (0) 44 380 63 20
```

Wijde Lombardsteeg
Enge Lombardsteeg
Sint Luciensteeg
Wijde Kapelsteeg
Enge Kapelsteeg
Watersteeg
Taksteeg
Kuipersteeg
Grimburgwal
Rokin
Spui
Singel
Begijnensteeg
Heisteeg
Wijde Heisteeg
Maagdenhuis
Universiteit

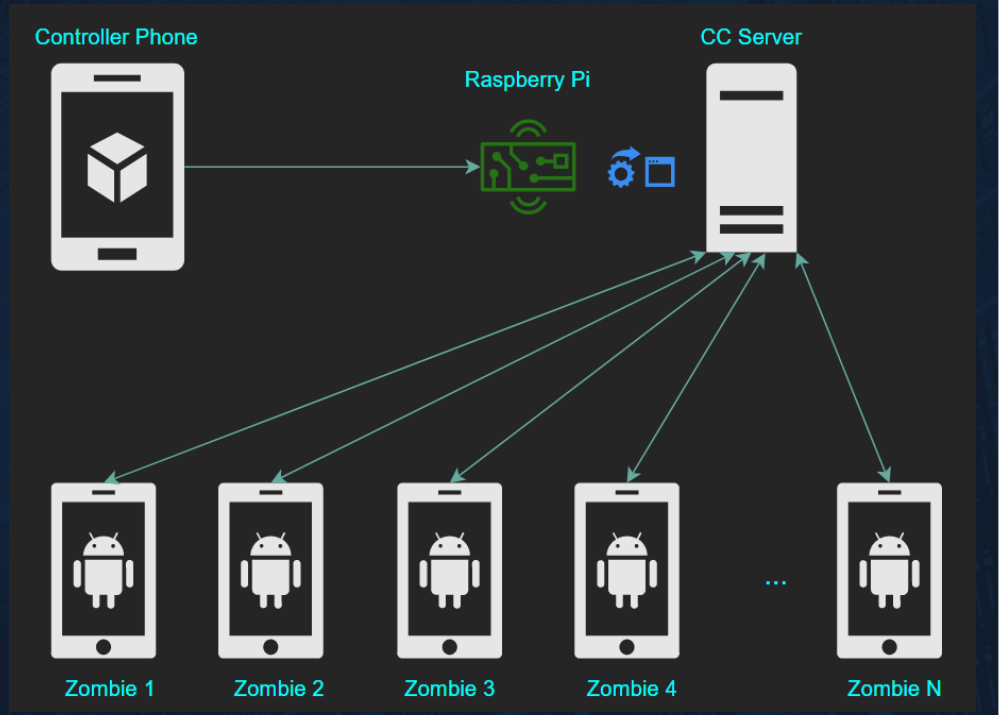
Android Spyware

- Open-source project (github.com/artikrh/SMS-Xombie)
- Any Android version
  - Constrains depending on release
- Retrieve SMS messages, call logs, contacts, geolocation, installed apps…



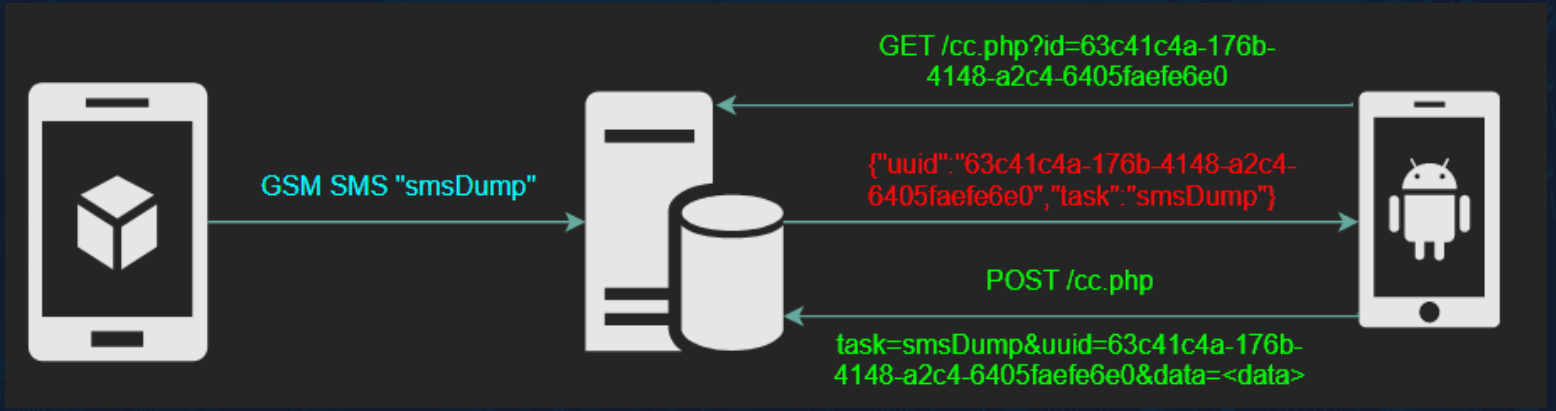
Android Spyware

- Infected devices
- CNC Server
- Controller



Android Spyware

- Communication occurs every 1 minute
- Each ‘zombie’ device has a unique ID



Key Security Measures

Security Awareness

Implement a regular awareness and training program. Because end users are targets, employees should be aware of the current threat environment

Security Controls

Managed devices, monitoring & auditing, role-based access management, remote patching, data isolation (business vs personal), security configurations

Business Continuity

Regular data backup, integrity check, avoiding single point of failures, connectivity, Disaster Recovery Center (DRC)

Keep in **mind:**

- Kosovo Police: Cyber Crime Unit
- Data Protection: The Information and Privacy Agency
- Cyber Security: National Authority for Cyber Security
- Computer Emergency Response Team: KOS-CERT

Investigative Podcast

- Darknet Diaries (*darknetdiaries.com*)
- Real life stories
  - Major cyber incidents and data breaches
  - Insider threats
  - Physical security assessments
  - Cyber espionage
  - Wiretapping

Thanks!

You can find me at:

- linkedin.com/in/artikarahoda
- artikrh.sh