SVEUČILIŠTE U ZAGREBU
Fakultet elektrotehnike i računarstva

Diplomski studij

Sigurnost komunikacija

Ak. godina 2021/2022

Sigurnost u mobilnoj telefoniji

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, preradu 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/.

Kako je sve počelo...

- 1970-te:
  - prve pokretne mreže (“1G”)
  - analogno, ograničeno
  - FDMA
- 1980-te:
  - evolucija mreža
  - prijedlog GSM-a
- 1990-te:
  - prva komercijalna GSM mreža u Finskoj
  - druga generacija mreža (2G)
    - TDMA, CDMA
  - 1997. mobilni Internet
    - WAP (Wireless Application Protocol)

Kako je sve počelo - sigurnost... (1/2)

- fizička sigurnost
  - uvijek aktualan problem
  - gubitak uređaja
  - količina informacija na uređaju nekada i danas nije ista!
- razina signala
  - prisluškivanje
    - bežično ili fizički na baznoj stanici
  - ometanje
    - emitiranje na istoj frekvenciji
  - 1986. - Electronic Communication Privacy Act

Kako je sve počelo - sigurnost... (2/2)

- identifikacija korisnika
  - SIM kartica (Subscriber Identity Module) – tajni ključ
  - šifriranje komunikacije - algoritam A5
  - kod UMTS-a – USIM – duži ključ
- identifikacija uređaja
  - tijekom prijave na mrežu
  - IMEI (International Mobile Equipment Identity)
- mobilni Internet
  - WTLS (WAP Transport Layer Security)
    - dosta problema, 3 klase (šifriranje i certifikati)
    - WAP Gap - “rupa” tijekom prijelaza s WTLS-a na SSL/TLS

Sigurnost u mobilnoj telefoniji

- tradicionalno
  - fizička razina
    - gubitak uređaja
  - razina radio signala
    - ometanje signala, prisluškivanje
  - signalizacija
    - identifikacija korisnika i uređaja

- "pametni" telefoni
  - sigurnost aplikacija
  - *bluetooth*
  - *malware*
  - *wardriving*
  - RFID *sniffing*
  - uskraćivanje usluge (DoS)
  - web aplikacije

Prijetnje na pametnim telefonima (1/4)

- sigurnost aplikacija
- *bluetooth*
  - *blue jacking, blue snarfing, blue bugging, blue sniping*
- *malware*
- *wardriving*
- RFID *sniffing*
- uskraćivanje usluge (DoS)
- web aplikacije

Prijetnje na pametnim telefonima (2/4)

- gubitak privatnosti
  - netko čita poruke, mailove, gleda slike
  - ali i: krade podatke o kontaktima (tel. brojevi, elektronička pošta)
- financijski gubici
  - slanje SMS poruka na premium brojeve
  - krađa podataka kartica (kao web)
- krađa identiteta
  - RFID na mobitelima
  - postojeće aplikacije na uređaju često i identificiraju korisnika radi lakšeg korištenja (m-token, Facebook, Skype)

Prijetnje na pametnim telefonima (3/4)

- pokretni uređaj sa zlonamjernom aplikacijom predstavlja prijetnju vlasniku ali i mreži na koju se spaja

- poslovna okolina (npr.)
  - mreža je dobro zaštićena prema Internetu, ali često se previđaju prijetnje “iznutra”
  - vlasnik pokretnog uređaja ne mora biti zlonamjeran niti svjestan prijetnji na vlastitom uređaju
  - ako mreža nije dobro zaštićena, virusi, crvi i trojanci mogu se neometano širiti u naizgled zaštićenoj mreži
  - potrebno dobro zaštiti bežične pristupne točke (WLAN AP)
    - firewall, detekcija napada, DMZ....

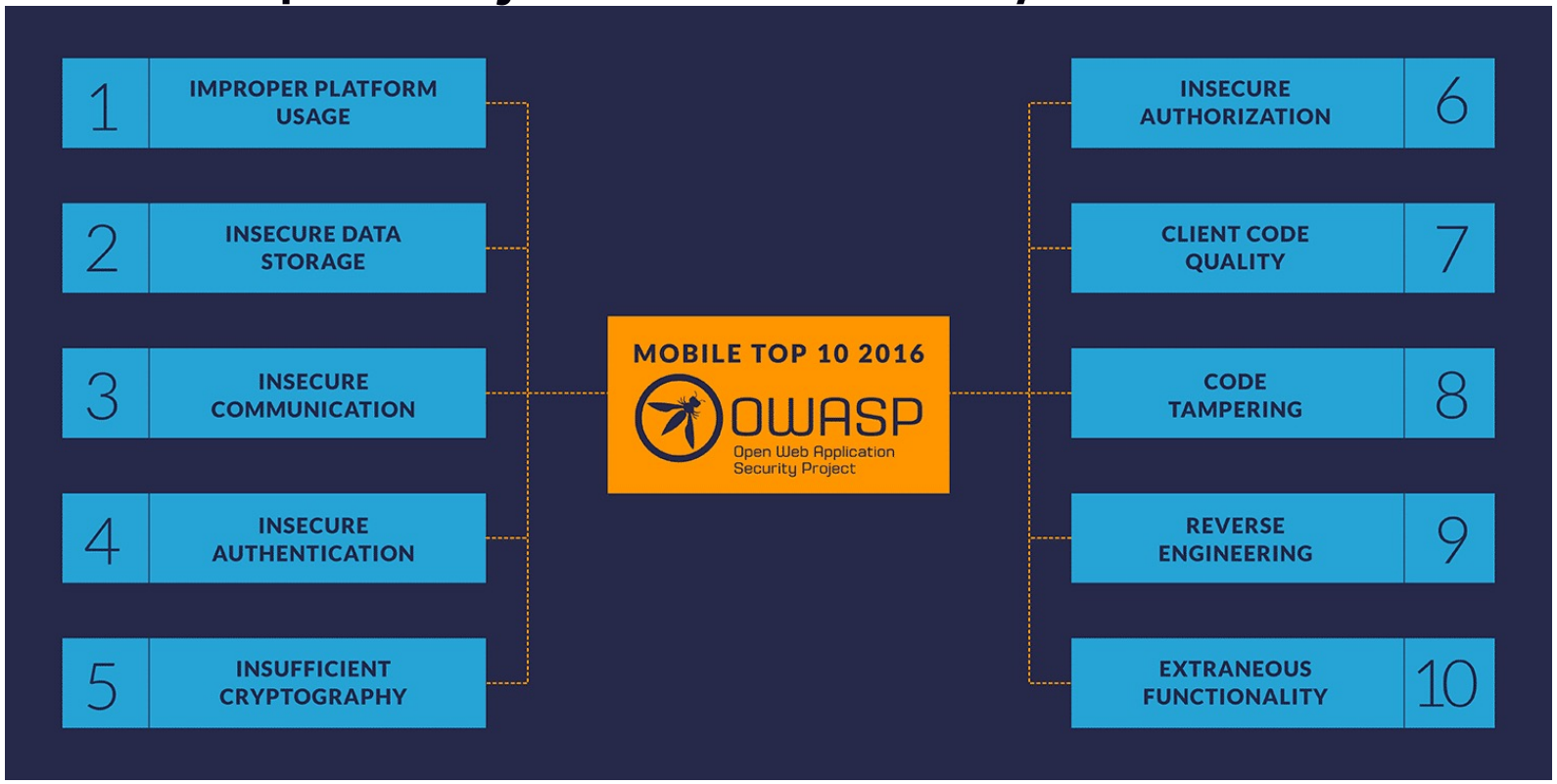
Prijetnje na pametnim telefonima (4/4)

- pametni telefoni danas se koriste gotovo isto kao i računala
  - pregledavanje weba, plaćanje računa, elektronička pošta, trenutačno poručivanje, društvene mreže

- stoga su i rizici vezani uz aplikacije i komunikaciju gotovo isti kao i kod računala ali:
  - na telefonima je lakše doći do novca preko operatora (npr. premium SMS), uz "standardne" prevare kreditnim karticama
  - pristup lokaciji korisnika
  - percepcija telefona nije ista kao i percepcija laptopa ili stolnog računala
    - prevare se "ne očekuju" jer korisnici nisu na njih navikli
    - lakši pristup privatnim mrežama (WLAN) - napadi iznutra

Sigurnost aplikacija - *OWASP top 10 mobile 2014*

Sigurnost aplikacija - *OWASP top 10 mobile 2016*



https://www.nowsecure.com/blog/2016/10/13/secure-mobile-development-testing-owasp-mobile-top-10/

Weak Server Side Controls

- Loša kontrola na poslužitelju
  - Obuhvaća sve što može poći po zlu na poslužitelju!

- Neki razlozi…
  - Kratki rokovi, mali budžet za sigurnost kod mobilnih aplikacija, oslanjanje na mobilni dio i zanemarivanje poslužiteljskog djela…

- Najčešći uzroci – OWASP *top 10 web* i OWASP *top 10 cloud*
  - Loša programska logika
    - ne pazi se na sve moguće obrasce korištenja usluge / aplikacije
  - Slaba autentifikacija
    - Provjera prava pristupa, kakve su lozinke, kako je proces autentifkacije zaštiće, koliko je proces autentifikacije složen
  - Upravljanje sjednicama
    - Kako se korisnici identificiraju? Je li moguće “ukrasti” sjednicu?
  - Konfiguracija poslužitelja
    - Jesu li sve komponente sigurne i ažurirane? “Cure” li podaci npr. u logove?
  - Napadi umetanjem (*injection*)
    - Umetanje SQL, javascripta i naredbi

Insecure Data Storage

- Nesigurna pohrana “osjetljivih” podataka
- Što su uopće osjetljivi podaci?

- Europska GDPR (General Data Protection Regulation)
  - Različite vrste podataka su deklarirane kao osjetljive
  - Česti auditi i velike kazne!

- Podaci na mobilnom telefonu
  - Jesu li šifrirani?
  - Vide li se podaci u logovima?
  - Problem s Androidom zbog (lošijeg) *sandboxing*-a
    - Šifriranje podataka na SD kartici
    - Koristiti poseban dio sa sklopovskim šifriranjem (*secure element*)?
  - Ali i s iOS-om
    - Npr. pohrana podataka za autentifikaciju korisnika u bazu podataka aplikacije bez šifriranja

Insufficient Transport Layer Protection

- Nedovoljna zaštita na transportnom sloju
- Česta ranjivost kod svih internetskih aplikacija općenito
- Gdje se sve šalju podaci iz mobilne aplikacije?
  - Jesu li ti podaci “osjetljivi”?
- Imamo li šifriranje na transportnom sloju?
- Koristiti HTTPS odnosno SSL / TLS

Unintended Data Leakage

- “Curenje” podataka
- Tijekom razvoja sve se zapisuje u logove a na produkciji ne bi smjelo (npr. brojevi kartica)
- Mobilne aplikacije
  - Najveći problem je priručno spremanje (*cacheing)*
  - Provodi se kako bi se optimiziralo izvođenje aplikacija
  - Provode ga:
    - aplikacije, radni okviri za razvoj aplikacija ali i operacijski sustav
  - Što se pohranjuje?
    - podaci, slike, tipkanje i sadržaj međuspremnika (*buffer*)
    - razvijatelji ne mogu previše na to utjecati!
- Očekivani ishod: *malware* dobije pristup pohranjenim podacima druge aplikacije

Poor Authorization and Authentication

- Loša autorizacija i autentifikacija

- Glavni problemi:
  - Razvijatelji poslužiteljske strane očekuju da će samo legitimni mobilni korisnici pristupati poslužitelju
    - Ali servis je otvoren za sve kao i svaki drugi web servis…
  - Razvijatelji pogrešno smatraju kako je mehanizam spajanja na poslužitelj nevidljiv korisnicima
    - Reverznim inženejrstvom moguće je doći do koda aplikacije
    - Snimanjem mrežnog prometa moguće je vidjeti poruke i pakete
  - Mobilne aplikacije često dozvoljavaju slabije lozinke (kraće!) radi bolje uporabljivosti što olakšava napad na lozinke

Broken Cryptography

- Loše upravljanje kriptografijom
  - Npr. kriptografija postoji ali ključevi su lako vidljivi napadačima

- Tipični scenariji
  - Korištenje (samo) ugrađenih mehanizama šifriranja
    - iOS šifrira kod aplikacija ali ga dešifrira prije podizanja u memoriju
    - Postoje alati koji u tom trenutku na *jailbreak* uređajima mogu doći do podataka
  - Loše upravljanje ključevima
    - Napadač može pristupiti datotekama s ključevima
    - Ključevi su zapisani u kodu aplikacije (*binary*) te napadač može doći do njih
  - Izrada vlastitih mehanizama šifriranja
    - Česte greške ako se ne posveti dovoljno vremena i znanja!
  - Korištenje zastarjelih algoritama
    - Mnogi algoritmi su već probijeni ili zahtjevaju veće duljine ključeva

Client Side Injection

- Umetanje na klijentskoj strani
  - Do sada smo razmatrali umetanje na poslužitelju (kod, SQL, javascript)
- Razmisliti o tome što sve korisnik unosi i pretpostaviti da neće unositi ono što očekujemo
- Što se sve može “ubaciti”?
  - Kao i kod poslužitelja, može unositi SQL (SQLLite) ali i datoteke (*File inclusion*)
    - Npr. na poslužitelj je ubačen sadržaj koji rezultira u ovom napadu kada apliakcija učita podatke
  - Ako aplikacija koristi mobilni preglednik moguće je umetati Javascript (XSS)
  - Preplavljivanje spremnika tj. metoda / funkcija – rušenje aplikacija (npr. *jailbreak*!)
    - Npr. jedna maliciozna aplikacija radi napad na drugu aplikaciju
  - Ubacivanje koda putem binarnih datoteka

Security Decisions Via Untrusted Inputs

- “Sigurnosne odluke na temelju nepovjerljivih izvora”
- Mehanizam *Inter Process Communication* (IPC)
  - Mehanizam za dijeljenje podataka između aplikacija
- Jedna aplikacija šalje ulazne podatke drugoj
  - zahtjev za lokacijom
  - autorizacija
  - prikaz podataka na karti…
- Moguće je mijenjati te podatke ili ubaciti lažne zahtjeve od strane *malwarea!*
- Ovim mehanizmom ne bi trebalo slati osjetljive podatke!
- Ako aplikacija takve podatke koristi kao ulaz onda ih treba dobro provjeriti i sanitizirati

Improper Session Handling

- Loše upravljanje sjednicom
  - Kao i kod poslužitelja
  - Sjednica = pristup pravima korisnika koji je “vlasnik” sjednice
  - Sjednicu kontrolira poslužitelj a kao korisnik se identificira aplikacija
    - Kolačići (cookie), tokeni s vremenskim istekom…

- Neki primjeri iz mobilnih aplikacija
  - Problemi s odjavljivanjem na poslužitelju
    - Korisnik se odjavi u mobilnoj aplikaciji ali se to stanje ne preseli na poslužitelj
  - Vremenska kontrola
    - Često je vremenska kontrola loše izvedena ili je nema pa jedna sjednica traje predugo što otvara prostor za napadače kojima ukradena sjednica “dulje vrijedi”
    - Djelomičan razlog su i dulja trajanja sjednica na mobiltelima zbog uporabjivosti aplikacija
  - Upravljanje kolačićima (rotacija)
    - Kada se korisnik prijavi trebao bi mu se izdati novi kolačić
  - Nesigurni tokeni
    - Korištenje zastarjelih tj. probijenih algoritama za kreiranje tokena

Lack of Binary Protections

- Nedostatak zaštite binarnog koda aplikacije
- Glavni problem: iz binarnog zapisa moguće je doći do izvornog koda aplikacije
  - *Reverse engineering*, mnoštvo alata, npr. APKTool, ClutchMod

- U originalnu aplikaciju se nakon otkrivanja izvornog koda ubacuje dodatni kod koji se prikriva kao korisna originalna aplikacija
  - Tipičan scenarij malwarea na Androidu!

- Zaštita?
  - Detektirati je li uređaj na kojem se aplikacija izvodi "*jailbreakan*" ili "*rootan*"
  - Provjeravati zaštitnu sumu kako bi se utvrdila promjena aplikacije
  - *Certificate Pinning Controls*
    - Korištenje predefiniranih certifikata pri spajanju na vanjske usluge
    - https://www.owasp.org/index.php/Certificate_and_Public_Key_Pinning
  - Detektirati je li aplikacija pokrenuta u *debug* načinu rada

Code tampering

- Jednom kada je aplikacija instalirana na uređaj sav kod i podaci se nalaze na uređaju
- Je li uređaj “rootan” / “jailbreakan”?
  - Root ovlast!
- Mijenjanje podataka koje aplikacija koristi
- Mijenjanje knjižnica koje aplikacija koristi
- “Put prema” reverznom inžinjeringu…

Reverse Engineering

- Koliko je teško doći do izvornog koda aplikacije?
  - Obfuksacija?
- Otkrivanjem izvornog koda mogu se otkriti
  - Sigurnosni mehanizmi
  - Korištenje ranjivih algoritama
  - Izbjeći neke provjere i kontrole
  - Pozadinski poslužitelji i komunikacija
  - Lokalno pohranjene lozinke, tokeni, ključevi…
- Promjena funkcionalnosti i ponovna objava aplikacije
  - Čest slučaj, ubacivanje malwarea!

Bluetooth ranjivosti (1/3)

- većina Bluetooth (BT) platformi ima ranjivosti
  - loše implementiran BT složaj
    - ne prati se duljina paketa
    - Buffer overflow napadi
  - pogrešne IRMC (*Integrated Remote Management Controller*) dozvole na datoteke
    - otvorene konekcije omogućuju pristup svim uređajima, a ne samo uparenim
  - loše implementirane usluge temeljene na BT
    - česti propusti u implementaciji koji omogućuju neovlaštene upade i pregledavanje datoteka na uređaju
  - otvoreni kanali
    - korisnici nisu svjesni prijetnji pa uređaj ostaje vidljiv i nakon korištenja (npr. nakon BT slušalica u vozilu)

Bluetooth ranjivosti (2/3)

- *blue jacking*
  - slanje poruka na uređaj putem BT
  - najčešće reklame ovisne o lokaciji (domet 10m)
  - bezopasno, ali oblik spama
- *blue snarfing*
  - neovlašteni pristup uređaju s BT
  - pronalazi otvorene BT kanale i tim putem pristupa uređaju
  - omogućuje:
    - pregledavanje i preuzimanje kontakata, slika, kalendara i poruka ovisno o uređaju
  - onemogućeno na novijim platformama (za sada)

Bluetooth ranjivosti (3/3)

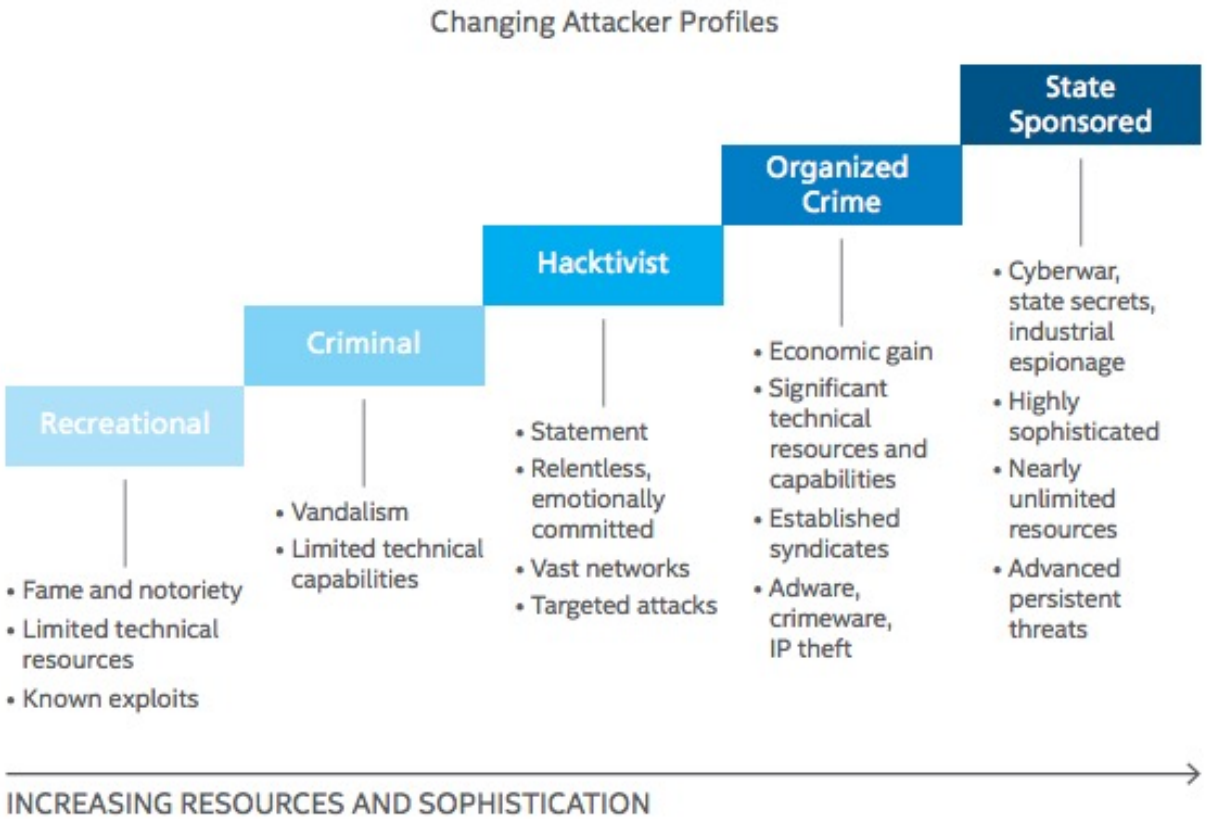
- *blue bugging*
  - kao bluesnarfing – napadač ostvaruje pristup uređaju žrtve
  - omogućuje slanje AT naredbi ciljanom uređaju
    - pozivanje brojeva, slanje SMS poruka
    - preusmjeravanje dolaznih poziva na uređaj napadača (uređaj se predstavlja kao BT slušalica)

- *blue sniping*
  - uobičajene BT antene dometa do 15 m (telefoni) ili do 100 m (laptop)
    - ograničenje kod napada
  - proširenje bluetooth napada većim dometom antene
    - na kućište se stavlja procesor i usmjerena antena velikog dometa koja omogućuje “snajpersko ciljanje “ uređaja
    - domet do 2 km

Malware

- virusi, trojanci i crvi
  - prvi mobilni malware identificiran 2004. godine (Mosquito)
    - trojanac skriven u igru
    - slanje SMS poruka na premium brojeve
- slični rizici kao na računalima uz “novosti”:
  - pristup lokaciji
  - pristup pokretnoj mreži (naplata)
- prijenos malwarea:
  - elektronička pošta (privitak)
  - linkovi na zlonamjerne stranice
  - instalacija naizgled korisnih aplikacija od strane korisnika
  - bluetooth
  - neizravno: nadogradnja opercijskog sustava (npr. jailbreaking)

Malware – “proizvođači” – ne samo mobilni!



http://www.mcafee.com/us/resources/reports/rp-quarterly-threats-aug-2015.pdf

Malware - prijetnje

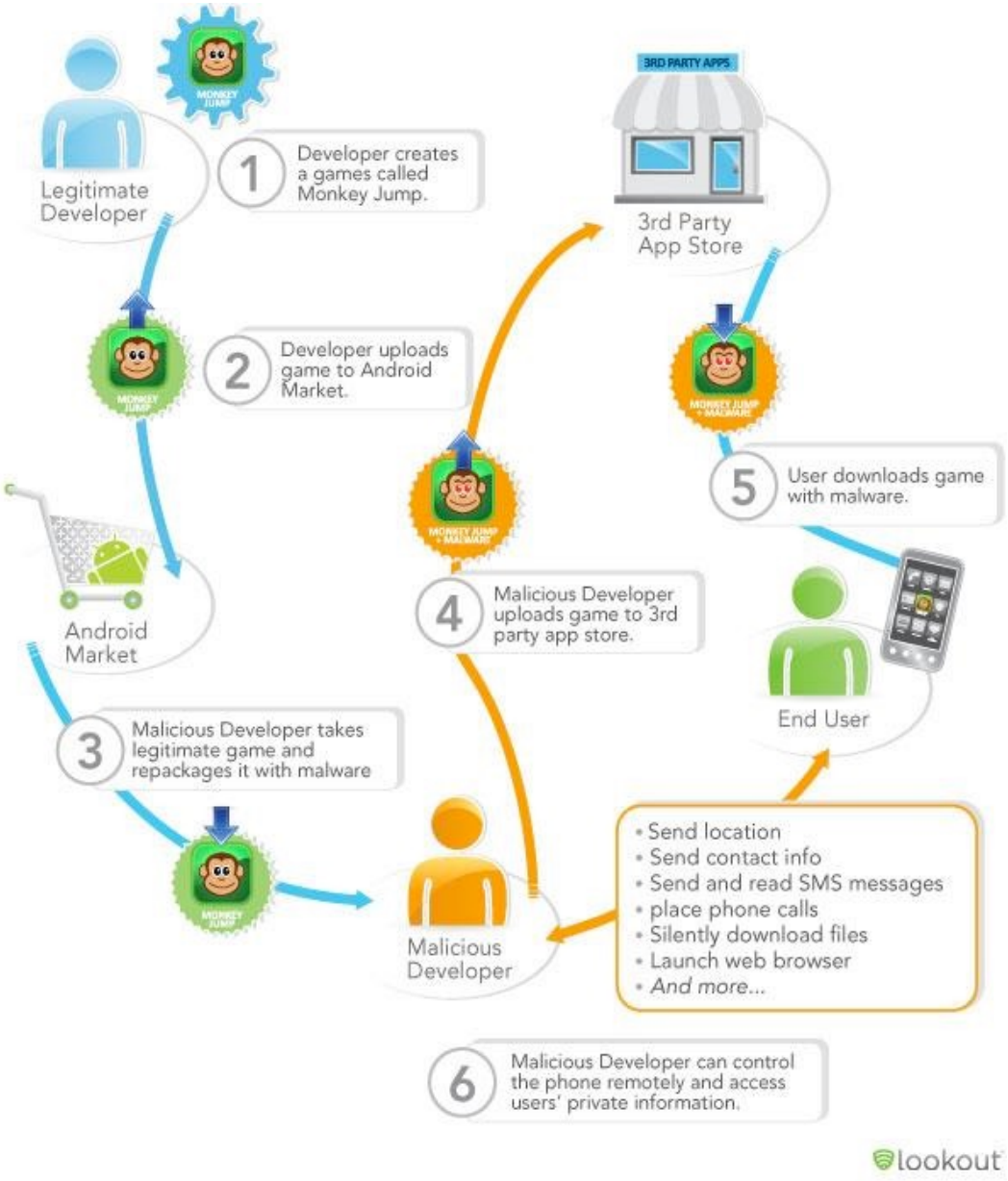
- što malware na pokretnom telefonu radi?
  - krađa lozinki
  - phishing aplikacije
    - prva 2010. na Androidu
    - predstavljala se kao aplikacija banke
  - krađa povjerljivih podataka
    - posebno lokacije korisnika
  - brisanje podataka s uređaja
  - slanje SMS poruka na premium brojeve
    - Mosquito 2004. (Symbian)
  - korištenje uređaja kao dio botneta
    - Symbian 2009.
  - uništavanje uređaja (*bricking*)

Malware – potpisivanje aplikacija

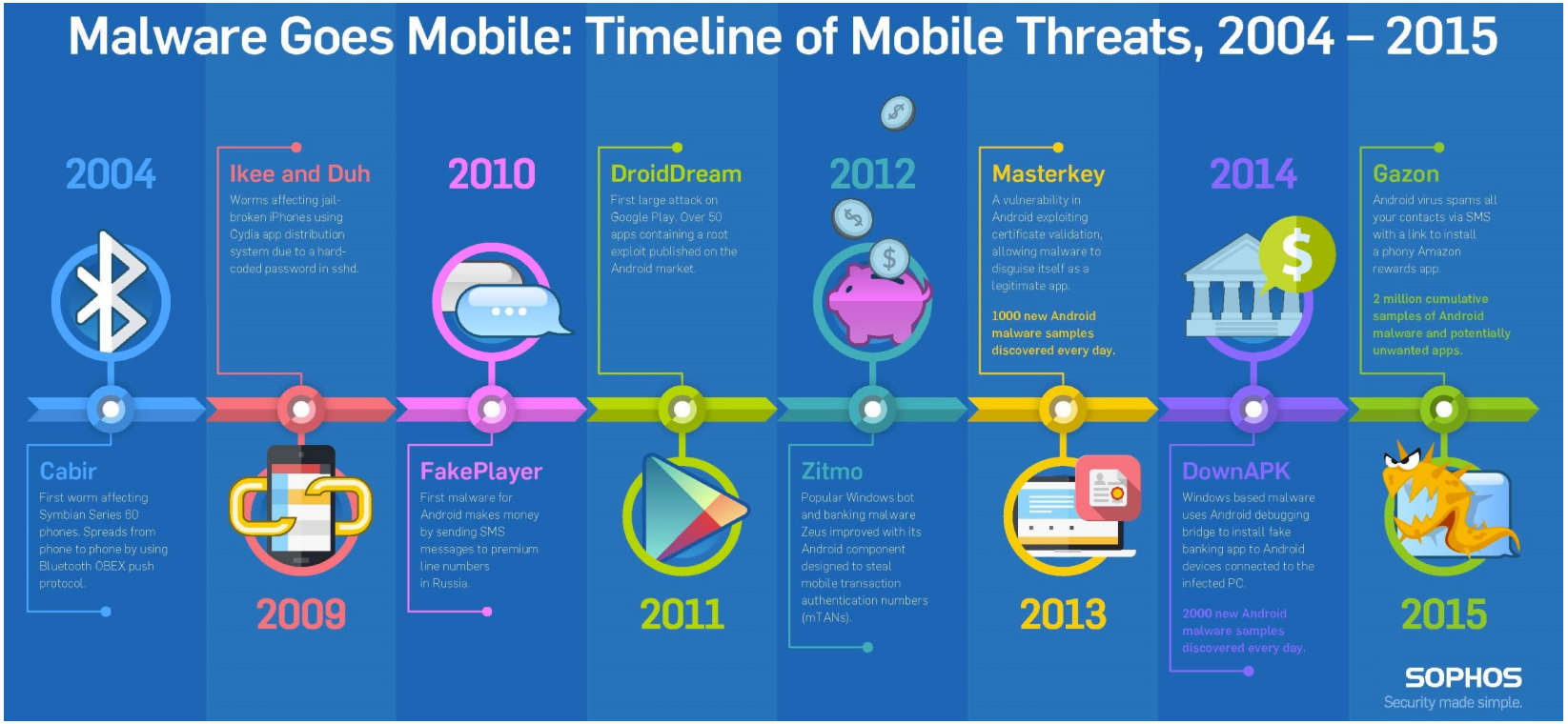
- malware u aplikacijama - kako ga spriječiti?
  - Ideja je testirati aplikacije kako bi se utvrdilo jesu li štetne za korisnike ili treću stranu (na bilo koji način)
  - ako su aplikacije u redu onda se izdaje potpis kojim se jamči da je aplikacija prikladna (npr. code signing)
  - primjeri:
    - Java ME
      - aplikacija koja nije bila potpisana morala je uvijek pitati korisnika može li pristupiti resursima uređaja (SMS, poziv i slično)
      - jedino potpisane aplikacije su mogle pristupati resursima bez pitanja
    - iPhone
      - koncept AppStorea - Jailbreak?
    - Android
      - Android market
      - instalacija aplikacija od strane korisnika

Tipičan scenarij

http://appleinsider.com/articles/11/08/03/lookout_retrevio_warn_of_growing_android_malware_epidemic_note_apples_ios_is_far_safer



Malware – operacijski sustavi (1/4)



https://www.404techsupport.com/wp-content/uploads/2015/05/sophos-mobile-malware-timeline-infographic.jpg

Malware – operacijski sustavi (2/4)

- Android
  - najugroženiji zbog velikog broja korisnika
  - trend malwarea
    - lipanj 2010. – siječanj 2011 – porast 400%!
    - Q1 2012 – porast od 1200%
    - 2012. – porast od 2180%!
  - preko 80 aplikacija je uklonjeno s Android Marketa jer su sadržavale maliciozan kod
  - glavna prijetnja
    - "provaljene" igre koje se inače naplaćuju
- Blackberry
  - najčešće spyware
  - trojan Zeus – autorizacija plaćanja preko SMS poruke

Malware – operacijski sustavi (3/4)

- Symbian
  - do nedavno najzastupljenija platforma
    - najviše postojećeg malwarea
  - problem s potpisivanjem aplikacija
    - korisnici mogu sami instalirati aplikacije preuzete s Interneta
  - prvi malware, prvi botneti, auto-dialeri ...
  - Symbian podržava Javu ME pa preuzima i taj dio rizika

- Windows Mobile
  - uz Symbian jedna od najstarijih i najnapadanijih platformi
    - sličan problem – korisnici mogu sami instalirati aplikacije
  - najčešće auto-dialeri zapakirani u korisne aplikacije

Malware – operacijski sustavi (4/4)

- iOS
  - prilično siguran zahvaljujući kontroli AppStorea i općenito (pre)restriktivnoj politici Applea
  - ipak, aplikacije koje korisničke profile pohranjuju na webu mogu biti predmet napada
  - Apple zapisuje kretanje korisnika? – baš i ne!
  - problem: *jailbreak*
    - omogućuje korisnicima da preuzimaju aplikacije iz drugih izvora
      - veliki rizik malwarea
    - većina korisnika nakon jailbreaka ostavlja početnu root lozinku
  - 2014. - *Keylogger* kao posljedica grešaka u implementaciji sustava
  - 2016. - Pegasus

Pegasus

- 2016.
- Iskorištavao ranjivosti Apple iOS do verzije 9.3.5.
  - *CVE-2016-4655: Information leak in Kernel – A kernel base mapping vulnerability that leaks information to the attacker allowing him to calculate the kernel's location in memory.*
  - *CVE-2016-4656: Kernel Memory corruption leads to Jailbreak – 32 and 64 bit iOS kernel-level vulnerabilities that allow the attacker to secretly jailbreak the device and install surveillance software.*
  - *CVE-2016-4657: Memory Corruption in Webkit – A vulnerability in the Safari WebKit that allows the attacker to compromise the device when the user clicks on a link.*
- Klikom na poveznicu telefon se "jailbreaka", instalira se malware koji čita poruke, prati pozive, lokacije…

AdWare – Android, 2019

- 2019.
- 42 aplikacije u Google Play Store-u s AdWare-om (istim)
  - Android/AdDisplay.Ashas
- Nakon instalacije legitimne aplikacije
  - adware se pokreće kao pozadinski servis
  - komunicira s C&C poslužiteljem i šalje podatke o uređaju, OS-u…
- U nasumična vremena podiže transparentni ekran preko aktivne aplikacije s oglasom
  - nasumičnost - teže za povezati iz koje aplikacije je inicijalno pokrenut
  - Zavarava korisnika korištenjem lažnih imena procesa (paket com.google.xxx)
- Kreator pronađen preko C&C poslužitelja (Vijetnam)
  - Zanimljivo: OSINT (Open Source INTellignece)

- https://www.welivesecurity.com/2019/10/24/tracking-down-developer-android-adware/

Wardriving

- geokodiranje pristupnih točaka bežične mreže
  - uređaj s tehnologijama WIFI i GPS
- “napadač” se kreće područjem i zapisuje razine signala okolnih bežičnih mreža s GPS koordinatama
- zlonamjerno?
  - može i ne mora biti
  - najčešća svrha je utvrđivanje otvorenih ili ranjivih pristupnih točaka
  - moguće i za pozicioniranje pokretnih uređaja pomoću WLAN APa ili baznih stanica
    - npr. Google i Geolocation API, Apple....
- alati za većinu mobilnih platformi
  - WiFi-Where (iPhone), G-MoN i Wardrive (Android), WlanPollution (Symbian)

RFID sniffing (1/2)

- RFID (Radio Frequency IDentification)
  - antena pobuđuje oznaku (tag) koja koristi EM polje antene kako bi odaslala vlastiti identifikator
  - neki noviji telefoni imaju ugrađene oznake (Nokia, Samsung, HTC...)
- RFID oznaka jedinstveno identificira korisnika
  - alternativa kreditnim karticama, članskim iskaznicama, kod evidencije radnog vremena....
- problem sigurnosti
  - pretpostavimo da pokretni telefon (ugrađeni tag) jedinstveno identificira korisnika
  - ako napadač ukrade ID korisnika može se lažno predstavljati!

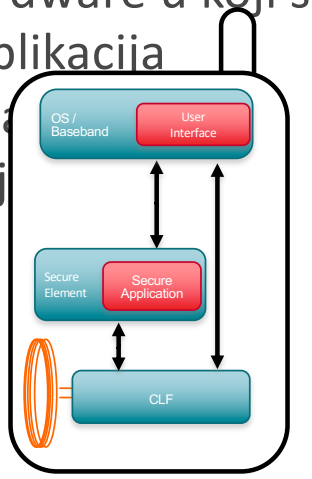
RFID sniffing (2/2)

- sigurnost je trenutačno veliki problem kod tehnologije RFID

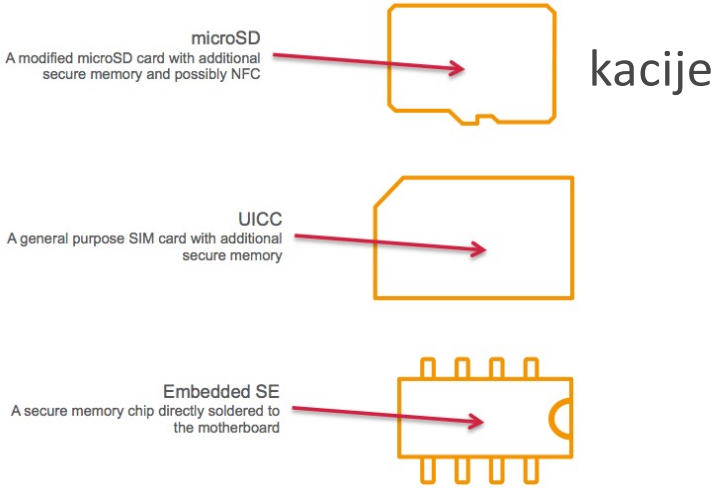
- zaštita
  - šifriranje podataka na oznaci
    - npr. MIFARE (studentske Xice)
  - ograničeni doseg antene
    - NFC antena odašilje na nekoliko cm
    - moguće povećanje dosega (sjetimo se blue snipinga...)?
  - beskontaktno plaćanje
    - *Secure Element*
  - još se u velikoj mjeri istražuje

Sigurnosni element i NFC

- *Secure element* (SE)
  - sigurnosni hardware u koji se smještaj
  - *sandboxing* aplikacija
  - sa ili bez NFC-
  - “kartica postaj



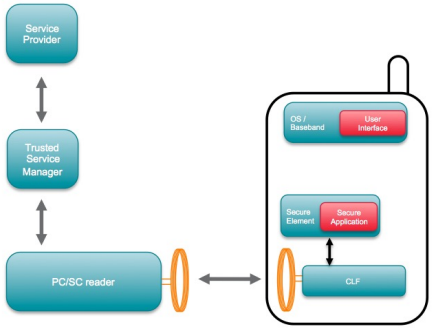
kacije

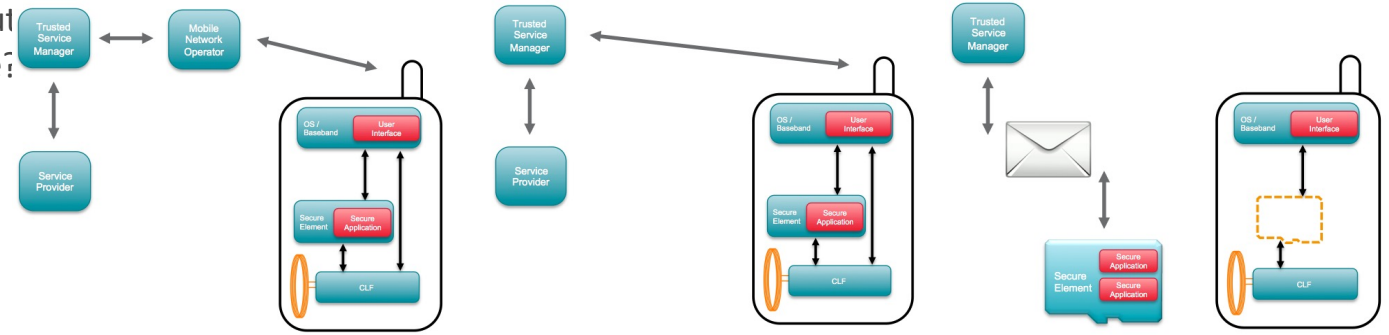


http://www.smartcardalliance.org/resources/ppt/NFC_Standards_for_the_NFC_Ecosystem_FINAL_103112.ppsx

Komunikacija sa sigurnosnim elementom

- *Provisioning*
  - smještanje aplikacija ili podataka na sigurnosni element
  1. OTA (over-the-air)
  2. putem Interneta
  3. putem NFCa
  4. fizički put
  - prijetnje?





http://www.smartcardalliance.org/resources/ppt/NFC_Standards_for_the_NFC_Ecosystem_FINAL_103112.ppsx

DoS

- DoS na pokretnim uređajima je dugo prisutan
  - ometanje signala
  - SMS bombardiranje
- novije tehnike
  - iskorištavanje funkcija pokretnog telefona pomoću malwarea
    - automatsko odbijanje dolaznih poziva
    - periodičko odspajanje s mreže
  - Napad pomoću tehnologije VoIP
    - uspostava puno paralelnih poziva prema istom broju
    - prekidanje i ponovno zvanje u slučaju javljanja
- napadi ove vrste ipak rijetki u mobilnoj telefoniji

Web aplikacije

- “pametni telefoni” slični računalima pa su izloženi sličnim prijetnjama
- najpopularniji *phishing*
  - nije nužno vezan uz mobilnu telefoniju
  - linkovi se šalju elektroničkom poštom, SMS porukama, društvenim mrežama...
- preuzimanje aplikacija s weba
  - automatsko preuzimanje kojeg korisnici nisu svjesni
- rizici kod prijenosa podataka
  - prisutnost SSLa, problem na starijim telefonima zbog WTLSa
  - transport podataka koji mogu biti lako čitljivi (npr. elektronička pošta)
- “rupe” u mobilnim preglednicima

Kako se štititi?

- Ažuriranje sustava na najnoviju verziju
  - posebno Android
- Ne koristiti aplikacije ili “dućane aplikacija” treće strane

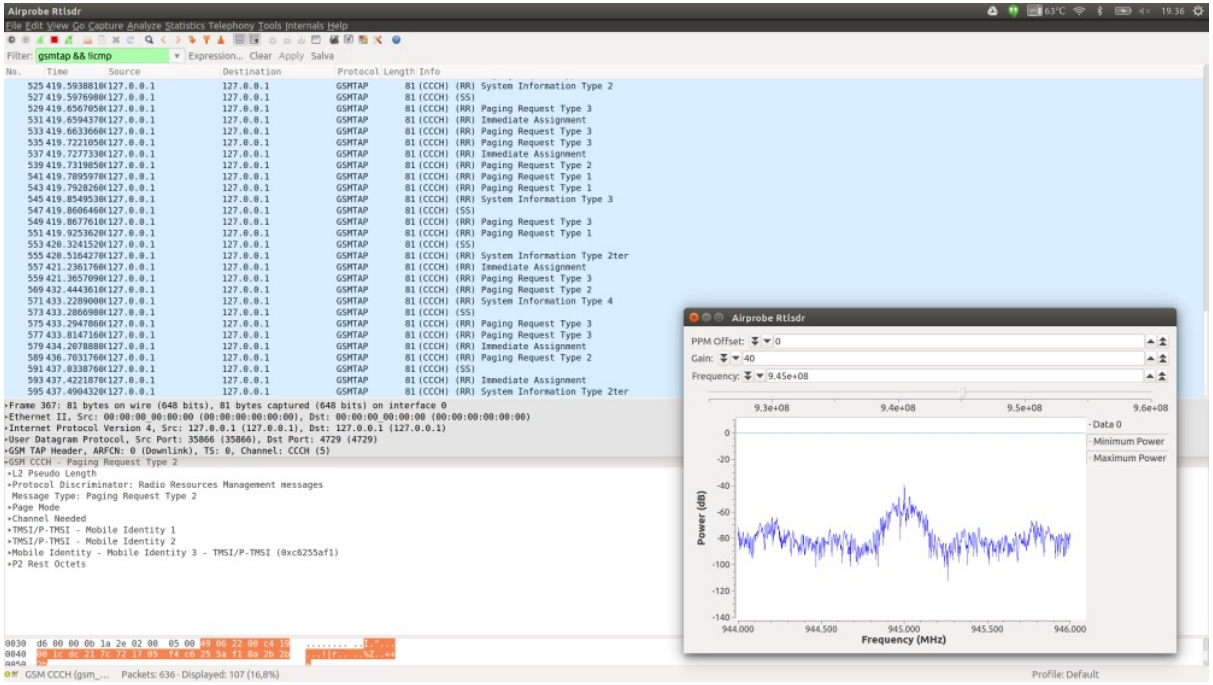
- Što je s tvrtkama?
  - BYOD (*Bring Your Own Device*) politika
    - postoji već dugo za prijenosna računala, sada popularna i za pametne telefone
  - Kako osigurati da “doneseni” privatni uređaji korisnika nisu rizik za informacijsku sigurnost tvrtke?
    - Kontejnerizacija (*containerization*)

Kontejnerizacija

- virtualna particija na pokretnom uređaju
  - na njoj se nalaze osjetjive aplikacije i podaci
  - *sandboxing* aplikacija
    - sjetimo se predavanja o operacijskim sustavima, virusima i crvima!
  - šifrirani podaci
- Uređaj ima profile
  - npr. obični i sigurni
  - nije moguće prebacivati podatke iz jednog u drugi
- Platforme
  - Apple iOS
    - standardno podržava na razini uređaja jer je tako izveden sustav
  - Android
    - potrebno instalirati dodatne platfrome
    - Knox (Samsung), Divider

Prisluškivanje mobilnog prometa?

- Uređaji SDR – *Software Defined Radio*
  - Npr. HackRF One
- Signalizacija i komunikacija – odvojeno!



... i što nas čeka u 2022.?

- širenje malware svih vrsta
  - ransomware
  - povećenje financijskih gubitaka
  - “malware će postati unosan posao na mobilnim platformama”
  - najviše prijetnji na Androidu
- top-lista prijetnji
  - širenje phishinga na mobilne uređaje
    - zbog sve više pametnih telefona
  - premium SMS/poziv prevare
  - botneti
    - očekuje se značajan rast aktivnih botneta
  - “rupe” u operacijskim sustavima
    - npr. *keylogger* na Apple uređajima