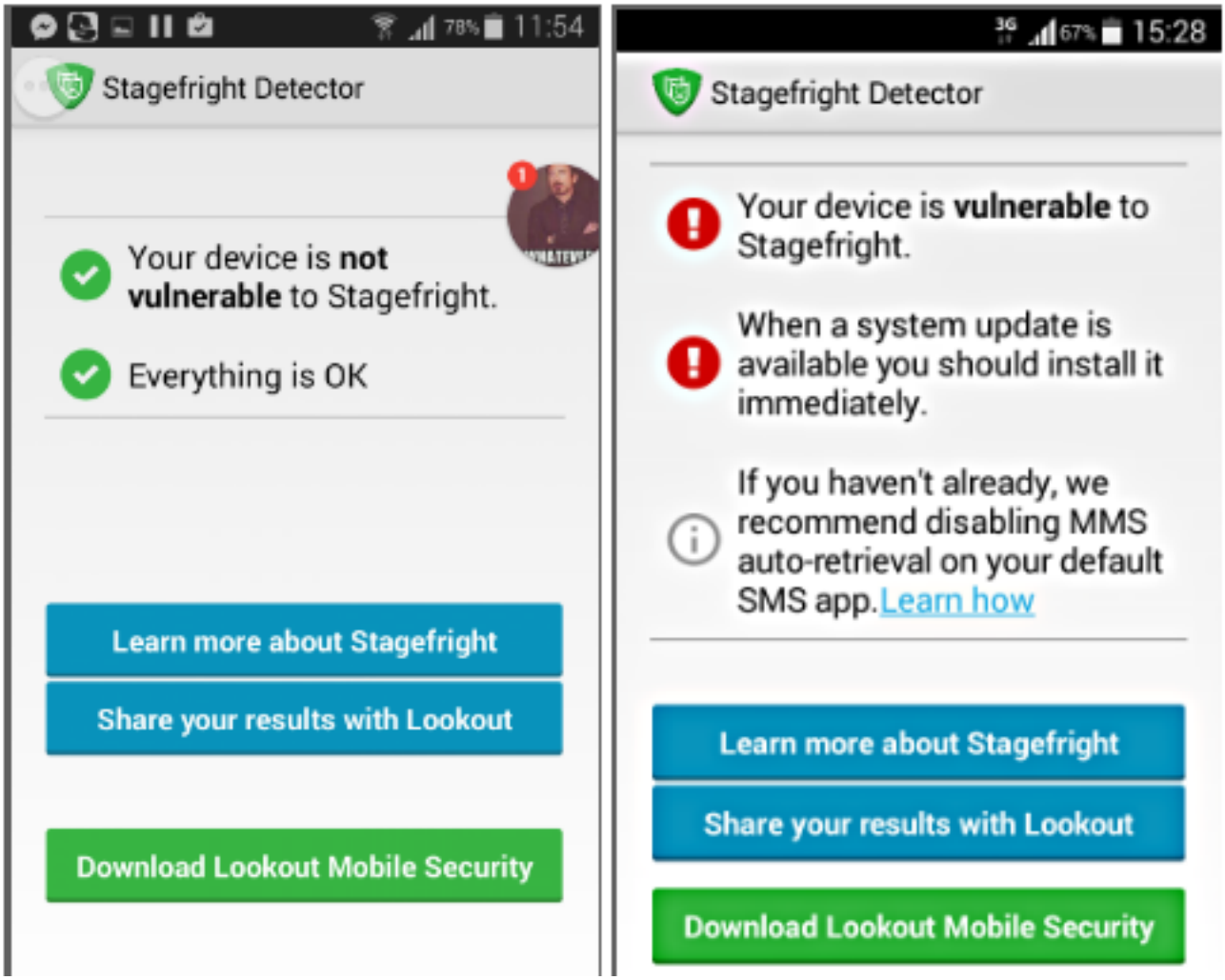
Android uređaji – samo je nesigurnost sigurna!

Procjena je, i to suzdržana, da Android pogoni preko dvije milijarde aktivnih mobilnih uređaja. S uzlaznim trendom rasta. Na tim uređajima korisnici drže osobne i službene podatke. Marshmallow, AOS sa značajno unaprijeđenim sigurnosnim značajkama u odnosu na prethodne verzije, nalazi se na kojih 8% tih uređaja.

Kritična ranjivost svih verzija Android operativnog sustava ispod Marshmallowa, uočena sredinom prošle godine, imenovana kao Stagefright - vidi https://en.wikipedia.org/wiki/Stagefright_(bug) [1] - na spektakularan je način potvrdila dijagnoze "katastrofičara" da je sigurnosna dimenzija AOS-a u velikom raskoraku s njegovom popularnošću. Naime, poput svakog kompleksnijeg softvera, neotporan je na mnoge vrste napada, a najgore je to što je logistika za efikasno otkrivanje i zatvaranje sigurnosnih rupa na embrionalnom razvojnom stupnju, jer ne surađuju oni koji mogu i moraju dati svoj doprinos, prvenstveno Google i tehnološki napredniji proizvođači uređaja.

Ono što je crv Sasser bio za Microsoft - okidač za sistematično bavljenje sigurnošću Windows OS-a - Stagefright je za kolovođe Android paradigme, Google i partnere. Što samostalno što surađujući, počeli su se ozbiljnije baviti raznim aspektima zaštite Android uređaja – (re)analizira se kod, otkrivaju se ranjivosti, objavljuju zakrpe... no i nadalje je primjena zakrpi za već objelodanjene ranjivosti nedopustivo spora, vremenski intervali mjere se u mjesecima. Također, poražavajuće je to što razne zločestobe mogu i danas, gotovo godinu dana od pojavljivanja Stagefrighta na svjetskoj sceni, u miru razvijati exploite (programski kod i metode) za iskorištavanje ove ranjivosti! Narednom ćemo slikom ilustrirati zašto. Na prvom je ekranu Galaxy S5 sa izvornim AOS-om 5.1.1, drugi je ekran skinut sa Galaxy S4 kojime upravlja izvorni AOS 4.4.4.

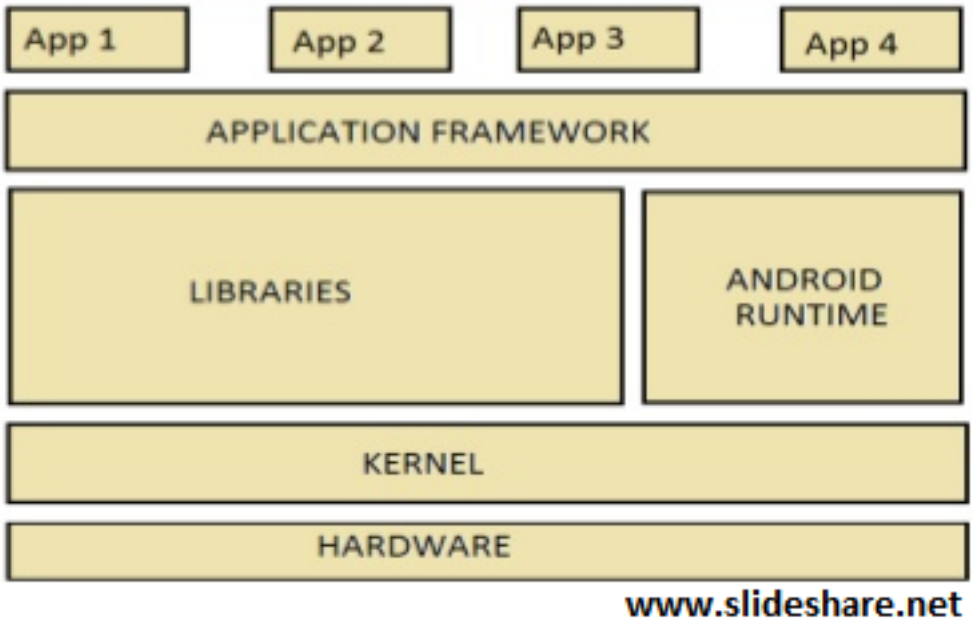


Slika otkriva tipičnu situaciju: Samsung je procijenio da mu se isplati pokrpati S5, a korisnicima S4 modela diskretno je poručio da si nabave noviji model ako se žele riješiti Stagefrighta. Podsjećamo da se je kod nas Galaxy S4 prodavao i 2015. godine, dakle, ne radi se o zastarjelom modelu. Bome, nit' jeftinom. Samsungov, recimo jasno – nekorektan - pristup primjenjuju i drugi razvikani proizvođači Android uređaja. Lako je stoga pretpostaviti u kakvoj su nezavidnoj situaciji vlasnici Android spravica proizvedenih od strane brojnih malih kuća. Uglavnom, eto zašto je Stagehfight i danas jako zanimljiv cyber podzemlju, naime, na terenu je trenutno barem milijarda uređaja koji nikada neće primiti anti-Stagefright zakrpu! Niti zakrpe novijeg datuma.

Deklarativno, kompletna elita Android industrije radi u interesu svojih kupaca, otvorili su web mjesta posvećena ranjivostima i ažuriranjima, ponešto i zakrpaju... napredak je vidljiv, ali ne drži korak sa ozbiljnošću situacije. Upućeni u problematiku tvrde da 97% aktivnog malwearea za mobilne uređaje otpada na Android platformu, također, smatra se da „olovna vremena“ tek dolaze zbog kontinuiranog porasta značaja mobilnih uređaja u sferi poslovanja, od SOHO do enterprise razine.

Pregledamo li Googleov repozitorij ranjivosti objavljenih unazad godinu dana na adresi https://source.android.com/security/bulletin/ [2], uočit ćemo njihovu prisutnost u svim slojevima AOS. Također, steći ćemo dojam da stanje i nije tako loše jer, eto, ranjivosti se otkrivaju, zakrpe objavljuju.... Nažalost, zbog općepoznatog sindroma fragmentacije Androida napori Googleovog tima ograničenog su dometa, odnose se samo na izvorni (vanilla) AOS. Poznato je da proizvođači izrazito prerađuju Application Framework i Libraries slojeve (vidi nižu sliku) stvarajući time vlastitu varijantu iste verzije AOS-a. Analitičari koda upozoravaju da su spomenuta dva sloja u sigurnosnom smislu neuralgična točka. Prvi je razlog navada da se nove funkcionalnosti dodaju a nepotrebne ne uklanjaju pa u konačnici dobijamo AOS instalaciju s talogom suvišnog koda koji se može zlorabiti, i slabo ispitanom instancom aktivnog koda. Drugi je razlog što se bugovi u nekim modulima Android Frameworka, poput WebKit i Chromium renderera web stranica, ne mogu krpati selektivno nego samo *flashanjem* novog firmwarea, što dramatično povećava tzv. *response time* na otkrivenu

ranjivost.

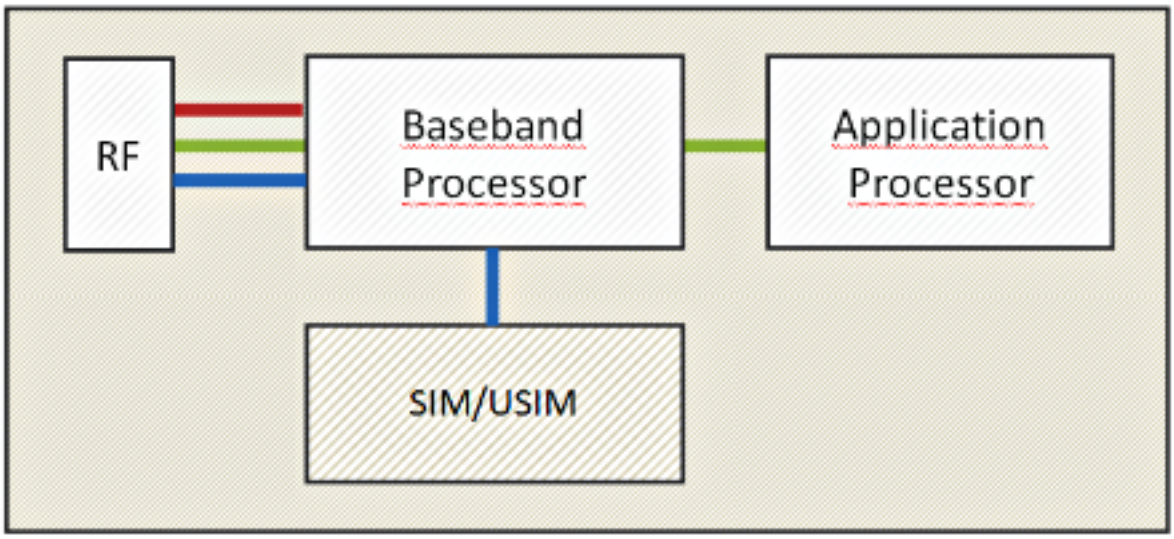


Što se tiče aplikativnog sloja, stanje je toliko zapetljano da je to teško opisati. Podsjetimo se samo da se na tipičnom Android uređaju nalaze predinstalirane aplikacije Googlea, proizvođača uređaja i telekoma. Tada dolazi na red korisnik koji instalirava aplikacije po vlastitom izboru, s raznih on-line dućana. Redovito taj korisnik jako voli kad u dućanu naleti na besplatnu aplikaciju ili, još bolje, „besplatnu“ verziju komercijalne aplikacije pa ju, ne sluteći da je u paketu i malware, s veseljem instalira na isti uređaj kojime obavlja bankovne transakcije ili pristupa IT resursima firme...

Upućeni ne dvoje da je većina repozitorija Android aplikacija na Webu pravo mrijestilište malwarea. Domišljate zločestobe uspijevaju nadmudriti čak i Bouncer, Googleovog softverskog inspektora koji traži maliciozni kod u aplikacijama neposredno pred njihovo objavljivanje. Ovdje možemo naći svježi primjer [3]. Jedna od raširenijih tehnika je uspavljivanje zloćudnih rutina sve dok se aplikacija ne instalira na uređaj, ili ih aktivira „ažuriranje“ te aplikacije. Spavanje se primjenjuje i na samom Android uređaju kako bi se zavaralo lokalno antimalware rješenje - trojan se spoji na C-C-Centar, prenese potrebne podatke i potom se deaktivira do iduće prigode.

Programeri Android aplikacija, uočeno je, koncentriraju se na funkcionalni i estestki aspekt svojih uradaka, sigurnosni je aspekt nisko na ljestvici prioriteta. S druge strane, hackeri jako vole klijentske aplikacije koje u pravilnim intervalima automatski povlače podatke sa Internet servera kako bi ih potom prezentirale korisniku kao notifikaciju ili konkretan sadržaj. Eto, na znanje i ravnanje! :-)

U specifikacijama Android uređaja neizostavno se spominju glavni (aplikacijski) i grafički procesori te verzija AOS-a, nećemo naći informaciju o tzv. baseband procesoru i njegovom operativnom sustavu. Taj modul – poznat je i kao radio modem - ima svaki uređaj koji se spaja na mobilnu mrežu (cellular network) jer upravo on obrađuje sve podatke što se generiraju na glasovnoj i podatkovnoj vezi – od spajanja na baznu stanicu preko odlaznih i dolaznih poziva i tekstualnih poruka... do uobičajene Internet komunikacije. Aplikativni front-end baseband modula poznat je kao Radio Interface Layer (RIL). Na nižoj slici vidimo da baseband modul prosljeđuje zaprimljene i obrađene podatke ključnim komponentama poput aplikacijskog procesora i SIM kartice.



Gornji kratak opis bio je potreban kako bi se stekla jasnija predodžba o još jednoj površini napada (attack surface) i to vrlo atraktivnoj jer ako uljez ovlada baseband modulom, može korisniku zadati dosta glavobolje a ujedno dobija priliku penetrirati u AOS i njegove aplikacije. Već su poznati napadi na toj razini, tipični su oni tipa Rogue Base Station i DNS spoofing jer se hackeri uspijevaju okoristiti propustima u arhitekturi i/ili implementaciji mobilnih komunikacijskih protokola. Za potrebe ovog članka važno je uočiti da se eventualne ranjivosti u baseband softveru (OS i RIL) ne mogu otkloniti selektivnim ažuriranjima nego samo flashanjem nove verzije firmwarea. Tako da opet imamo veliki raskorak između otkrivanja i krpanja ranjivosti, ako do čina krpanja uopće ikada dođe!

I SIM kartica ima svoj operativni sustav te, posljedično, specifične ranjivosti. Nipošto bezazlene, slijedi „kratki & slatki“ primjer: https://www.quora.com/Can-an-attacker-hack-my-SIM-card-like-this [4].

Nema dvojbe, pred Googleom i partnerima velik je posao. Kako to već biva u poslovno-prihodovnoj sferi, posebno onoj internacionalnih razmjera, jako je teško uskladiti partikularne i kratkoročne interese sa zajedničkima i dugoročnima. Do sada su dominirali prvospomenuti ali, srećom, postoji jedan važan razlog za intenziviranje suradnje, ime mu je Android for Work. Sve dok ne dosegne višegodišnji Lifecycle Support i nizak response time na uočene ranjivosti, Android se ne može i neće tretirati kao zrela, pouzdana tehnologija za primjenu u iole zahtjevnijim poslovnim okruženjima. A Google & Co imaju goleme aspiracije u tom smislu.

pon, 2016-06-27 21:01 - Ratko Žižek**Vijesti:** Sigurnost [5]
Kategorije: Operacijski sustavi [6]
Vote: 0

No votes yet

Source URL: https://sysportal.carnet.hr/node/1657

Links
[1] https://en.wikipedia.org/wiki/Stagefright_(bug)

[2] https://source.android.com/security/bulletin/
[3] http://www.theregister.co.uk/2016/02/29/worlds_worst_android_play_store_attack_sends_millions_to_p0rn_sites/
[4] https://www.quora.com/Can-an-attacker-hack-my-SIM-card-like-this
[5] https://sysportal.carnet.hr/taxonomy/term/13
[6] https://sysportal.carnet.hr/taxonomy/term/26