EFF'S SURVEILLANCE SELF-DEFENSE

SIMU ZA MKONONI: PROGRAMU HASIDI

https://ssd.eff.org/en/about-surveillance-self-defense

ELECTRONIC FRONTIER FOUNDATION

LOCALIZATION LAB

Programu hasidi

Simu zinaweza kuathiriwa virusi na aina nyingine za programu hasidi, kwa sababu mtumiaji alidanganywa ili kusakinisha programu hasidi, au kwa sababu mtu fulani aliweza kudukua kifaa kwa kutumia hitilafu ya usalama katika programu iliyopo ya kifaa. Kama ilivyo kwa aina nyingine za vifaa vya kompyuta, programu hasidi inaweza kupeleleza mtumiaji wa kifaa.

Kwa mfano, programu hasidi kwenye simu ya mkononi inaweza kusoma data ya binafsi kwenye kifaa (kama vile ujumbe wa maandishi uliohifadhiwa au picha). Programu hasidi inaweza kufanya hili kwa kutumia dosari ya usalama, kama vile mfumo wa uendeshaji wa simu uliopitwa na wakati. Inaweza pia kuwezesha vitambuzi vya kifaa (kama vile maikrofoni, kamera, GPS) ili kupata mahali simu ipo au kufuatilia mazingira, baadhi ya programu hasidi zina uwezo wa kubadilisha simu kuwa kifaa cha kusikiliza au cha ufuatiliaji kwa kuwasha kamera au maikrofoni kisiri. Programu hasidi pia inaweza kutumika kusoma maudhui ya huduma za ujumbe uliosimbwa kwa njia fiche kama vile Mawimbi au Whatsapp wakati ujumbe kama huo haujasimbwa kwenye simu kwa ajili ya kusoma au kuandika.

Kwa maelezo zaidi, angalia Je, Ninawezaje Kujilinda dhidi ya Programu hasidi?

Serikali zenyewe mara nyingi hukataza watu, hata wafanyakazi wa serikali, kubeba simu za binafsi katika vituo fulani nyeti—hasa kwa kuzingatia wasiwasi kwamba simu hizo zinaweza kuwa na programu hasidi ili kuzifanya zirekodi mazungumzo.

Kama tulivyojadili hapo juu, tahadhari zinazotokana na kuzima simu zinaweza kutambuliwa na kampuni ya huduma za mawasiliano; kwa mfano, watu kumi wakisafiri kwenda kwenye jengo moja na kisha wote wazime simu zao kwa wakati mmoja, kampuni ya huduma za mawasiliano, au mtu anayechunguza rekodi zake, anaweza kuhitimisha kwamba watu hao wote walikuwa kwenye mkutano mmoja na kwamba washiriki walizingatia mkutano huo kuwa nyeti. Hii itakuwa ngumu kugundua ikiwa washiriki walikuwa wameacha simu zao nyumbani au ofisini.

Faida na Hasara za Kuzima Simu Yako

Kuna wasiwasi mkubwa kwamba simu zinaweza kutumika kufuatilia watu hata wakati hazitumiwi kupiga simu. Kwa hivyo, watu wanaofanya mazungumzo nyeti wakati mwingine huambiwa wazime simu zao kabisa, au hata watoe betri za simu zao.

Pendekezo la kutoa betri huonekana kulenga hasa kuwepo kwa programu hasidi ambayo hufanya simu ionekane kuwa imezimwa ombi hilo linapotumwa (hatimaye kuonyesha skrini tupu tu), huku ikibaki ikiwa imewashwa na kuweza kufuatilia mazungumzo au kupiga au kupokea simu bila kuonekana. Kwa hivyo, watumiaji wanaweza dhani kuwa walikuwa wamezima simu zao lakini hawakuzizima. Programu hasidi kama hizo zipo, angalau kwa vifaa vingine, ingawa tuna taarifa ndogo kuhusu jinsi zinavyofanya kazi au zimetumika kwa kiwango gani. Pia, kwa ujumla ni vigumu zaidi kutoa betri kutoka kwa simu mahiri kwa sababu ya miundo mipya iliyo na kipochi cha nyuma na skrini ya mbele ambazo ni ngumu kutenganisha kwa kutumia mkono tu (na inaweza kubatilisha dhamana).

Njia nyingine ya kuzuia mawimbi kwenda kwa simu ni kutumia vizimba vya Faradayau mifuko. Hata hivyo, mifuko ni ya bei nafuu zaidi na ya vitendo. Hizi husaidia kuzuia mawimbi kufikia simu ikiwa kwenye begi, hata kama kifaa kimeathirika. Ishara hizi ni pamoja na 2G, 3G, 4G, 5G, Bluetooth, WiFi na GPS.

Simu ya Kutupa Baada ya Kutumia kwa Muda Mfupi.

Simu zinazotumiwa kwa muda mfupi na kisha kutupwa mara nyingi hujulikana kama Simu ya kutupa baada ya kutumia kwa muda mfupi.. Watu wanaojaribu kuepuka ufuatiliaji wa serikali wakati mwingine hujaribu kubadilisha simu (na nambari za simu) mara kwa mara ili iwe vigumu zaidi kutambua mawasiliano yao. Watahitaji kutumia simu za kulipia kabla (zisizohusishwa na kadi ya binafsi ya mkopo au akaunti ya benki) na kuhakikisha kwamba simu na kadi zao za SIM hazikusajiliwa kwa kutumia utambulisho wao; katika baadhi ya nchi hatua hizi ni za moja kwa moja, ilhali katika nyingine kunaweza kuwa na vikwazo vya kisheria au vitendo vya kupata huduma ya simu ya mkononi bila usajili.

Kuna idadi ya mapungufu kwa mbinu hii.

Kadi za Simu

Kwanza, kubadilisha tu kadi za SIM au kuhamisha kadi za SIM kutoka kwa kifaa kimoja hadi kingine hutoa ulinzi mdogo, kwa sababu mtandao wa simu hufuatilia kadi ya SIM na kifaa pamoja. Kwa maneno mengine, kampuni hiyo ya huduma

za mawasiliano hujua historia ya ni kadi gani za SIM zimetumika katika vifaa gani na inaweza kuzufuatilia vitofauti au zote kwa pamoja. Pili, serikali zimekuwa zikiunda mbinu za uchanganuzi wa eneo la simu ambapo ufuatiliaji wa eneo unaweza kutumika kutengeneza miongozo au nadharia tete kuhusu iwapo vifaa vingi ni vya mtu mmoja. Kuna njia nyingi hii inaweza kufanywa. Kwa mfano, mchanganuzi anaweza kuangalia ikiwa vifaa viwili vilikuwa vikisonga pamoja, au ikiwa, hata kama vilitumika kwa nyakati tofauti, vilionyesha kubebwa kwenye maeneo sawa.

Ujumbe kuhusu teknolojia ya eSIM (SIM iliyopachikwa), au kadi za SIM za programu. Hiki ni kipengee kilichopachikwa kwenye simu ambacho humpa mtoa huduma wa mtandao uwezo wa kuongeza au ‘kutoa’ wasifu wa SIM Mtandaoni (OTA).

Miundo ya Ufuatiliaji na Simu za Kutupa Baada ya Kutumia kwa Muda Mfupi

Tatizo lingine kwa mafanikio ya utumiaji wa huduma za simu bila usajili ni kwamba mifumo ya watu kupiga simu huwa ya kipekee sana. Kwa mfano, unaweza kuwapigia simu watu wa familia yako na wafanyakazi wenzako. Ingawa kila mmoja wa watu hawa hupokea simu kutoka kwa watu mbalimbali, kuna uwezekano kuwa wewe ndiye mtu pekee ulimwenguni ambaye huwapigia simu wote wawili kwa kutumia nambari sawa. Kwa hivyo hata ikiwa ulibadilisha nambari yako ghafla, ikiwa uliendelea na mtindo ule ule wa simu ulizopiga au kupokea, itakuwa rahisi kuamua ni nambari gani mpya ilikuwa yako. Kumbuka kwamba makisio haya hayajafanywa kwa kuzingatia tu ukweli kwamba ulipiga nambari moja mahususi, bali juu ya upekee wa mseto wa nambari zote ulizopiga. (Kwa hakika, shirika la *The Intercept* liliripoti kuwa mfumo wa siri wa serikali ya Marekani unaoitwa PROTON hufanya hivyo hasa, kwa kutumia rekodi za simu kutambua watu waliopiga simu kwa “njia sawa na walengwa mahususi” kutoka kwa nambari mpya za simu.) Mfano wa ziada unaweza kupatikana. kwenye hati ya FOIA ya Hemisphere. Hati hii inaelezea hifadhidata ya Hemisphere (hifadhidata kubwa ya rekodi za simu za kihistoria) na jinsi watu wanaoiendesha wana kipengele kinachoweza kuunganisha simu za kutupa baada ya kutumia kwa muda mfupi kwa kufuata ufanano wa mifumo yao ya simu. Hati hii inarejelea simu za kutupa baada ya kutumia kwa muda mfupi kama "simu zilizotupwa" kwa sababu mtumiaji wake "atatupa" moja na kuanza kutumia nyingine—lakini algoriti za uchanganuzi wa hifadhidata zinaweza kuonyesha muunganisho kati ya simu moja na nyingine hali hii inapotokea, mradi simu zote mbili zilitumika kupiga au kupokea simu kwa seti sawa za nambari za simu.

Kwa pamoja, ukweli huu unamaanisha kuwa utumiaji mzuri wa simu za kutupa baada ya kutumia kwa muda mfupi ili kujificha dhidi ya ufuatiliaji wa serikali

unahitaji, angalau: kutotumia tena kadi ya SIM au vifaa; kutobeba vifaa tofauti pamoja; kutounda ushirikiano wa kimwili kati ya mahali ambapo vifaa tofauti hutumiwa; kutotumia simu ya kutupa baada ya kutumia kwa muda mfupi kama suluhisho la muda mrefu; na kutopiga simu au kupigiwa simu na watu wale wale wakati wa unatumia vifaa tofauti. (Hii si lazima iwe orodha kamili; kwa mfano, hatujazingatia hatari ya ufuatiliaji wa kimwili wa mahali simu iliuzwa, au mahali ilipotumiwa, au uwezekano wa programu kutambua sauti ya mtu fulani kama njia ya kiotomatiki ya kuamua ni nani anayezungumza kupitia simu fulani.)

Uchanganuzi wa Simu na Simu Zilizochukuliwa na Mamlaka za Kisheria

Uchanganuzi wa Kisayansi wa Simu Zilizochukuliwa na Mamlaka za Kisheria

Kuna utaalamu uliokuzwa vizuri wa uchanganuzi wa kisayansi vifaa vya mkononi. Mchanganuzi mtaalamu ataunganisha kifaa kilichochukuliwa na mamlaka ya kisheria na mashine maalum, ambayo husoma data iliyohifadhiwa ndani ya kifaa hicho, ikiwa ni pamoja na rekodi za shughuli za awali, simu, picha, ujumbe wa Whatsapp, historia ya eneo, data ya programu na ujumbe wa maandishi. Uchanganuzi wa kisayansi unaweza kupata rekodi ambazo mtumiaji hakuweza kuona au kufikia kwa kawaida, kama vile ujumbe wa maandishi uliofutwa, ambao unaweza kurejeshwa. Uchanganuzi wa kisayansi wakati mwingine unaweza kufungua skrini zilizofungwa zilizolindwa na nambari ya siri, haswa kwenye simu za zamani.

Kuna programu nyingi za simu razini na vipengele vya programu ambavyo hujaribu kuzuia uchanganuzi wa kisayansi wa data na rekodi fulani, au kusimba data kwa njia fiche ili kuifanya isisomeke kwa mchanganuzi. Kwa kuongeza, kuna programu ya mbali ya kuifuta, ambayo huruhusu mmiliki wa simu au mtu aliyechaguliwa na mmiliki kutuma ombi kwa simu ili ifute data fulani. Hata hivyo, si njia zote za kufuta ni sawa na zinaweza kuzuiwa, hasa ikiwa mhusika aliyeteuliwa anahitaji ufikiaji wa mbali kwa simu ili kuifuta.

Programu hii ya zana tepe inaweza kuwa muhimu kulinda data dhidi ya kupatikana ikiwa simu yako imechukuliwa na wahalifu. Hata hivyo, tafadhali kumbuka kuwa uharibifu wa kimakusudi wa ushahidi au kizuizi cha uchunguzi unaweza kushtakiwa kama uhalifu tofauti, mara nyingi huwa na matokeo mabaya sana. Katika baadhi ya matukio, hii inaweza kuwa rahisi kwa serikali kuthibitisha na kuruhusu adhabu kubwa zaidi kuliko uhalifu unaodaiwa kuchunguzwa hapo awali.

Uchanganuzi wa Kompyuta wa Miundo ya Matumizi ya Simu

Serikali pia zimekuwa na nia ya kuchanganua data kuhusu simu za watumiaji wengi kwa kompyuta ili kupata mifumo fulani kiotomatiki. Mifumo hii inaweza kumruhusu mchanganuzi wa serikali kupata matukio ambapo watu walitumia simu zao kwa njia isiyo ya kawaida, kama vile kuchukua tahadhari mahususi za faragha.

Mifano michache ya mambo ambayo serikali inaweza kujaribu kubaini kutokana na uchanganuzi wa data: kubaini kiotomatiki ikiwa watu wanafahamiana; kugundua wakati mtu mmoja anatumia simu nyingi, au kubadili simu; kugundua wakati vikundi vya watu vinasafiri pamoja au kukutana mara kwa mara; kugundua wakati vikundi vya watu vinatumia simu zao kwa njia zisizo za kawaida au za kutiliwa shaka; kubainisha vyanzo vya siri vya mwandishi wa habari.

Aina hizi za uchanganuzi kulingana na muundo zimekuwa rahisi sasa kwa kuwa watu wengi wanamiliki simu mahiri na kwa hivyo mifuko yao imejaa vihisi na moduli zinazowasiliana na aina nyingi za data. Ni kila mtumiaji pekee anayeweza kufafanua mtindo wake wa hatari na tunawahimiza watumiaji kutathmini hatari zao za binafsi na hatua wanazoweza kuchukua ili kujilinda.

Taarifa zaidi

- Kuhudhuria Maandamano
- Mambo ya Kuzingatia Unapovuka Mpaka wa Marekani