Lokalizace T-mobile SIM karet

Vložil/a eldis [1], 11 Leden, 2006 - 23:56

- Anonymita [2]
- Security [3]

Článek použitelný v praxi informující o možnostech lokalizace mobilního telefonu i v případě, že se nejedná o váš mobil.

Tak na začátek trochu teorie

Tato metoda je zcela “oficiální” až na to že my ji využijeme nelegálně. A jak vlastně může operátor zjistit polohu mobilního telefonu ve své síti? Když si představíme model dnešní bezdrátové sítě, tak tady v podstatě máme hromadu přístupových bodů (BTS stanice) vysílající v pásmu 1800MHz což je Evropský standart (v Americe se využívá 1900MHz ale podstata je stejná). Na BTS se připojují klienti pomocí mobilních telefonů. Komunikace je oboustraná - díky tomu můžeme odpovídat, ne jako u rádia nebo televize. A vzhledem k tomu že mobil je věc malá, tudíž není příliš prostoru pro anténu a kmitočet na kterém probíhá komunikace je poměrně vysoký, signál nekopíruje tak dobře terén, je snadněji ovlivnitelný překážkami a rušením. To se sice částečně kompenzuje vyšším vyzářeným výkonem BTS, ale díky normám se operátoři musí krotit (jinak by jste si mohli na okně paneláku smažit vajíčka) díky těmto i jiným nepříznivým vlivům je zapotřebí dostatečně velké množství BTS, zvláště pak v hustě osídlených oblastech kde se navíc musí brát v potaz počet připojených uživatelů. Neřeknu vám přesně kolik vysílačů pokrývá například Prahu, ale pravděpodobně je to víc než si myslíte :). A od toho se také odvijí problém s přesnou pozicí hledaného mobilu. Obecně platí, že čím více BTS je v dosahu, tím přesnější je lokalizace. Takže to máme první parametr, operátor ví ke kterým stanicím jsme připojeni, také jak kvalitní na ně máme signál a jak dlouho trvá než k mobilu informace od BTS a zpět dorazí (v podstatě jako ping) díky tomu vypočítá přibližný okruh kde se může mobil nacházet. T-mobile udává přesnost v hustě osídlených oblastech v řádech desítek metrů, ve vesnicích a málo zalidněných oblastech toleranci až několik kilometrů. Typická přesnost je tak 100m. Takže to bysme měli technologii, ale jak je to z právního hlediska? Operátor nemůže každému kdo si o to řekne sdělit polohu jeho zákazníka, stejně jako vám neřekne co kdo psal v sms. Avšak existují výjjimky, jako například policie, ale ani oni nemůžou jen tak kontrolovat koho si zamanou, každý případ by MĚL být odůvodněný, stejně jako odposlechy. Takže jak je možné, že si může legálně zjišťovat zaměstnavatel polohu svích zaměstnanců? Jednoduše, stačí aby s tím souhlasili. A na tom je založená celá služba „Kde je …“ kterou poskytuje T-mobile a proto je také nutné znát LPIN hledaného čísla a je nutné aby na něm byla služba aktivní. Na začátek si musíme ujasnit pár věcí, například:

a) zdali má naše oběť vůbec t-mobile
b) využívá t-zones
c) zdali můžeme alespoň na 5 minut získat přístup k jeho telefonu

Pokud se jedná o obyčejného Frantu uživatele který ví že se s mobilem dají odesílat sms a volat, a jeho maximem bylo že přišel na to jak se dají posílat sms z netu, máme ulehčenou práci. Můžeme postupovat více cestami, jako příklad uvedu dvě. Bezpečněší pro nás ale zároveň trošku obtížnější je metoda, kdy vůbec nebudeme potřebovat mobil oběti, stačí její účet na t-zones.

První metoda, uživatel je již registrován u t-zones

Jako první bude zjištění hesla, způsob nechám na vaši fantazii, například se můžete pokusit o náhodné zadání, keylogger, nebo pokud je připojen přes wifi nebo je v nějaké LAN síti můžete využít

sniffer, sociální inženýrství, falešný login nebo exploit, či snad poprosit ho jestli vám heslo neřekne dobrovolně? :) Dále je možno heslo na t-zones požadavkem přenastavit, ale o tom více v druhé metodě.

Druhá metoda, máme jeho telefon

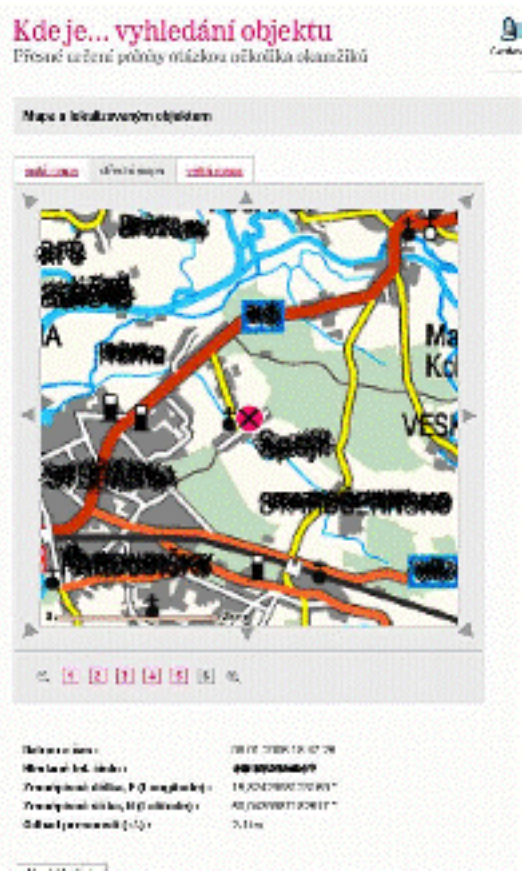
Takhle to půjde mnohem rychleji, a nemusíme se bát potvrzovacích zpráv, neboť je po sobě smažeme. V případě že už je registrován do t-zones, není důvod se pachtit s jeho heslem, můžete mu ho s pomocí telefonu změnit. Stačí následovat instrukce na t-zones. Pokud není zaregistrován, není nic snažšího než ho zaregistrovat ;) pokud namítáte, že pro registraci je potřeba PUK2 (resp. Myslím že jenom jeho první 4 číslice) není problém ho hovorem na infolinku získat, operátorka vám ho ráda sdělí (ověřeno) takže když už jsme úspěšně zaregistrováni, jdeme dále.

Cesta otevřena

Počítám že jste se nakonec k heslu dopracovali, takže bude následovat samotné zapnutí služby “Kde je” ta se dá nalézt po úspěšném přihlášení na www.t-zones.cz [4] v záložce “informace” => “Kde je …” Systém se vás dotáže na telefoní číslo a takzvaný LPIN. Toto zatím ignorujte, o kousek níže je na stránce odkaz na nastavení LPINu, což je vlastně 8-místné heslo které se teprve musí nastavit, takže si zvolte nějakou kombinaci čísel. VYPNĚTE notifikaci (jinak by měl přehled o tom že byl vyhledáván) a zaškrtněte “povolit lokalizaci”. Tím byla úspěšně služba aktivována a bude následovat informační zpráva na mobil oběti. (v případě že máte jeho telefon jste teď v pohodě a dalších pár řádků vás nemusí trápit) S tím bohužel nic nenaděláte, takže to prostě musíte překousnout a doufat že oběť bude tuto zprávu chápat jako omyl (skoušel jsem zatím 3 lidi, a nikomu to nevrtá hlavou), což je pravděpodobné vzhledem k obsahu zprávy která bude:”T-mobile:Vazeny zakazniku, na Vasi zadost jsme Vam aktivovali sluzbu Kde je … s temito parametry:Povoleni lokalizace Ano, Notifikace Ne.”. Nebo se to můžete pokusit urovnat, pomáhá například z jeho účtu odeslat sms na jeho vlastní číslo s obsahem typu “omlouváme se zákazníkům za drobnou poruchu sítě, veškeré obdržené systémové systémové zprávy za posledních 24 hodin byly poslány z důvodu chyby interního systému. Děkujeme za pochopení, váš T-mobile” ale neposílejte mu to ihned, dejte aspon 1 hodinu mezeru nebo tam napište neco lepšího, v socialním inženýrství nejsem zrovna dobrej ;). No a odteď můžete bez vědomí majitele SIM karty zjišťovat jeho momentální polohu ;) to se dá buďto na webu (uvidíte ho na přehledné mapě) nebo pomocí SMS (postup popsán na t-zones, stejně tak jako přístup přes wap a účtování) a těď taková třešnička na dortu. Služba je sice zpoplatněna (tušim 4,70Kč za jedno dohledání), ale když budete lokalizovat přes t-zones z jeho vlastního účtu, poplatky zaplatí on.

Závěr

Pokud máte nějaké dotazy, či snad jsem něco uvedl špatně nebo neúplně, dejte vědět, opravím to. Na konec uvádím screenshot ze služby "Kde je …".



[5]

URL článku: https://security-portal.cz/clanky/lokalizace-t-mobile-sim-karet

Odkazy:
[1] https://security-portal.cz/users/eldis
[2] https://security-portal.cz/category/tagy/anonymita
[3] https://security-portal.cz/category/tagy/security
[4] http://www.t-zones.cz
[5] http://www.security-portal.cz/img/clanky/74/scrshot.jpg