České vysoké učení technické v Praze, katedra telekomunikační techniky
GTS Novera, s.r.o

Technické aspekty realizace podvodů v telekomunikačních sítích

Pavel Troller

Motivace podvodů v telekom. sítích

- Finanční úspora za volání
- Skrytí vlastní identity (telefonní kriminalita)
- Získání přístupu do neveřejných sítí nebo ke speciálním službám
- Přímý zisk (podvody s prémiovými sazbami), podvodní operátoři
- Psychologické pohnutky

Podvody v telekom. sítích

- Zneužití účastnického přístupu (vedení)
- Zneužití slabých míst signalizace
- Zneužití chyb konfigurace systémů (ústředen)
- Záměrné vytváření možností podvodu ("finty")
- Krádež identity a další způsoby u VoIP technologie

Podvádění v přístupové síti

- **Napojení na účastnické vedení**
  - Vyžaduje fyzickou přítomnost u vedení
  - Těžko se prokazuje (účastník musí prokázat, že nevolal on)
  - Venkovní účastnické rozvody k této možnosti mnohdy nabádají
  - Identita útočníka skryta napadeným účastníkem - vhodné např. pro různé druhy telefonní kriminality
- **Podvojné přípojky**
  - Velmi jednoduchý fyzikální princip, umožňují za určitých okolností volat na účet (z linky) podvojného účastníka
  - Tato zranitelnost existuje desítky let, nikdy nebyla seriózně řešena
  - S ústupem podvojných přípojek využitelnost klesá.

Zneužívání telefonních automatů

- **Technickými prostředky**
  - Falešné mince, náhražky
  - Upravené mince (na provázku atd.)
  - Poškození přístroje (vyvrtání otvoru atd.)
  - Falešné telefonní karty
- **Netechnickými prostředky (využití logické, programové chyby)**
  - Trik s příchozím hovorem
  - Trik s tísňovým voláním
  - Další triky

Vzhledem ke snižujícímu se používání VTA ustupuje ztráta těmito druhy podvodu do pozadí.

Nedostatečně zabezpečené bezdrátové technologie

- Staré typy bezšňůrových telefonů - dnes se nepoužívají
- První prototypy mobilních sítí (SELEX, AMR)
- Zneužitelnost sítě NMT (krádež identity bez dostatečné autentikace) – dodatečná instalace tzv. SIS modulu
- Dnes aktuální: Nedostatečně zabezpečené WiFi s VoIP provozem

Podvody v pobočkových ústřednách

- Překonání kategorizace (starší typy PBX)
- Využití nedokonalosti programu nebo konfigurace
- Krádež autorizačního kódu
- Záměrné vytvoření "finty" v PBX správcem nebo hackerem - bývalo velmi časté, vyskytuje se i dnes
- Zneužití DISA provolby (zejména s ukradeným aut. kódem)
- Zneužití IVR systému - hlasová pošta, aut. spojovatelka
- Technické zařízení - aut. propojovač dvou PBX linek – možné i ve veřejné síti

Podvody s využitím signalizace

- Signalizace je třeba pro sestavování a rušení spojení
- Dříve – různé druhy analogových signalizací pro místní, meziměstské a mezinárodní relace
- Nyní – SS7 na všech úrovních PSTN
  - Analogové signalizace mohou přežívat v pobočkových sítích
- Nový fenomén – VoIP signalizace (SIP, H.323...)
  - Nabízí nové možnosti zneužití a využití

Z historie: USA - „barevné boxy“

- Blue box: Zneužití tónové signalizace č. 5 pro bezplatná volání
- Black box: Zajištění bezplatných hovorů pro volajícího (při příchozím hovoru).
- Red box: Umožnění bezplatných hovorů z mincovního telefonního automatu.
- Purple box: Při připojení k běžné lince simuluje kategorii mincovního automatu, vhodné ke skrytí identity (pro praktické využití obvykle třeba ještě Red box)
- Cheese box: Propojuje 2 linky a tím umožnuje různé druhy podvodů (vhodné v kombinaci s Black boxem)
- Silver (gold) box: Zařízení kombinující několik výše uvedených funkcionalit.

„Blue box“

- V podstatě generátor dvojfrekvenční signalizace č. 5
- Princip použití:

  - Běžným způsobem se zavolá na bezplatné číslo přes relaci vedenou signalizací č. 5

  - Pomocí boxu se tónově vyšle signál závěru, čímž vzdálená ústředna zruší volání, místní ústředna ale „o ničem neví“ a dálkový okruh je tedy stále připojen k volajícímu.

  - Pomocí boxu se vyšle signál nového volání, následovaný telefonním číslem a signálem „start“ (požadavek propojení). Toto číslo již není bezplatné, může být mezinárodní, se zvýšeným tarifem, atd. Hovor je vzdálenou ústřednou spojen.

  - Po skončení hovoru se normálně zavěsí. Vzhledem k tomu, že pro místní ústřednu byla manipulace s boxem „neviditelná“, hovor bude vyúčtován stále jako bezplatný.

  - Ti, kteří si nedokázali zkonstruovat nebo zakoupit vlastní Blue Box, si často nechávali nahrát tónové sekvence často volaných čísel např. na kazetu a pak podváděli s pomocí běžného magnetofonu.

- V Evropě se signalizace č. 5 nepoužívala, takže Blue boxy zde šly používat jen velmi omezeně – prostřednictvím zámořských relací na bezplatná čísla, tj. na služby typu „USA Direct“ apod. Nedoznaly zde tedy většího rozšíření.

A co u nás ??

- Místní sítě: Signalizace typu P a K (stejnosměrné, případně s kodem R2), prakticky nenapadnutelné.
- Okrajové místní telefonní obvody: zpravidla bývaly připojeny dvoudrátovými okruhy se signalizací 50 Hz nebo v nadhovorovém pásmu, napadnutelné.
- Meziměstské a mezinárodní okruhy: Kratší příčkové okruhy – dvoudrátové – napadnutelné, delší a tranzitní okruhy – čtyřdrátové – jen zřídka napadnutelné.

Historie: Napadení dvoudrátové jednofrekvenční signalizace

- Používalo se frekvence 50 Hz nebo v nadhovorovém pásmu.
- Dopředným směrem se přenášely volicí impulsy, zpětně signál přihlášení – pro oba směry byla použita stejná frekvence.
- Pokud jedna strana vysílala frekvenci, nebyla schopna ji přijímat.
- Pokud tedy byla vysílána volba v okamžiku přihlášení volaného, signál přihlášení se nepřenesl do volající ústředny a nebyla započata tarifikace hovoru. Toho šlo využít tím, že se opakovaně volilo (nejlépe číslice 0 – 10 pulsů) i po skončení volby čísla až do zjištění, že volaný se přihlásil, nebo se šlo domluvit např. na vyzvednutí během třetího vyzváněcího pulsu a volbu provést v synchronismu.

Možnosti napadení signalizace č.7

- Tato signalizace je dnes nosičem všech informací v klasických pevných i mobilních sítích -> lákavé možnosti
- K této signalizaci se nelze dostat z účastnického přístroje, je třeba mezioperátorské připojení -> značně omezuje možnosti, prakticky vylučuje individuální napadení
- SS7 rozhraní bývá považováno za „trusted“ (důvěryhodné) a nebývají příliš hluboké kontroly -> zvyšuje možnosti napadení
- Známy případy podvodů s masovým rozesíláním SMS v mobilních sítích
- Známy případy záměrného škození (obdoba DoS útoku) zahlcováním signalizace nesmyslnými nebo záměrně škodícími zprávami (např. náhodné ukončování hovorů).

Dnes použitelná metoda: potlačení přihlášení

- Stejný princip jako americký „Black box“, tj. podvodu je dosaženo na straně volaného potlačením signálu přihlášení.
- Nutno mít k dispozici PBX s ISDN nebo CAS připojením a možností softwarových úprav (např. Open Source - Asterisk).
- Zpravidla nutná speciální konfigurace rozhraní i na veřejné ústředně (speciální povolení akustického propojení před přihlášením), neplatí ale pro všechny systémy všech operátorů.
- Dnes jsou v síti implementovány časové kontroly, takový hovor je po 30 – 120 sekundách terminován.
- Vzhledem k výše řečenému je zneužití velmi obtížné, ale z principu technicky možné.

Zneužití chyb konfigurace systémů

Chyby konfigurace mohou způsobit nemalé škody, prakticky většina dnešních podvodů v klasických sítích spadá do této kategorie.

- „Zřetězení prefixů“ - např. 004210084 – chyba směrovací databáze operátora v kombinaci s nesprávně konfigurovaným propojením

- „Tam a zpět“ - např. přes podústřednu nebo PBX – jen u zjevného číslovacího plánu, dnes u nás prakticky vyloučeno vzhledem k povaze číslovacího plánu, ale v jiných zemích dosud běžné

- „Neočekávaný vstup“ - např. použití nedekadických číslic A-D u DTMF, více než deseti pulsů u pulsní volby, velmi dlouhého čísla či (případ z poslední doby) atypického sufixu (***) k číslu atd.

Zneužití zvláštních služeb a zařízení operátora

- Testovací zařízení, při nedostatečném zabezpečení snadno zneužitelná k různým druhům podvodů:

  - Testovací linky a vedení

  - Automatické zkušební zařízení zvonků

  - „Loop-arounds“ - smyčková vedení – bývala oblíbená v USA

- Speciální zařízení, vedení, sítě...

- Bývalé poloautomatické příčky, určené pro spojovatelky – dostup na speciálních číslech, která při jejich znalosti nebyla dále autentikována

- Speciální sítě – např. ZTS/UTS, dostupné přes různé utajované, ale snadno nalezitelné směry, dnes řešeno jako VPN

Historie: Poloautomatické příčky

Určeny pro spojovatelky, s malou kapacitou, nepoužitelné pro automatický provoz

- Na speciálních číslech, která šla poměrně snadno nalézt
- Dostup do lokalit, ještě automaticky nedostupných (např. Praha -> Pieštany přes Trenčín: 983 – 28 – 95 – XXXX
- V koncové ústředně instalovány SPN – Signální přijímače napojení – frekvence 2700 Hz – dala se napodobit např. upravenou píštalkou na psa a pak došlo k napojení do probíhajícího hovoru (hovořící účastníci měli slyšet tzv. napojovací signál, ale mnohdy tato signalizace chyběla).
- V některých zemích (SSSR) bylo použití těchto příček částečně zveřejněno a byly dostupné např. ze speciálních míst (pošty).

Záměrné vytváření „děr“ v síti („Finty“)

- Oblíbené hlavně v minulosti správci PBX, ale i veřejných systémů
- Mnohdy bylo upraveno jiné zařízení, běžně užívané, aby jako „vedlejší efekt“ umožnilo volání zdarma nebo na účet někoho jiného (např. vlastníka PBX)
- Záměrné vytváření možnosti zneužití typu „tam a zpět“
  - Nejjednodušší případ: Do PBX (519) a ihned ven (0) – velmi snadno odhalitelné a zneužitelné, přesto dlouhá léta funkční („Diesel“)
  - Složitější případ: V PBX bylo nutno volit speciální číslo, mnohdy maskované např. falešným obsazovacím tónem (např. 218 – 66 – 0), „Chemička“
  - Obdoba „Cheese boxu“, propojení provolbového přenašeče na běžnou veřejnou linku, které umožnilo volat kamkoliv na účet této linky (dvoustupnová volba s využitím DTMF, na svou dobu neobvyklé)
- Vytváření speciálních prefixů na veřejných ústřednách (např. dlouho funkční prefix „0207“ („Kotěhůlky“), umožnující volat v 80. letech zdarma automaticky do USA, záp. Berlína, na Kubu a do jiných vzácných destinací...
- Dnes: Nejčastěji virtuální provolby, autentikované autorizačními kódy, speciální úpravy zelených čísel (800), callbacky, aktivace pomocí SMS nebo e-mailu či webem.

Zneužití VoIP technologií

- Útoky na infrastrukturu operátorů: Brány médií, registrační servery, proxy
- Odposlech síťového provozu a následný pokus o průnik
- Útoky na VoIP PBX - prostřednictvím VoIP protokolu
- Útoky na administrativní rozhraní systémů a následná změna konfigurace (povolení příjmu a směrování volání z podvodných zdrojů

Zneužití bran médií a obdobných prvků

- Jednodušší brány nemají možnost autentikace a autorizace, pracují v trunkovém režimu
- Obslouží jakýkoliv smysluplný požadavek z libovolné IP adresy
- Vícekanálové brány (např. s rozhraním E1) mohou během hodiny způsobit škodu až stovky tisíc Kč
- Tyto útoky jsou zpravidla organizovány podvodnými operátory, kteří do nalezených bran následně terminují provoz svých zákazníků
- Způsob ochrany: Pokud je brána současně vybavena IP routerem (např. brány Cisco), nastavit IP access list jen na seznam známých IP adres. U jednoduchých bran předřadit router/firewall.
- Vlastní zkušenost: Během testování nového typu brány tato byla objevena do cca 2 hodin od zprovoznění a během 10 dalších minut přes ni začal téci provoz do destinace "Cuba Mobile" - během půl hodiny škoda přes 8000 Kč (naštěstí má tato destinace nízké ASR).

Útoky na registrační servery

- Cílem je krádež identity účastníka a následně volání na jeho účet (a s jeho identifikací)
- Nejčastější princip: Hrubá síla (hádání uživatelského jména a hesla)
- Pokud je uživatelské jméno totožné s tel. číslem, má útočník zjednodušenou práci
- V řadě defaultních konfigurací mají všichni účastníci stejné (a velmi jednoduché) heslo, např. 1234
- Ochrana: Uživatelská jména jiná než tel. čísla (nemusí být podporováno všemi VoIP terminály)
- Silná hesla (některé VoIP terminály však mají jen numerická hesla)
- Maskování důvodu selhání autentikace (špatný userid, špatné heslo atd.) jen jedním obecným chybovým kódem (v rozporu s RFC, ale zvyšuje bezpečnost)

Odposlech provozu a využití získaných dat k útoku

- Monitorováním SIP komunikace lze zjistit např. tel. čísla a toho následně využít při hádání (viz předchozí text)
- Vlastní zkušenost: Cca 15 minut po skončení VoIP hovoru přes WiFi připojení jednoho lokálního operátora započal útok hrubou silou, cca 400 REGISTER požadavků za sekundu, který trval celkem 42 hodin, trvalý datový tok během útoku byl 350 kbit/s
- Pro útok bylo použito dat zjištěných odposlechem (byla simulována SIP hlavička velmi podobná reálnému hovoru)
- Útok trval, přestože registrační server vůbec neodpovídal (patrně šlo o automatizovaný útok bez manuální kontroly)
- Bylo použito nástroje SIPVicious (http://sipvicious.org)
- Útok byl veden z USA, ISP na "abuse e-mail" samozřejmě nereagoval.

Jak se bránit ? - pohled VoIP účastníka

- Používat výlučně silných hesel.
- Pokud operátor podporuje, používat zabezpečenou signalizaci (SIPS), šifrování médií (SRTP) zvýší ochranu před odposlechem, ale nesníží nebezpečí možného útoku
- Pokud operátor podporuje, stanovit poměrně nízký limit na volání - v případě úspěšného útoku a odcizení identity pak nehrozí velká finanční ztráta
- Pravidelně kontrolovat výpis volání, zda se neobjevují hovory neznámého původu a na neznámé destinace.
- U lepších typů VoIP ústředen je možnost využít např. uzamčení účtu PINem v případě, že nebude delší dobu využíván.

Jak se bránit ? - pohled provozovatele VoIP PBX nebo VoIP operátora

- Dbát na (přidělovat) výlučně silné autorizační údaje
- Umožnit šifrovanou a bezpečnou signalizaci (SIPS), např. podporováno v Asterisku 1.6, podpora u terminálů dosud slabší
- Napsat nebo nainstalovat alespoň jednoduchý FDS (Fraud detection system, systém detekce podvodů), který bude kontrolovat hovorové záznamy alespoň na výskyt nejběžnějších příznaků podvodu (prudký nárůst počtu volání, změna charakteru - převážně mezinárodní provoz atd.)
- Pravidelně studovat logy systému, ze kterých lze vyčíst případně probíhající (i dosud neúspěšné) útoky a zabránit jim
- Zamezení tzv. anonymního přístupu bez registrace (což je v rozporu např. s využitím ENUM), případně se ujistit, že je konfigurován ve zcela samostatné kategorii s dostupem výlučně na vlastní účastníky
- Pokud PBX (soft switch) umožňuje, nastavit možnosti zamykání účtu PINem či blokování některých destinací účastníkem (mezinárodní směry, prémiová čísla atd.) a účastníky o této možnosti informovat.
- Zkontrolovat bezpečnost administrativního rozhraní (portálu) systému a případně omezit jeho dostupnost jen pro vlastní zákazníky a pracovníky operátora.

Závěr

- Podvody v telefonních sítích existovaly od jejich vzniku, existují dosud a vždy existovat budou
- Se změnami technologie se mění i principy podvodů, je nutno je studovat, abychom se byli schopni bránit
- S masovým rozvojem VoIP technologií stoupá prudce možnost podvádění vzhledem k nedostatečné odbornosti provozovatelů technologie - je nutné vzdělávání, aby byla technologie správně používána a nedocházelo k vyslovování chybných závěrů o "globální nebezpečnosti VoIP technologie"

Děkuji za pozornost.

patrol@sinus.cz

www.comtel.cz

www.gtsnovera.cz