Závěrečná zpráva „Podpora vědy a výzkumu v Moravskoslezském kraji“ prostřednictvím investic

Doc. Ing. Miroslav Vozňák, Ph.D.
Fakulta elektrotechniky a informatiky
VŠB-Technická univerzita Ostrava
17. listopadu 15/2172, 708 00 Ostrava

Zabezpečení komunikace v sítích GSM, UMTS, LTE

A. Zhodnocení

V rámci výzkumu podpořeného Moravskoslezským krajem jsme se zabývali bezpečnostními riziky mobilních sítí. Provedli jsme zmapování zranitelností mobilních sítí a analyzovali současná rizika. Na zařízeních pořízených v rámci dotace, a to především FPGA hradlových polích USRP, jsme realizovali experimenty s vlastní vytvořenou základnovou stanicí mobilní sítě, jsme úspěšně prakticky demonstrovali zranitelnost mobilních technologií.

Konkrétně se jednalo o výzkum těchto rizik:

1. Podvržení BTS stanice.

Vytvořili jsme základnovou stanici mobilní sítě a v laboratorních podmínkách jsme demonstrovali podvržení základnové stanice, na kterou se automaticky registrovaly mobilní telefony v okolí. Ekonomická náročnost řešení vychází řádově v desítkách tisíc. K realizaci jsme využili pořízenou HW platformu z dotace s hradlovým polem FPGA a především open-source projekty open-BTS a SDR (SW defined radio) a Asterisk, které jsme doplnili o vlastní kód, který umožňoval automatickou registraci mobilního telefonu nacházející se v okolí. Zde bylo využito slabiny GSM technologie, kde mobilní stanice preferuje základnovou stanici s nejsilnějším signálem. Při experimentech jsme samozřejmě postupovali tak, abychom nenarušili chod mobilní sítě žádného operátora a pracovali jsme pouze v laboratoři s omezeným výkonem, který pokrýval pouze danou místnost. Díky zkušenostem, které jsme získali, jsme navázali spolupráci s kolegy z ČVUT v Praze, kteří řeší v rámci bezpečnostního výzkumu Ministerstva vnitra detekci falešných BTS. Společně jsme opakovaně provedli experimenty na nově vyvíjeném zařízení pro odhalování podvržených základnových stanic v mobilní síti.

2. Rušení GSM/UMTS/LTE

Dále jsme se zabývali rušením mobilních sítí a navrhli jsme sedm způsobů rušení, kde jsme popsali výhody a nevýhody návrhů ve formě technické zprávy.

3. Odposlechy komunikace v mobilních sítích

V tomto bodě jsme demonstrovali možnost pasivního odposlechu, prolomení zabezpečení v GSM síti a následnému přístupu k obsahu komunikace (případy, kdy docházelo k zachycení/dešifrování komunikace, jsme prováděli pouze v laboratoři pro předem určenou mobilní stanici). Kromě pořízeného USRP s nákladností odposlechu několika desítek tisíc korun jsme rovněž úspěšně demosntrovali odposlech pomocí DVB-T přijímače s řádově nižší ekonomickou náročností na vybavení, který obsahoval chipset s laditelným tunerem v rozsahu frekvencí 35 MHz až 1100 MHz, což zahrnovalo pásmo GSM 900. Dalším způsob odposlechu je možný pomocí podvržené BTS, kterou jsme realizovali na USRP a při vypnutém šifrování na BTS je jeho realizace poměrně snadná a v reálném čase. Některé mobilní telefony upozorňují uživatele na vypnuté šifrování.

4. Odchycení IMSI

IMSI je unikátní kód přidělený každé SIM kartě mobilním operátorem, zpravidla 15-ti místný, a jeho odhalení zvyšuje riziko odposlechu či získání lokalizačně-provozních údajů konkrétního účastníka. Pro získání IMSI jsme použili IMSI catcher a pořízné zařízení USRP společně s OpenBTS s cílem podvrhnout falešnou základnovou stanici. Využili jsme vlastnosti GSM sítě, kdy nedochází k autentizaci BTS vůči MS, a je tak možné ji podvrhnout.

5. Kvalita služeb v mobilních sítích

Pořízené zařízení v projektu nám umožnilo rovněž získat kvalitativní údaje komunikace v mobilních sítích a tak jsem se nad rámec stanovených úkolů rovněž zabývali kvalitou služeb v mobilních sítích. Vytvořili jsme výpočetní model pro stanovení kvality hlasové a video komunikace (včetně IPTV) pro mobilní sítě, především nově budovanou LTE technologii.

B. Výsledky projektu

Realizovaný projekt nám umožnil identifikovat rizika bezpečnosti současných mobilních komunikací a jejich zranitelnosti, přispěl ke zvýšení profesní kvalifikace týmu řešitelů a během jeho řešení vznikla řada výstupů, které jsme publikovali na vědeckých konferencích.

Celkově vzniklo v rámci řešeného projektu šest výstupů, tři konferenční příspěvky, jeden do časopisu, jedna technikcá zpráva a jedna diplomová práce.

Koncem srpna 2014 byl podán projekt s názvem “Bezpečnost mobilních zařízení a komunikace“ s rozpočtem ve výši 13 524 000 Kč pro příjemce VŠB-TUO v rámci Programu podpory spolupráce v aplikovaném výzkumu a experimentálním vývoji prostřednictvím společných projektů technologických a inovačních agentur DELTA (TA ČR). Projekt je nyní hodnocen a v případě přijetí bude zahájena jeho realizace v roce 2015.

C. Publicita

Ve všech publikacích byla zajištěna publicita projektu ve formě poděkování v jazyce anglickém, v diplomové práci pak samostaným vloženým listem s logem a poděkováním v českém jazyce.

[1] L. Sevcik, M. Voznak, M. Prokes, P. Fazio, H. Total-Cruz, Study of security issues in GSM network and their practical demonstration, In Proceedings of the 2014 Networking and Electronic Commerce Research Conference, Trieste, Italy, ISBN 978-0-9820958-0-5, pp. 297-305.

[2] L. Sevcik, J. Frnda, M. Voznak, Degrading effect analysis, packet loss and out of order data on various tips and video resolution, In Proceedings of the 2014 Networking and Electronic Commerce Research Conference, Trieste, Italy, ISBN 978-0-9820958-0-5, pp. 130-138.

[3] M. Voznak, F. Rezac, K. Tomala, Advanced Emergency Voice Messaging, In Proceedings of the 2014 Networking and Electronic Commerce Research Conference, Trieste, Italy, ISBN 978-0-9820958-0-5, pp. 60-68.

[4] J. Kominek, M. Voznak, J. Zidek, Automatic Loss Adjustment for CDMA2000 and 1xEV-DO Standard for Downlink and Uplink, In Journal Advances in Electrical Engineering (Accepted with requested minor revisions).

[5] M. Prokeš, M. Vozňák (vedoucí práce), Bezpečnostní problémy GSM, Diplomová práce VŠB-TUO, 2014, Import 05/08/2014 URI: http://hdl.handle.net/10084/103798

[6] M. Dvorský, Rušení GSM/UMTS/LTE, Technická zpráva, VŠB-Technická Univerzita Ostrava, 7.7.2014, URL: http://homel.vsb.cz/~voz29/files/ruseni_gsm.pdf

O realizaci projektu jsme informovali na webových stránkách v sekci řešených projektů na pracovišti (Katedra Telekomunikační techniky, FEI VŠB-TUO), informace tak byly dostupné veřejnosti, viz. URL:

http://comtech.vsb.cz/index.php?option=com_content&view=article&id=93&Itemid=42&lang=cs

Zabezpečení komunikace na sítích GSM, UMTS, LTE

Moravskoslezský kraj

Mobilní sítě jsou široce používaným prostředkem pro moderní komunikaci, přičemž prolomení bezpečnostních algoritmů, které jsou inherentní pro tyto technologie (např. algoritmy A3, A5, A8 pro GSM), představuje velké bezpečnostní riziko z hlediska ochrany soukromí i citlivých dat. Dalším rizikem je vývoj technologií a dostupnost nových zařízení pro útoky v oblastech, kde dříve nebezpečí útoků nehrozilo díky velké finanční náročnosti či unikátnosti řešení. Současné hardwarové i softwarové možnosti přináší hrozby i do těchto nových oblastí, kde se v době jejich vzniku s podobnými útoky nepočítalo.

Výzkum je řešen v rámci projektu „**Podpora vědy a výzkumu v Moravskoslezském kraji 2013 DT 2 – Podpora výzkumu a vývoje VŠB-TUO prostřednictvím investic" (č. s. 02540/2013/RRC)**. Podpořeno z rozpočtu Moravskoslezského kraje.

Odpovědný řešitel projektu: doc. Ing. Miroslav Vozňák, Ph.D.

V Ostravě, 19.9.2014