Doc. Ing. Ladislav Hudec, CSc., Ústav počítačového inžinierstva a aplikovanej informatiky,
Fakulta informatiky a informačných technológií STU, Mlynská dolina, SK-842 16 Bratislava

---

Oponentský posudok dizertačnej práce

Dizertant: Ing. Libor Polčák, Fakulta informačních technologií, Vysoké učení technické v Brně
Názov práce: Zákonné odpočúvanie: detekcia identity (Lawful interception: identity detection)

Problematika identity entity v kybernetickom priestore je v súčasnosti vysoko aktuálnou témou výskumu v oblasti informatiky a informačných technológií. Vyplýva to nielen s rozširujúcim poskytovaním a využívaním služieb zabezpečujúcich dôveru, ale aj schopnosti a možnosti identifikovať zdroje aktivít v kybernetickom priestore. Dizertácia sa zaoberá identifikáciou v moderných počítačových sieťach vo vzťahu k potrebám zákonného odpočúvania. Téma dizertácie je vysoko aktuálna a spadá do odboru Výpočtová technika a informatika.

Predložená dizertačná práca je nadštandardného rozsahu. Obsahuje 10 kapitol, tri prílohy a 198 citovaných zdrojov. Celkovo má 182 strán.

Pôvodným prínosom dizertačnej práce je mechanizmus identifikácie adries IP (IPv6) v lokálnej počítačovej sieti. Detekcia priradenia adries IPv6 vychádza z analýzy premávky správ ND (Neighbor Discovery). Sledovanie priraďovania adries IPv6 je založené na časovanom prevodníku. Koncept časovaného prevodníka je originálnym výsledkom dizertačnej práce. Časovaný prevodník vytvára správy, ktoré sú základom pre záznamy IRI (Intercept Related Information) posielané subjektom LEMF (Law Enforcement Monitoring Facility) a správy umožňujúce konštrukciu grafu identity. Navrhnutý mechanizmus sledovania adries IPv6 najmä deteguje všetky adresy IPv6 každého uzla v lokálnej počítačovej sieti, okamžite signalizuje novo priradenú adresu a deteguje, ktorá adresa Ipv6 bola zrušená. Funkcia časovaného prevodníka je opísaná kombináciou automatu typu Mealy a časovanou tabuľkou prechodov. Prechody v časovanom prevodníku sú špecifikované v časti 6.4.4. Z textu dizertačnej práce nie je jasné, či sú špecifikované všetky možné prechody a nie je zrejmé, čo nastane, ak by sa mal vykonať nešpecifikovaný prechod. Podobný problémom je demonštrácia, že prechody pokrývajú všetky možnosti nájdené v rôznych operačných systémoch.

Druhým hlavným prínosom práce je analýza možností identifikácie vzdialeného počítača na základe hodinového sklonu. Dizertant navrhol a overil algoritmus na odhad hodinového sklonu (algoritmus 7.3.), napodobňovanie hodinového sklonu iného počítača (algoritmus 7.4.) a zlubovoľnenie stabilného hodinového sklonu počítača (algoritmus 7.5.). Analýzy ukázali, že protokol NTP vplýva na časové značky TCP. Ďalej dizertant analýzou rozdelenia hodinového posuvu v reálnych sieťach zistil, že väčšina odhadov reálnych hodinových sklonov je prakticky 0 ppm (parts per million). Z toho vyplýva, že krátkodobý odtlačok hodinového sklonu nemôže spoľahlivo identifikovať počítače výhradne pomocou hodinového sklonu.

Tretím hlavným prínosom práce je originálne zostrojenie grafu identity, ktorý ukladá identifikačné údaje z počítačovej sieti získané z distribuovaných detektorov parciálnej identity. Ako detektory parciálnej identity sú vzaté do úvahy analyzátory premávky, analyzátory záznamových súborov a rozšírenia programov (program extensions). Na základe analýzy dizertant špecifikoval šesť kategórií identifikátorov. Pre graf identity stanovil algoritmy na zaobchádzanie so začiatočnými, pokračujúcimi a koncovými správami (algoritmus 8.1., 8.2. a 8.3). Ďalej stanovil obmedzujúce funkcie, ktoré obmedzujú vzťahy medzi identifikátormi resp. obmedzujú prechody medzi kategóriami identifikátorov. V multigrafe identity je zavedené aj časové obmedzenia na detekciu identity a obmedzenie dané nepresnosťou parciálnych detektorov. V dizertácii sa uvádza hodinový sklon ako príklad obmedzenia nepresnosti. Mohol by dizertant uviesť aj iné príklady obmedzenia nepresnosti, prípadne čo je považované za ešte akceptovateľnú úroveň nepresnosti a ako to ovplyvní presnosť detekcie identity?

Jadro dizertácie bolo publikované v 10 článkoch a príspevkoch doma a v zahraničí. Dva príspevky boli na domácich konferenciách. Zvlášť oceňujem časopisecké publikácie v IEEE Transactions on Dependable and Secure Computing, Journal of Universal Computer Science, The Journal of Digital Forensics, Security and Law a dva príspevky vydané v zborníku Springer. Na základe uvedených skutočností možno konštatovať, že jadro dizertácie bolo dostatočne posúdené odbornou komunitou.

Taktiež možno konštatovať, že na základe celkovej publikačnej činnosti dizertanta ako aj na základe predloženej dizertačnej práce je dizertant je pracovník s vedeckou erudíciou.

Predložená dizertačná práca dokumentuje nielen schopnosť dizertanta, že ovláda vedecké metódy práce a priniesol nové vedecké poznatky, ale aj schopnosť vykonávať vysoko odbornú inžiniersku prácu. Výsledky dizertačnej práce boli využité na vyriešenie projektu zákonného odpočúvania SLIS (Sec6Net Lawful Interception System). Projekt SLIS bol úspešne prezentovaný českým orgánom činným v trestnom konaní. Dosiahnuté výsledky v poznaní parciálnych identít možno využiť aj vo forenznej analýze počítačových sietí a v softvérovo definovaných sieťach.

Celkové hodnotenie dizertačnej práce.
Dizertačnú prácu Ing. Libora Polčáka považujem za prínosnú pre aktuálnu problematiku detekcie identity v moderných počítačových sieťach a práca zodpovedá všeobecne uznávaným požiadavkám pre udelenie akademického titulu.

V Bratislave, dňa 19.9.2017 podpis oponenta