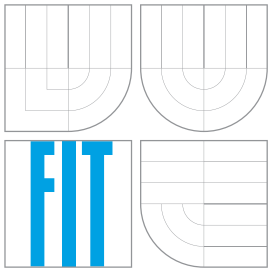
Vysoké učení technické v Brně
Brno University of Technology



Fakulta informačních technologií

Faculty of Information Technology

Zabezpečenie Skype

Odborná práca do predmetu IBS

Autor práce Ladislav Šulák

Login xsulak04

Brno 5/2015

Obsah

Kapitola 1

Úvod

Skype je voľne dostupná aplikácia, ktorá slúži pre komunikáciu prostredníctvom sieti internet. Je nenáročná na výkon, má viacero funkcií, a je kompatibilná s mnohými operačnými systémami a platformami. Pomocou nej je možné zasielať správy, posielať súbory, alebo uskutočnovať videohovor či len samotný prenos hlasu. V roku 2011 bola odkúpená spoločnosťou Microsoft a v roku 2013, desať rokov po vzniku tejto aplikácie, bolo uvedené[1], že má 300 miliónov aktívnych užívateľov. V súčasnosti sa používa väčšinou v komerčnej sfére, no v poslednej dobe často aj v obchodnej. Únik alebo poškodenie informácií môžu mať v mnohých prípadoch negatívny dopad, preto je bezpečnosť a ochrana dát Skypu často horúcou témou.

Nasledujúca podsekcia popisuje sieťovú architektúru celého systému. Potom budú vymenované technológie, ktoré Skype používa. Informácie o tejto problematike budú čerpané z [3], [7], [9], [4] a [1]. Obsahom tejto práce je predovšetkým bezpečnosť dát, aplikácie i celého systému, so zameraním na ochranu súkromia užívateľov. Tejto problematike sa bude venovať kapitola 2. V kapitole 3 budú uvedené hlavné prístupy v súčasnosti aj v minulosti, ktorých cieľom je odhaliť nejakú zraniteľnosť alebo zneužiť súkromie užívateľa. Na záver, v kapitole 4 budú zhodnotené dosiahnuté poznatky.

1.1 Sieťová architektúra a protokoly

Aplikácia Skype využíva technológie a algoritmy služby VoIP. Architektúra tohto systému je *peer-to-peer*, čo znamená, že klienti, teda komunikujúce strany, sú medzi sebou prepojené priamo, nie cez prostredníka, napríklad serveru. Ako ale bude vysvetlené neskôr, nemusí to platiť vždy. Celá sieťová architektúra obsahuje nasledovné entity:

- Štandardné uzly, angl. *ordinary nodes*, sú aplikácie Skype na strane klienta. Používajú sa pri zasielaní textu, súborov, hlasu, alebo videohovoru. Musia byť pripojené na super uzol a následne byť autentizované serverom pre prihlásenie. Každý štandardný uzol vždy zasiela požiadavok na vytvorenie relácie viacerým super uzlom. Ten, čo zareaguje prvý, bude vybraným super uzlom na danej relácii. Čo sa týka autentizácie, tá môže prebiehať priamo alebo prostredníctvom super uzlu. Po úspešnom prihlásení sú v super uzle aktualizované údaje o klientovi, ako napríklad IP adresa, dostupný

[1] Štatistiky z roku 2013 zahrňujúce počty užívateľov sú dostupné na http://blogs.microsoft.com/firehose/2013/08/29/skype-celebrates-10-years-300-million-users-and-1-4-trillion-minutes-of-voice-and-video-calls/.

a otvorený port pre komunikáciu a rôzne ďalšie informácie ako napríklad prítomnosť užívateľa (*Online*, *Not Available*,...).

- Super uzly, angl. *super nodes*, sú koncové zariadenia v Skype sieti. Sú to jednotky slúžiace pre udržiavanie distribuovaného priečinku obsahujúceho globálny index, pomocou ktorého spolu užívatelia navzájom dokážu komunikovať. Každý štandardný uzol sa môže stať super uzlom, pokiaľ má verejnú IP adresu, dostatok výkonu a pamäte, no rozhodujúcim faktorom je aj šírka prenosového pásma. Každý super uzol má kontaktné informácie o ostatných super uzloch, a pomocou globálneho indexu je možné nájsť akýkoľvek uzol, ktorý bol prihlásený do sieti za posledných 72 hodín. Jeden super uzol uchováva časť distribuovaného priečinka, čo predstavuje niekolko stoviek užívateľov. Len pre predstavu, podľa [2] bolo v roku 2006 okolo 20 000 super uzlov, lokalizovaných hlavne v Európe, Severnej Amerike a juhovýchodnej Azií. Kedže je dnes počet užívateľov v porovnaní s rokom 2006 približne 3 násobne väčší, počet uzlov bude pravdepodobne predstavovať tiež omnoho vyššie číslo.

- Server pre prihlasovanie, angl. *login server*, obsahuje informácie o užívatelských účtoch a slúži pre autentizáciu klienta. Autentizácia prebieha vždy na začiatku každej relácie. Od verzie Skypu 1.2 zanikla samostatná entita, ktorá slúžila ako server obsahujúci zoznam priateľov. Táto informácia je uložená spoločne s dátami o užívateľských účtoch. Pri vyhľadávaní užívateľského mena nejakého priateľa klient obdrží jeho verejný kľúč.

- Skype server pre aktualizáciu systému má v tejto sieťovej architektúre tiež svoju úlohu. Počas prihlasovania, teda na začiatku relácie, aplikácia na strane klienta zašle HTTP GET požiadavok za účelom zistiť, či aktuálna verzia systému je najnovšia. Z podobných dôvodov je kontaktovaný aj po úspešnej inštalácií produktu.

1.2 Technológie

Grafické a užívateľské prostredie aplikácie boli nápísané hlavne v jazyku Delphi. Sieťová časť, kodeky, algoritmy pre šifrovanie a mnoho ďalších funkcionalít, bolo implementovaných v jazyku C++. Skype používa pre kompresiu zvuku kodek SILK. Jedná sa o proprietárny kodek vytvorený samotnou spoločnosťou Skype. Nahradil starší s názvom iSAC, ktorý bol vyvinutý spoločnosťou Global IP Solutions, ktorú v roku 2011 odkúpil Google. Čo sa týka prenosu videa, v najnovších verziách je použitý kodek VP7, no v niektorých situáciach, hlavne pri požiadavke na vyššiu kvalitu obrazu kodek H.264.

Na zabezpečení sa podieľa viacero algoritmov, hlavne takých, ktoré slúžia na silné šifrovanie komunikácie a prenášaných dát. Zasielanie požiadavkov, prenos dát a mnohé ďalšie funkcie využívajú služby TCP aj UDP na náhodne zvolených portoch. Na mnohých ďalších miestach, nie len v komunikácií ale aj v implementácií samotnej klientskej aplikácie, sú využívané stochastické procesy a generovanie pseudonáhodných čísel. Zabezpečenie bude bližšie popísané v nasledujúcej kapitole. Znalosti o bezpečnostných mechanizmoch pochádzajú hlavne z [6].

Kapitola 2

Zabezpečenie aplikácie Skype

Táto kapitola začína opisom postupného priebehu komunikácie so zameraním na zabezpečnie. Po úspešnej inštalácií klientského produktu nasleduje proces registrácie. Užívateľ zadá prihlasovacie údaje a aplikácia vygeneruje z hesla hash a 1 pár kľúčov RSA. Uvádza sa [2], že generuje dve 512-bitové čísla, teda 1024-bitové RSA verejné/súkromné klúče, ktoré reprezentujú užívateľa. Tento hash a súkromný RSA kľúč sú uložené v počítači. Tento asymetrický algoritmus, sa používa pre výmenu kľúčov medzi jednotlivými uzlami a je bezpečný pri dostatočne veľkej dĺžke klúča. Autentizácií samotnej musí ešte predchádzať pripojenie štandardného uzlu na super uzol. Zistilo sa, že je to realizované zasielaním UDP paketov s určitou malou veľkosťou prenesených dát na aplikačnej vrstve. Toto je možné zachytiť, no nie je to také triviálne ako sa zdá kvôli použitiu náhodných portov, veľkostí paketov a iných atribútov. Po pripojení k super uzlu nasleduje ďalšia fáza, v ktorej sa zasliela požiadavok centrálnym Skype serverom pre akceptovanie prihlasovacích údajov. Na tomto serveri sa ukladajú verejné kľúče užívateľov so zahashovanými hashmi hesiel. Okrem priamej manipulácií s aplikáciou na strane klienta je Skype účet dostupný aj na internetových stránkach (skype.com), kde je možné vykonávať operácie pre prihlásenie alebo registráciu užívateľa. Podľa [1] sú tieto prenášané informácie šifrované protokolom SSL. Ten funguje tak, že šifruje všetky dáta pred odosielaním a dešifrovať ich môže až cieľový uzol v sieti. To má za následok, že pri odpočúvaní komunikácie nie je možné získať prihlasovacie údaje, poprípade iné dáta alebo ich zmeniť.

Ak je užívateľ prihlásený do siete Skype a chce komunikovať s iným užívateľom, je medzi nimi vytvorené TCP spojenie. Pred vzniknutím samotnej relácie je nutné, aby bola overejná integrita oboch klientov a aby sa dohodli na relačnom kľúči. Integrita je v tomto prípade zaistená výmenou verejných kľúčov klientov pomocou proprietárneho protokolu dotaz-odpoveď. Tieto kľúče sú podpísané autoritou Skypu. Každý klient zasiela 8-bajtovú výzvu pre podpísanie a až potom sú autentizovaní a následne vyberajú symetrický kľúč pre danú reláciu.

Je nutné poznamenať, že pri nadväzovaní komunikácie môžu nastať rozdielne situácie, ako sa systém zachová. Viacero VoIP riešení má problém prenášať dáta ak sú uzly za službou NAT alebo za firewallom. Skype obišlo toto obmedzenie tak, že v prípade tejto situácie preposiela komunikáciu medzi klientami cez super uzly. Dokonca obsahuje aj inteligentné preposielanie dát podľa najefektívnejšej trasy, pretože si ukladá cesty a necháva ich pre prípad neskôršieho využitia otvorené. Týmto prístupom Skype dokáže optimálne prenášať dáta. Na transportnej vrstve je najčastejšie použitý UDP prokotol pre posielanie dát, no v určitých situáciách, najmä ak je z nejakého dôvodu UDP komunikácia nedostupná, bude typ transportnej vrstvy automaticky zmenený na TCP, dokonca aj uprostred hovoru.

Pre šifrovanie dát využíva symetrický algoritmus AES (*Advanced Encryption Standard*) s 256-bitovými kľúčmi a pre ich výmenu asymetrický algoritmus RSA (podľa autorov Rivest, Shamir, Adleman) s 1546 až 2048 bitovými kľúčmi. Signalizácia je zaistená algoritmom RC4, ktorý je jednoduchý a rýchly. Je to prúdová šifra, ktorá využíva generovanie pseudonáhodných čísel. Algoritmus RC4 bol v programe implementovaný ako veľká funkcia, ktorá slúži pre obfuskáciu sieťovej prevádzky, nie primárne pre zaistenie súkromia.

Najdôležitejšie požiadavky súvisiace s bezpečnosťou tohto systému ako celku budú popísané v nasledujúcich sekciách. Informácie boli čerpané najmä z [5].

2.1 Súkromie

Všetky dáta sú v Skype zašifrované. Nie je možné komunikáciu odpočúvať, avšak je otázne, či sú jednotlivé zabezpečovacie mechanizmy použité v systéme dostatočne silným prostriedkom. Závisí to od konkrétnej implementácie jednotlivých algoritmov a protokolov, no tieto informácie aj napriek viacerým pokusom chýbajú. Avšak, ako bolo vysvetlené v sekcií 1.1, počas prihlasovania a autentizácie prebiehajú aj ďalšie činnosti, čo môže mať pri odpočúvaní komunikácie za následok zbieranie informácií o IP adresách a užívateľoch, ktorí spolu navzájom komunikovali, a v akom čase. Získané IP adresy je možné použiť pri DDoS, alebo inom sieťovom útoku. Narušiť súkromie by bolo možné napadnutím inej služby bežiacej v počítači a získať informácie zo súborov, ktoré si Skype ukladá. Obsahujú napríklad dáta o histórii správ, o súboroch, ktoré boli prenášané, alebo o zozname priateľov. To isté platí ak si užívateľ hovor nahrával a uložil lokálne do súboru. Kvôli nedostatku informácií o implementácii systému nie je možné určiť, či okrem známej funkcionality nie je vykonávaná nejaká ďalšia. Napríklad, pokiaľ sa komunikácia preposiela cez super uzly, či sa nepreposiela na nejaké iné miesto, poprípade či sa niekam neukladá. Komunikácia medzi jednotlivými uzlami väčšinou prebieha priamo, no pokiaľ je nejakým spôsobom, napríklad pomocou firewallu obmedzená komunikácia, prenos dát prebieha týmto spôsobom, teda prostredníctvom super uzlov.

2.2 Autentizácia

Registrácia do Skype siete prebieha zaslaním užívateľského mena a hesla v klientskej aplikácii. Tá ich zašifruje a odošle na jeden z centrálnych serverov. Centrálny server nemá heslá uložené v klasickej podobe, ale ako zahashované hashe hesiel. Použitie slovníkového útoku je takmer nemožné, pretože okrem viacnásobného hashu je nastavené, že po niekoľkých pokusoch centrálny server užívateľa odpojí. Pokiaľ by ale útočník bol úspešný v kompromitovaní inej služby alebo systému, kde má užívateľ rovnaké prihlasovacie údaje, bolo by možné zneužiť identitu niekoho iného. Pri prenose hlasu je možné určiť, či dáta naozaj pochádzajú od očakávaného užívateľa. Táto biometrika sa z časti tiež môže podieľať na autentizácii.

2.3 Dostupnosť

Závisí od stability internetového pripojenia a tiež od dostupnosti serverov, voči ktorým sa klient autentizuje. O týchto serveroch nie je známe ako veľmi sú stabilné a odolné, preto nebude ďalej uvažovaná ani odolnosť systému ani schopnosť pretrvať nejaký útok alebo zly-

hanie siete. Je nutné ale dodať, že pri zmene IP adresy je systém veľmi rýchlo prispôsobivý, no pri problémami s autentizáciou je užívateľovi od Skype siete prístup zamietnutý.

2.4 Integrita

Je otázne či môžu byť zasielané dáta pozmenená, či už hlasové, textové informácie, alebo binárne súbory. V porovnaní s inými systémami pre prenos súborov Skype pravdepodobne neobsahuje žiadny interný antivírus, ktorý by kontroloval binárne súbory. Risk prítomnosti potencionálne škodlivého súboru sa znižuje ale tým, že komunikácia neprebieha s neznámymi osobami. Ak by útočník našiel v klientskom systéme zraniteľnosť, bolo by možné dáta pozmeniť a narušiť tým ich integritu.

Kapitola 3

Možnosti narušenia bezpečnosti

Možnosti narušenia bezpečnosti aplikácie alebo nejakej časti tohto systému sú očividne dosť obmedzené. Aplikácia je typu closed-source a implementačné detaily nie sú a zdá sa, že ani nebudú zverejnené. Tento fakt a silné bezpečnostné mechanizmy zabraňujú útočníkom pre zneužitie zraniteľností v systéme a ich následnú exploitáciu. Takisto odpočúvanie komunikácie je takmer nemožné. Narušenie bezpečnosti alebo obídenie týchto mechanizmov môže byť pre mnohých ľudí, najmä hackerov výzva a je možné sa stretnúť s 2 hlavnými prístupmi, ktoré bližšie objasňujú nasledovné 2 sekcie.

3.1 Detekovanie prebiehajúcej komunikácie

Identifikácia sieťovej prevádzky aplikácie Skype nie je triviálna, nebeží na jednom, unikátnom porte, prenos paketov sa uskutočňuje aj keď aplikácia nie je priamo využívaná, ale iba zapnutá[2], protokol pre komunikáciu medzi uzlami v sieti nie je verejne dostupný, dáta sú zašifrované a naviac existuje viacero verzií s mierne odlišným správaním, čo platí najmä pre zastaralejšie verzie pod operačným systémom s linuxovým jadrom. K aktualizácii tejto aplikácie dochádza pomerne dosť často, a pri zmene niektorých parametrov alebo použitých algoritmov môže dôjsť k posilňeniu bezpečnosti, pretože tieto nové informácie nie sú známe a pri procese detekovania spojení typu Skype môže dôjsť k vyššej miere chybovosti. Pri úspešnom detekovaní prebiehajúcich sieťových prenosoch medzi jednotlivými entitami v tomto systéme je možné odhaliť komunikujúce strany. To môže v určitých prípadoch viesť k porušeniu súkromia, napríklad pri zbieraní IP adries jednotlivých komunikujúcich klientov, časov týchto komunikácií, alebo približnej veľkosti prenesených dát. Získané IP adresy môžu byť použité pre lokalizáciu komunikujúcich strán, alebo napríklad pre útoky typu DDoS. Klasifikáciou a identifikáciou tejto komunikácie sa zaoberalo viacero prác, napríklad [11], [10] a [8]. Pri určovaní stavu komunikácie boli napríklad vyhľadávané UDP pakety, ktorých veľkosť pochádzala z určitého vypozorovaného intervalu a určitej periodicity zasielania. Okrem toho boli využívané metódy pre behaviorálnu analýzu a na základe určitých štatistických metrík snaha o identifikovanie a klasifikáciu požadované spojenia, pričom sa experimentovalo s rôznymi algoritmami pre strojové učenie s ďalšími so zameraním na zber dát o užívateľoch a ich činnostiach na sieťovej prevádzke.

[2]Sem patria napríklad požiadavky, výzvy alebo správy typu *ping*, ktoré sa podieľajú na rôznych aktualizáciách, ako napríklad na aktualizícií globálneho indexu a dát v super uzle, alebo správ o aktuálnej verzií systému a podobne.

3.2 Reverzné inžinierstvo

Nájsť zraniteľné miesta alebo chyby v aplikácií, pochopiť ako fungujú niektoré dôležité a kritické komponenty je kľúčové pre úspešné napadnutie systému. Touto oblasťou sa zaoberajú mnohí experti [2] či iné skupiny ľudí, zo zvedavosti, ale aj takí, čo to berú ako výzvu alebo chcú dosiahnuť nejaké vlastné ciele. Skype bol implementovaný tak, aby jeho zdrojové kódy neboli ľahko získateľné a dekompilované ani metódami reverzného inžinierstva. Zdá sa, že Skype ma vlastný packer, kód je obfuskovaný a je použitých viacero techník znemožňujúce ladenie. Je výnimočne odolný voči manipulácií, pokiaľ dôjde k jeho modifikácii na úrovni binárneho súboru, aplikácia sa zastaví alebo spadne na náhodnom mieste. To je spôsobené tým, že sa v kóde nachádzajú desiatky, stovky alebo až tisíce kontrólnych súčtov, ktoré sú naviac mierne odlišné. Tento polymorfizmus je len jeden z viacerých mechanizmov [2], akým si program chráni vlastnú integritu.

Kapitola 4

Záver

Skype je viac ako len obyčajná sieťová aplikácia. Dokonca aj po jej skončení sa môžu vykonávať nejaké činnosti na pozadí , spojené napríklad s preposielaním informácií o uzloch v sieti a tak v istej miere spotrebovávať procesorový výkon či sieťové alebo pamäťové prostriedky. Pre úplné eliminovanie tejto činnosti, ktorú si ľudia často neuvedomujú, je nutné skončiť všetky procesy, ktoré patria do množiny procesov tohto systému. Ako bolo vysvetlené v predchádzajúcich kapitolách, klientská aplikácia a ostatné časti systému s protokolmi a algoritmami je v podstate veľká čierna schránka, tzv. *black box*. Naviac je pre komerčnú sféru voľne dostupná, teda je otázne či v sebe neukrýva škodlivý kód typu trójsky kôň, nespúšťa zadné vrátka, alebo neobsahuje iný druh nežiaducej aktivity. Podozrivé môže byť aj to, že binárny súbor má relatívne veľkú veľkosť, no to môže byť zapríčinené bezpečnostnými mechanizmami.

Zo známych poznatkov, ktoré boli popísané v tejto práci je zrejmé, že zabezpečenie aplikácie Skype je naozaj veľmi silné. Narušiť súkromie užívateľa, zneužiť alebo porušiť integritu dát je ale možné, napríklad pomocou kompromitovania cieľového zariadenia pomocou inej zraniteľnej služby alebo aplikácie. V súborovom systéme sa nachádzajú viaceré súbory, do ktorých si aplikácia ukladá určité dáta. Niektoré z nich sú len slabo zašifrované alebo vôbec. Mená užívateľov zo zoznamu priateľov je napríklad veľmi ľahko možné získať a následne zneužiť. Takisto uložené konverzácie je možné získať, poprípade lokálne modifikovať, čo platí aj o ďalších dátach alebo metadátach ukladaných klientskou aplikáciou. Ako bolo uvedené v predchádzajúcej kapitole, zistiť aké subjekty a v akom čase medzi sebou komunikovali je tiež možné. V tomto momente sa vynárajú v princípe dve otázky: je aplikácia Skype a systém na ktorom je postavená dostatočne zabezpečená? Nevykonáva nejaká jej časť nežiadúcu činnosť, ktorá je nám zatiaľ skrytá?

Literatúra

[1] Skype Security [online].
http://www.skype.com/en/security/.

[2] Viacero výskumov zaoberajúcich sa bezpečnosťou Skype [online].
http://www.cs.columbia.edu/~salman/skype/.

[3] Baset S., Schulzrinne H.: An Analysis of the Skype Peer-to-Peer Internet Telephony Protocol. Technická zpráva, Columbia University, 2004.

[4] Chen Ch., Chu C., Yeh S., Chu H., Huang P.: Measuring the perceptual quality of Skype sources. *W-MUST. Proceedings of ACM SIGCOMM workshop on Measurements up the stack*, 2012: s. 1–6.

[5] Garfinkel, S.: VoIP and Skype Security. Technická zpráva, Columbia University, 2005.

[6] Hayes, B.: Skype: A Practical Security Analysis. Technická zpráva, SANS Institute, 2008.

[7] Korpela, T.: IT Security Evaluation of Skype in Corporate Networks. Technická zpráva, Helsinki University of Technology, 2006.

[8] Leontjeva A., Goldszmidt M., Xie Y., Yu F., Abadi M.: Early security classification of skype users via machine learning. *AISec. Proceedings of ACM workshop on Artificial intelligence and security*, 2013: s. 35–44.

[9] Lisha G., Junzhou L.: Performance Analysis of a P2P-Based VoIP Software. *Proceedings of the Advanced International Conference on Telecommunications and International Conference on Internet and Web Applications and Services*, 2006.

[10] Perényi M., Molnár S.: Enhanced Skype Traffic Identification. Technická zpráva, Budapest University of Technology & Economics, 2007.

[11] Suh K., Figueiredo D., Kurose J., Towsley D.: Characterizing and detecting relayed traffic: A case study using Skype. Technická zpráva, University of Massachusetts, 2005.