TECHNISCHE UNIVERSITÄT DRESDEN

Zentrum für Informationsdienste und Hochleistungsrechnen

Skype @ Sicherheit

Frank Schulze / Jens Syckor

München, 21. November 2014

ZIH
Center for Information Services & High Performance Computing

Agenda

- Geschichte
- Funktionsweise
- Sicherheitsaspekte
- Regelung an der TU Dresden
- Fazit

Skype - Geschichte

- VoIP-Software eines estnischen Entwicklerteams (das auch KaZaa entwickelt hatte)
- 2003: Gründung von Skype Ltd. mit Sitz in Luxemburg durch Niklas Zennström und Janus Friis
- „Sky peer-to-peer“ → Skyper → Skype
- August 2003: erste öffentliche Beta von Skype
- September 2005: eBay erwirbt Skype (3,3 Milliarden US-Dollar)
- September 2009: eBay verkauft 65% der Anteile an die Investmentgesellschaft Silver Lake
- Mai 2011: Microsoft übernimmt Skype (8,5 Milliarden US-Dollar)
- Oktober 2012: mehr als 45 Millionen Nutzer zeitgleich online über Skype
- November 2012: Skype ersetzt vollständig den Windows Live Messenger
- 01.01. 2014: ca. 663 Millionen registrierte Nutzer
- ab 01.08. 2014: Blockierung ältere Versionen von Skype bei der Anmeldung

Skype - VoIP

- Proprietäre VoIP-Lösung (Skype-Protokoll nicht öffentlich, nur durch Skype-Software nutzbar); nicht kompatibel zu anderen VoIP-Lösungen, die auf H.323 oder SIP basieren
- Kostenloses Telefonieren zwischen Skype-Nutzern
- Kostenpflichtig für Telefonate ins Festnetz und Mobilnetz (SkypeOut)
- Annahme von Telefonaten aus dem klassischen TK-Netz (Online-Nummer)
- Anrufweiterleitung an Skype-Konten oder ins klassische TK-Netz
- Konferenzgespräche mit bis zu 25 Personen
- SILK Audio Codec (Entwicklung von Skype, 6 bis 40kbit/s)
- Clients für Windows, Linux, Mac OS X, Android, iPhone, Symbian, Panasonic und Samsung TV
- Kostenpflichtige Weiterleitung eingehender Telefonate von Skype zur SIP-Anlage möglich

Skype - Features

- Kostenfreie Sprachkonferenzen bis zu 25 Teilnehmern
- Kostenfreie Videokonferenzen
  - mit zwei Teilnehmer unbegrenzt nutzbar
  - „Faire Nutzungsbedingungen“ empfehlen max. fünf Teilnehmer
  - Beschränkung auf 100h / Monat; 10h / Tag und 4h / Konferenz
- Instant Messaging (Chats mit mehreren Teilnehmern, Integration über Plugins in Third-Party IM-Tools)
- SMS Textnachrichten; Dateiübertragung; Screen-Showing
- Skypekit (Bibliothek zur Einbindung in Third-Party-Software, Beta-Tests)
- Facebook-Integration (Facebook-Kontakte in Skype-Telefonbuch, Statusmeldungen)
- seit 14.11.2014 im Betatest: „Skype for web“ (lauffähig ab IE 10 und den aktuellen Versionen von Firefox und Google); Zusammenführung mit WebRTC geplant

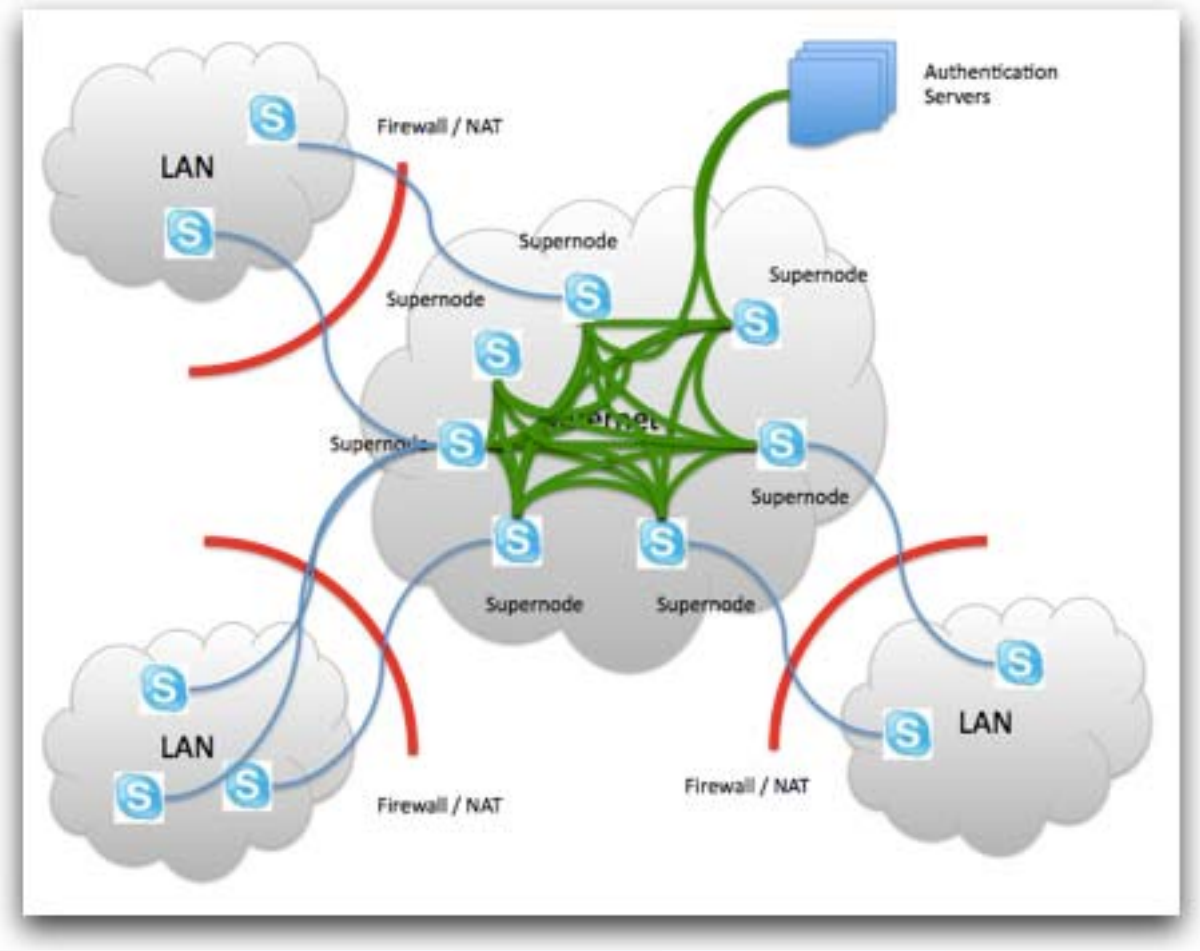
Skype - Protokoll

- Peer-to-Peer (P2P), Clients sind gleichberechtigt, kein zentraler Server
- Hybride P2P-Architektur per Overlay-Netzwerk
- Dezentrale Struktur, d.h. P2P für Skype-Dienste wie VoIP, IM, Videocalls
- Zentrale Struktur für Authentifizierung, Abrechnung, Übergang in klassische Telefonie (SkypeOut)
- Unterscheidung von drei Node-Typen
  - Ordinary Node: Standard Skype-Client
  - Super Node: Verteilung des Skype Nutzerverzeichnisses, sind untereinander verbunden
  - Relay Node: Weiterleitung der Kommunikation von Clients, die nicht direkt miteinander kommunizieren können (Firewall, NAT)
- Auswahl der Super Nodes durch Skype anhand von Merkmalen des Clients
  - Öffentliche IP-Adresse, Bandbreite, CPU, RAM, ...

Skype - Datennetz (I)

- Kommunikation über UDP und TCP, keine Default-Ports, Einsatz einer Variante des STUN-Protokolls (Session Traversal Utilities for NAT)
- Verwendung von TCP Port 80 bzw. 443 (optional)
- Super-Nodes ermöglichen Kommunikation durch Firewalls und aus NAT-Umgebungen (NAT Traversal)
- Super-Nodes routen nicht nur Signalisierungsdaten sondern seit Juli 2012 auch Sprachdaten
- Verbindungsaufbau:
  - UDP Verbindung zu Skype Authentication-Servern (in Client fest codiert)
  - Wenn nicht erfolgreich, neuer Versuch mit TCP
  - Wenn nicht erfolgreich, neuer Versuch mit TCP 80 (http)
  - Wenn nicht erfolgreich, neuer Versuch mit TCP 443 (https)
- Nach Start des Skype Clients zufälliger Port für eingehende Verbindungen, zusätzlich offene Ports 80 und 443

Skype - Datennetz (II)



Dan York 2010

Skype - Sicherheit

- Schutz der Skype-Software vor Reengineering (Anti-Debugging, Code Check, Verschlüsselung des Binaries, Code Obfuscation)
- Einsatz von asymmetrischen und symmetrischen Kryptoverfahren zur Verschlüsselung der Kommunikation und Authentifizierung der Nutzer
  - AES-256 Transport Layer Encryption (Ende-zu-Ende)
  - Reverse Engeneering zeigte auch Einsatz von (angreifbaren) RC4-Algorithmen
  - Schlüssel zur Aushandlung der symmetrischen AES-Schlüssel wird mit 1536 bis 2048 bit RSA übertragen
  - Berechnung nutzt Login und Passwort des Skype Nutzers
  - Super Nodes halten Public Key und Login der Nutzer, signiert von Skype

Skype - IT-Sicherheit aus Sicht des Nutzers (I)

- Vertraulichkeit
  - Keine Offenlegung des Skype-Protokolls, obwohl Einsatz von bekannten Kryptoverfahren
  - Immer wieder Probleme (April 2012: Skype-Accounts können mit einfachsten Mitteln von Fremden bei Kenntnis der E-Mail-Adresse des Besitzers übernommen werden)
- Integrität
  - Zertifikat über Nutzeridentität ausschließlich von Skype
  - Nutzername, Passwort (mindestens 6 Zeichen)
  - Frage der Super-Nodes
  - Skype-Zugangskonto ist nicht löschbar
- Verfügbarkeit
  - Grundsätzlich höhere Bewertung bei P2P; aber am 22.12.2010 Ausfall von Super-Nodes durch Software-Bug
  - Kein Notruf über Skype möglich

Skype - IT-Sicherheit aus Sicht des Nutzers (II)

- Installation greift tief in die Einstellungen des zu Grunde liegenden Betriebssystems ein ➔ voreingestellte Haken deaktivieren
- Authentizität des Nutzers wird nicht geprüft
- "We provide a safe communication option. I will not tell you whether we can listen or not.“ (Kurt Sauer, Chief Security Officer of Skype, 2007)
- Microsoft scannt alle übertragenen Inhalte und nimmt sich das Recht zu dessen eigener Verwertung
- US-Behörden haben seit 2008 Zugriff auf alle Skype-Daten (z.B. Konfigurations- Zugangs-, Kontakt- und Präsenzinformationen), auch wenn diese in Europa liegen (Telekom „DuD 2013“)
- Microsoft meldete am 23.06.2011 ein Patent zum unbemerkten Aufzeichnen von Kommunikationsinhalten an

Skype - IT-Sicherheit aus Sicht des Nutzers (III)

- Im Rahmen von PRISM kann die NSA auch in Echtzeit überwachen
- In der chinesische Variante TOM-Skype werden alle Inhalte, Namen, IP-Adressen usw. vollständig von den Landesbehörden mitprotokolliert; auch wenn der Partner im Ausland sitzt und die „normale“ Version nutzt
- Österreichische Behörden können Skype mindestens seit 2008 abhören
- Seit mind. Oktober 2010 nutzt der deutsche Zoll eine spezielle Software „Skype Capture Unit“ zum Kopieren von Gesprächsinhalten in Skype

➔ Bundesdatenschutzbehörde sieht Einsatz von Skype kritisch; personenbezogene Daten sind nicht sicher und es kommt beim Einsatz der Software zu Verstößen gegen das Bundesdatenschutzgesetz

Skype - Risiken im universitären Umfeld

- Aushebelung von Netz-Sicherheitskonzepten (Firewall, DMZ)
- Ressourcen der Universität für Skype-Kommunikation (Super Nodes)
  - Bandbreite, Rechenleistung, ...
  - im Leerlauf bis zu 1 GByte im Monat; 1h Audio braucht ca. 30 MByte
- Nutzer bekommen keine Information, wenn Skype Client Super Node wird
- Deaktivierung der Super Node Funktionalität nur unter Windows möglich
- Dateiübertragung, Screen-Sharing (Data Loss Prevention)
- Sicherheitsrisiko Skype API
  - keine Zertifizierung/Test von Skype
  - unbeschränkter Zugriff auf Skype
  - Anwendungen sind verpflichtet, keine personenbezogenen Daten zu erfassen
  - Botnetz auf Skype unter Verwendung der API (Nappa et al. 2010)

Skype - Empfohlene Einstellungen

unter `HKEY_LOCAL_MACHINE\Software\Policies\Skype\Phone`

- Deaktivierung der Supernode-Funktionalität:
  `DisableSupernode, REG_DWORD = 1`
- Deaktivierung von Dateiübertragungen:
  `DisableFileTransfer, REG_DWORD = 1`
- Deaktivieren der API-Fähigkeit:
  `DisableApi, REG_DWORD = 1`

➔ Diese Einstellungen sind für Nutzer ohne Administratorrechte nicht änderbar. Auch nicht bei Start von einem USB-Stick!

Skype - Regelung an der TU Dresden

- Einsatz kann vom zuständigen Leiter untersagt werden
- Deaktivierung „Skype bei Betriebsystemstart ausführen“
- Deaktivierung Autologin
- Account in Skype darf keine Daten von Accounts der TU Dresden verwenden
- Skype im Datennetz der TU Dresden nur über Port 41234
- Deaktivierung Supernode-Funktionalität unter Windows
- Aktuell vorgehaltener Virenscanner auf Skype Client

- Einsatz nur auf Systemen, die keinen besonderen Schutzbedarf haben
- Einsatz nur mit Kenntnis des zuständigen Leiters und in Absprache mit dem zuständigen Administrator
- Keine Dateiübertragung

Skype - Fazit

- Skype: VoIP-Software mit höchster Verbreitung (Apple Facetime)
- Skype Software Closed-Source
- Skype Protokoll proprietär und closed
- Sicherheitsbedenken bei Einsatz in geschützten Umgebungen
- Ressourcen der Universität werden ohne Wissen der Nutzer Skype zur Verfügung gestellt
- Datenschutz
- DFN Webkonferenz-Dienst als Alternative (Adobe Connect)
- Weitere Informationen: http://it-sicherheit.tu-dresden.de

Danke für Ihre Aufmerksamkeit!

TU Dresden

Zentrum für Informationsdienste und Hochleistungsrechnen

Kompetenzzentrum für Videokonferenzdienste

Frank Schulze

01062 Dresden

Tel.: 0351 / 463 354 38

E-Mail: frank.schulze@tu-dresden.de

http://vcc.zih.tu-dresden.de