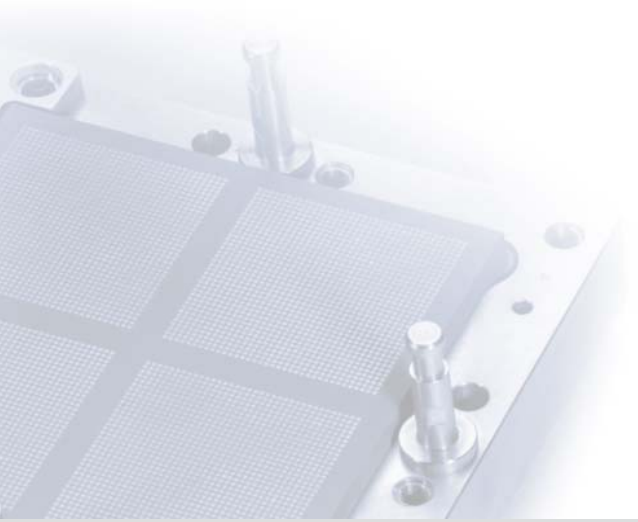
R|R|Z|N|
Regionales Rechenzentrum für Niedersachsen

Leibniz Universität Hannover

Sicherheitstage SS 2008

Skype an der LUH

Christine Peter
18. Juni 2008



Problematische Eigenschaften von Skype

- Proprietäres Protokoll
- Verschlüsselter Programmcode
- Unbemerkte Verbreitung von Schadcode
- Nutzt P2P-Technologie
- Liest sämtliche BIOS-Informationen aus
- Skype greift auf Userdaten, Informationen der Benutzerkonten und Daten aus der Datei /etc/passwd zu.
- Überwindet jegliche Art von Firewalls

Problematische Eigenschaften von Skype

- **Abhörsicherheit von Skype ist nicht erwiesen**
  - **Zitat (zdnet.de) Kurt Sauer, Chief Security Officer bei Skype:**

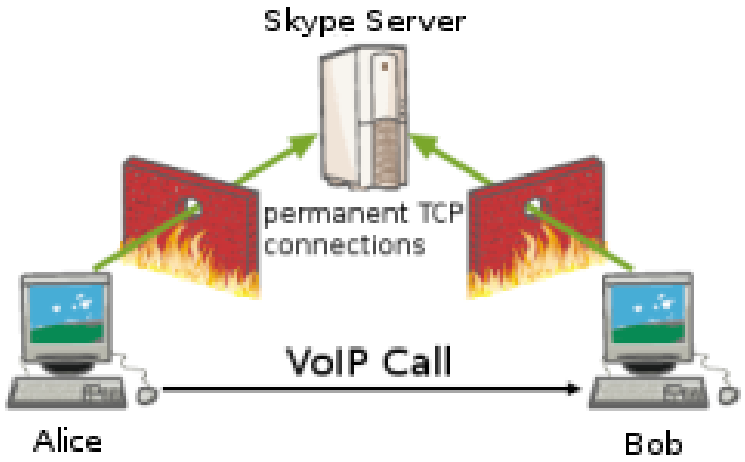
    „Wir stellen eine sichere Kommunikationsmöglichkeit zur Verfügung.

    Ich werde Ihnen nicht sagen, ob wir dabei zuhören können oder nicht.“

P2P-Technologie

- Jeder Skype-Client trägt das Potential zum Supernode.
- Delegation geschieht automatisch durch benachbarte Supernodes.
- Supernodes bieten Telefonbuch- und Vermittlungsdienste für andere Skype-Teilnehmer.
- Manchmal werden ganze Gespräch über den Supernode abgewickelt.
- Netzbelastung durch Supernodes ist erheblich.

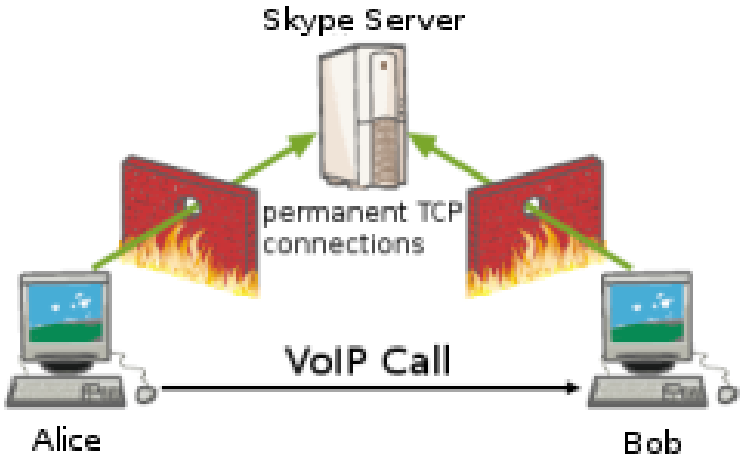
Überwindung von Firewalls: UDP Hole Punching



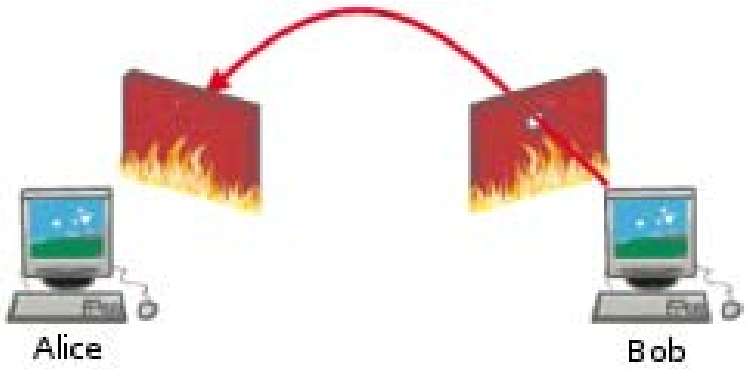
- Alice und Bob sind bei Skype angemeldet.
- Der Vermittlungsrechner kennt von beiden IP und Quellport.

Quelle der Bilder: Jürgen Schmidt - Skype & Firewalls
http://ph33r.org/updates/2006/12/17/skype-firewalls.html

Überwindung von Firewalls: UDP Hole Punching

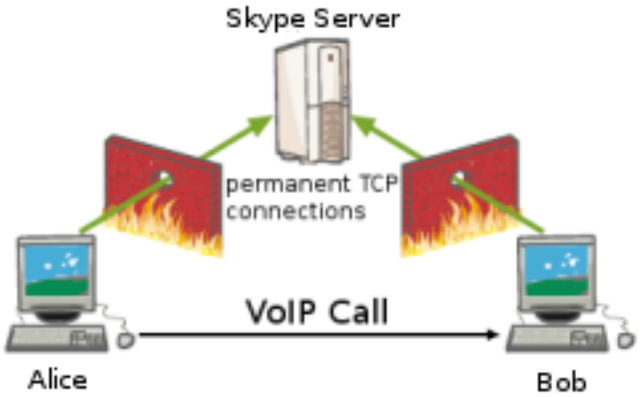


- Alice will Bob anrufen
- Der Vermittlungsrechner teilt dem Client von Bob IP, Port und Gesprächswunsch von Alice mit.

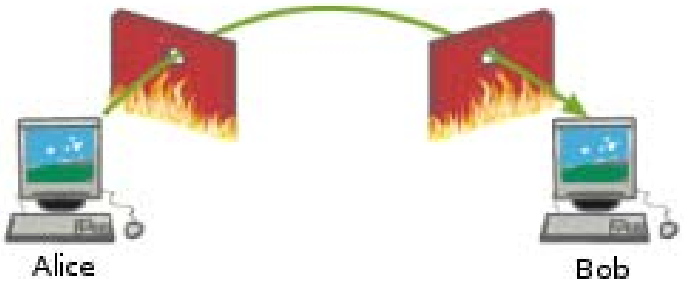


- Client von Bob schickt an Alice ein Paket mit dieser IP/Port-Kombination.
- Dadurch hat Bob seine Firewall für „Antworten“ von Alice geöffnet.

Überwindung von Firewalls: UDP Hole Punching



- Der Vermittlungsrechner teilt dem Client von Alice die IP von Bob mit und unter welchem Port er auf „Antworten“ von Alice wartet.



- Client von Alice versucht Bob mit der weitergegebenen IP/Portnummer zu erreichen.
- Bobs Firewall denkt, es handelt sich um eine Antwort der eben geöffneten Anfrage und lässt das Paket passieren.

Es klingelt bei Bob.

RRZN-Vorgaben: Konfiguration von Skype (1)

Prinzipiell:

Skype darf nicht auf Rechnern installiert werden, die wochen- oder auch nur tagelang durchlaufen müssen.

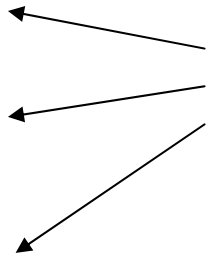
- Die Einstellung „Skype bei Windows-Start ausführen“ muss deaktiviert werden.
- Autologin muss deaktiviert werden.

Händisch im Client

RRZN-Vorgaben: Konfiguration von Skype (2)

Unter Menü-Punkt: "Aktionen - Optionen - Verbindungen:

- Den Port **41234** festlegen. (Einstellung der Oxford University).
- Die Ports 80 und 443 als Alternative nicht erlauben.



Ab Version 3.0

- Über einen Registry-Eintrag kann verhindert werden dass der Rechner zu einem Supernode wird.

Liegt als Datei luh-skype.reg zum Download unter

http://www.rrzn.uni-hannover.de/its_skype.html

RRZN-Vorgaben: Konfiguration von Skype (2a)

- Registry-Eintrag, der verhindert, dass der Rechner zu einem Supernode wird:
  HKEY_LOCAL_MACHINE\Software\Policies\Skype\Phone, DisableSupernode,
  REG_DWORD = 1
- Registry-Eintrag, der den vorgeschriebenen Skype-Port 41234 automatisch festlegt:
  HKEY_LOCAL_MACHINE\Software\Policies\Skype\Phone, ListenPort,
  REG_DWORD = 41234 (dezimal)
- Registry-Eintrag, der die Ports 80 (HTTP) und 443 (HTTPS) als Alternative verbietet
  HKEY_LOCAL_MACHINE\Software\Policies\Skype\Phone, ListenHTTPPorts,
  REG_DWORD = 0
- Liegt als Datei luh-skype.reg zum Download unter

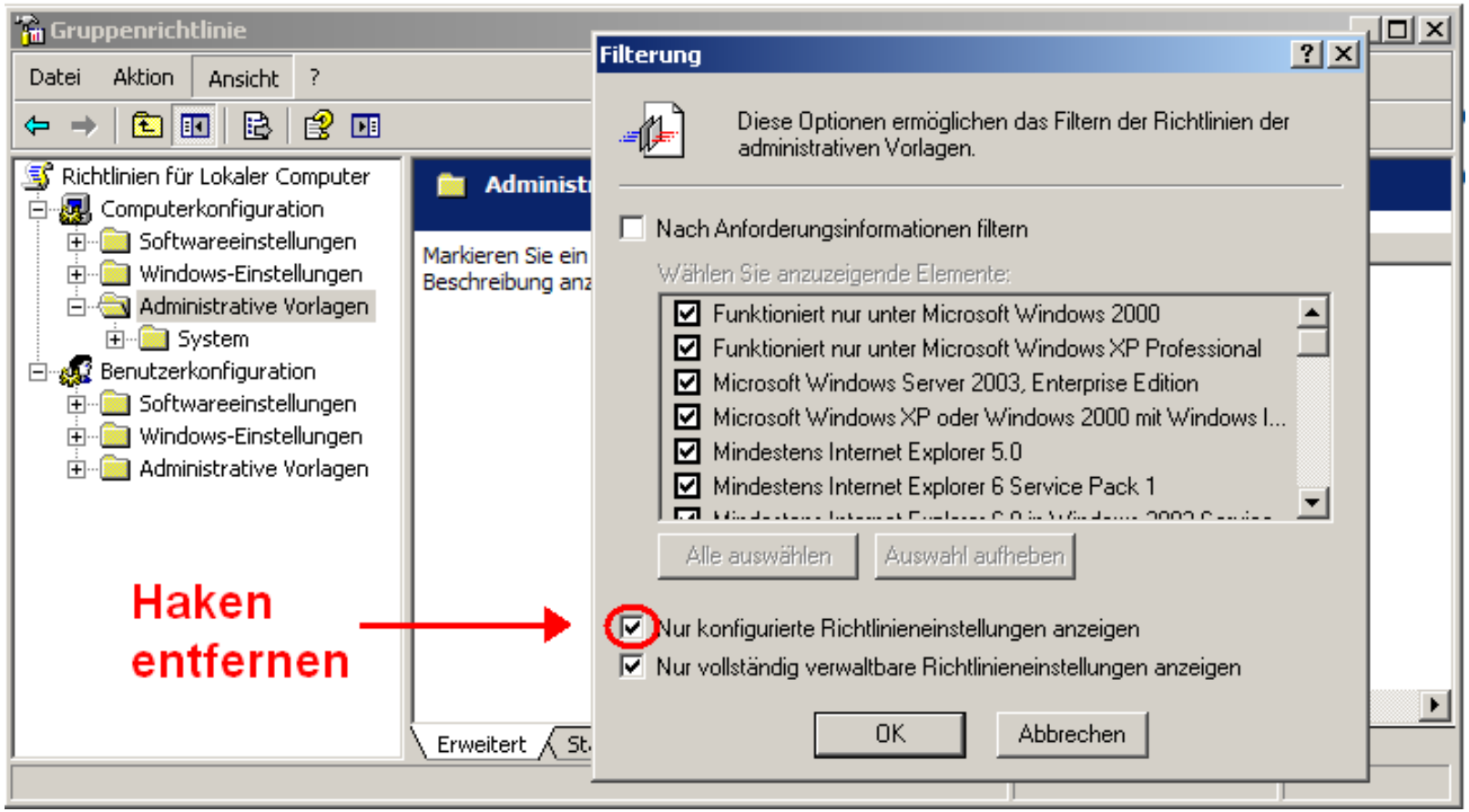
  http://www.rrzn.uni-hannover.de/its_skype.html

Zentrale Administration: Gruppenrichtlinien(1)

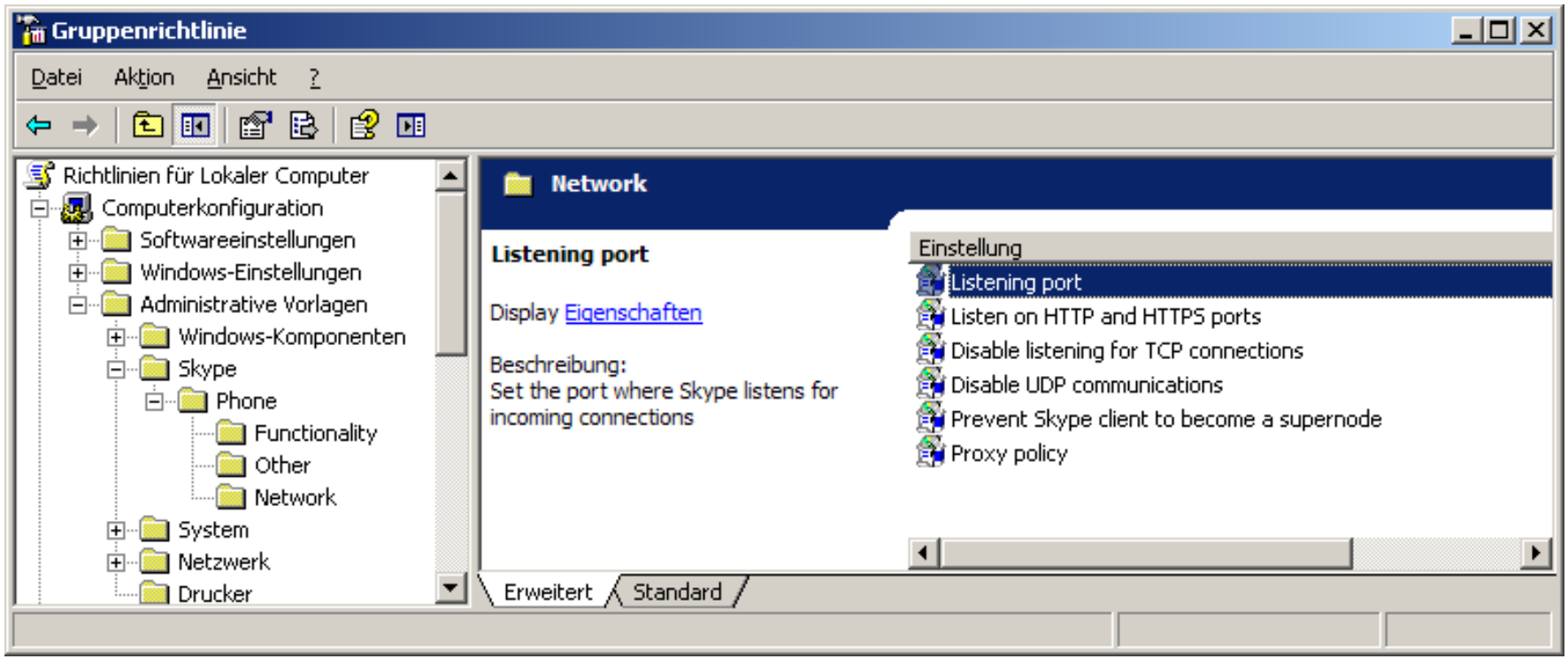
- Importierbare Administrative Vorlage von skype.com: skype-v1.5.adm
- Ausführliche Anleitung und Link zum Download der Datei unter
  - http://www.rrzn.uni-hannover.de/its_skype.html

    Abschnitt: Zusätzliche Informationen für Administratoren

Zentrale Administration: Gruppenrichtlinien(2)



Zentrale Administration: Gruppenrichtlinien(3)



Zentrale Administration: Gruppenrichtlinien(4)

```
Skype_v1.5.adm
; Skype Group Policies Administrative Template
;Copyright 2006, Skype Limited
;
; Change log:
; 1.0 - initial version
; 1.1 - added policies to CLASS USER
; 1.2 - added DisableUDP policy
; 1.3 - added DisableUDP policy to CLASS USER
; 1.4 - changed 1/0 settings to NUMERIC
; fixed ProxyPassword value name
; 1.5 - changed the max value for listen port policies to 65535
CLASS MACHINE
  CATEGORY !!SkypeCat
    CATEGORY !!PhoneCat
      KEYNAME "Software\Policies\Skype\Phone"
        ...
```

Bei Problemen:

Vor Import in der Datei Kommentarzeilen entfernen

Links zum Thema

- **http://www.rrzn.uni-hannover.de/its_skype.html**
- **http://www.skype.com/security/guide-for-network-admins-30beta.pdf**
- **http://www.skype.com/security/**
- **http://ph33r.org/updates/2006/12/17/skype-firewalls.html**
- **http://www.ossir.org/windows/supports/2005/2005-11-07/EADS-CCR_Fabrice_Skype.pdf („Skype uncovered“ Security-Study)**
- **http://www.blackhat.com/presentations/bh-europe-06/bh-eu-06-biondi/bh-eu-06-biondi-up.pdf („Silver Needle in the Skype“)**