GEORG-SIMON-OHM
FACHHOCHSCHULE
NÜRNBERG

Internet Security Vortrag

SMB / CIFS Sicherheit

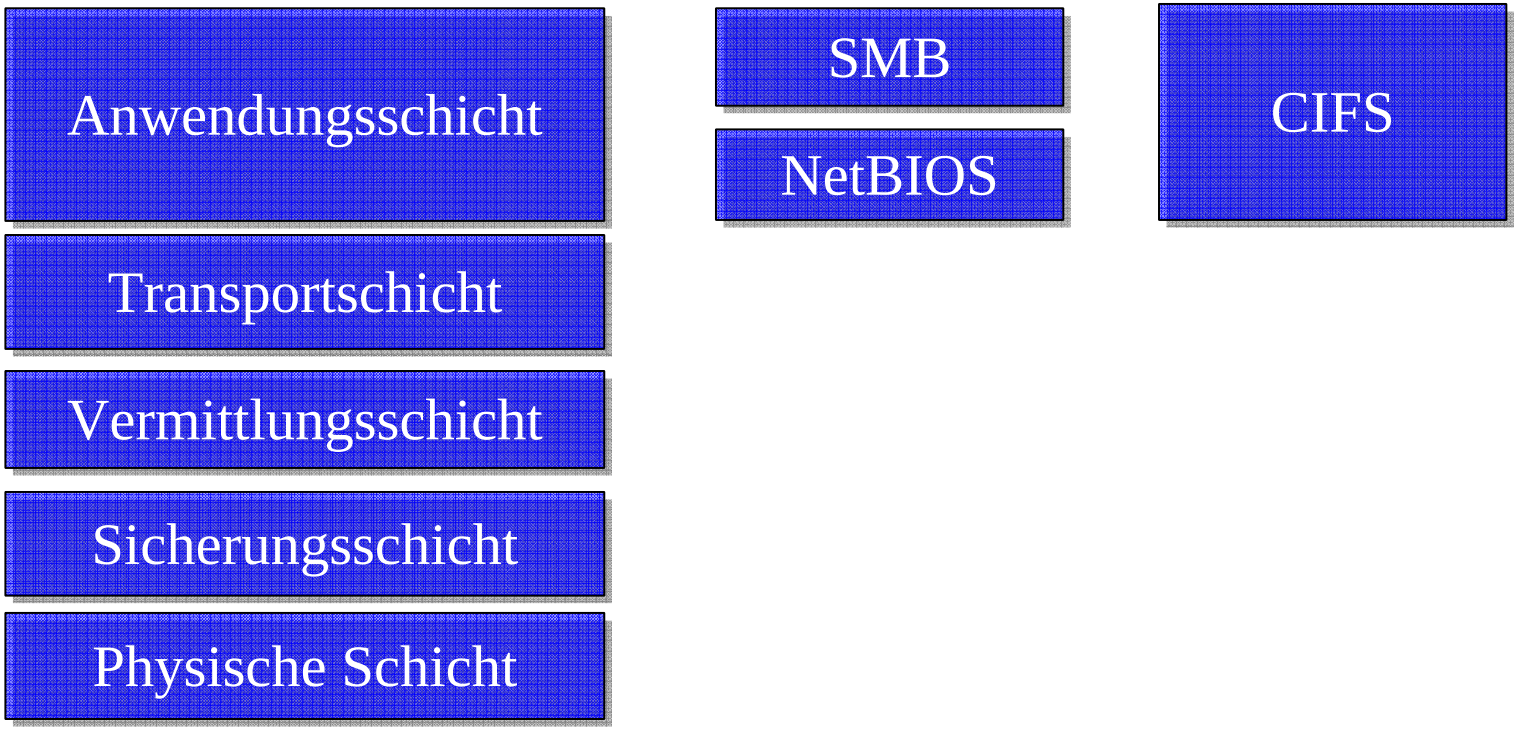
Mario Bacic

27.04.2004

Inhalt

1. Einordnung

Einordnung


Anwendungsschicht
Transportschicht
Vermittlungsschicht
Sicherungsschicht
Physische Schicht
SMB
NetBIOS
CIFS

2. Geschichte

Geschichte

GEORG-SIMON-OHM FACHHOCHSCHULE NÜRNBERG

Server **M**essage **B**lock Protokoll

- Anfang 1980 von MS und Intel entwickelt
- Datei und Druckerfreigabe in WfW und NT
- Anfang 1992 von Andrew Tridgell durch Reverse Engeering unter Unix implementiert
- Ende 1992 wird SMB “offener” Standard durch Open Group
- 1994 wird das “Open Source” Projekt SAMBA gestartet
- 1997 reicht MS ein CIFS Internet Drafts bei der IETF ein

GEORG-SIMON-OHM FACHHOCHSCHULE NÜRNBERG

3.Klassisches SMB Protokoll

- NetBIOS über TCP/IP
- Sicherheitsmodelle
- SMB Sitzung

Klassisches SMB Protokoll

"Da ist […] der klassische Browser-Dienst, der NetBIOS verwendet […]. Dieses Kapitel bringt Hintergründe […], die helfen sollen, das manchmal recht obskure Verhalten verstehen zu können."

Aus „Microsoft Windows 2000 im Netzwerk“,
Microsoft Press 2002, Seite 329.

Klassisches SMB Protokoll

GEORG-SIMON-OHM FACHHOCHSCHULE NÜRNBERG

NetBIOS über TCP/IP (NetBT/ NBT)

- **NetBIOS** = **Net**work **B**asic **I**nput **O**utput **S**ystem
- 1985 von IBM für „PC Network“ entwickelte API
- Spezifiziert in RFC1001 und RFC1002
- Beschreibt Routinen zur Netzwerkkommunikation z.B. Sitzungsaufbau und Datentransfer
- Ermöglicht kein Routing
- **NetBEUI** = **NetB**IOS **E**xtended **U**ser **I**nterface

Klassisches SMB Protokoll

GEORG-SIMON-OHM FACHHOCHSCHULE NÜRNBERG

NetBIOS Bestandteile

- Name Service UDP Port 137
  - Namensverzeichnis aller Netzteilnehmer
- Datagram Service UDP Port 138
  - Austausch von Kontrollinformationen
- Session Service TCP Port 139
  - Zuverlässiger Sitzungsdienst

Klassisches SMB Protokoll

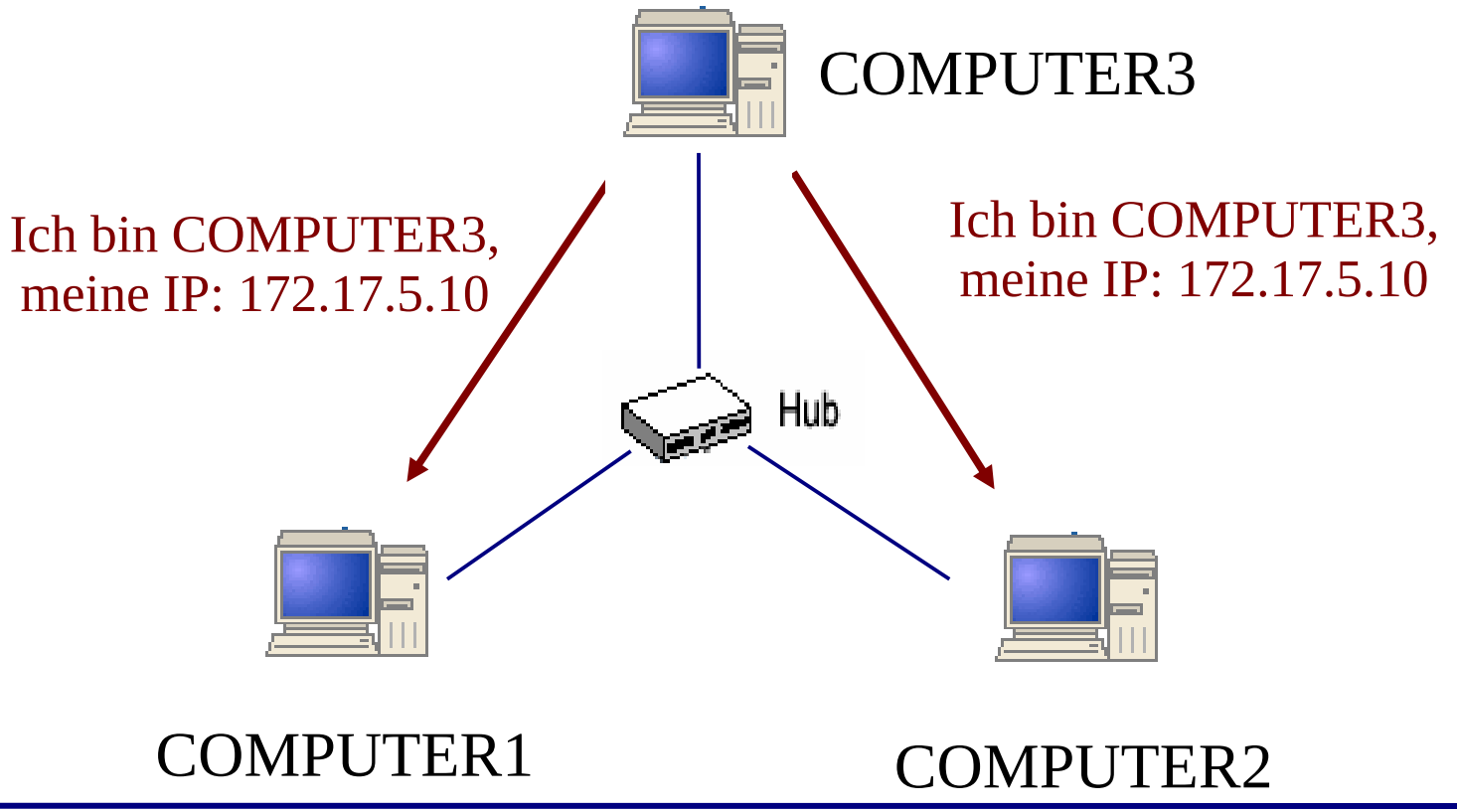
GEORG-SIMON-OHM FACHHOCHSCHULE NÜRNBERG

NetBIOS Name Service

- Dynamisches Verzeichnis aller Teilnehmer
- NetBIOS Namen identifizieren Netzteilnehmer (15 Bytes + 1 Byte Suffix)
- Enthält Einzel- und Gruppenbezeichnungen z.B. für Client- und Arbeitsgruppennamen
- Realisierung durch Broadcasts und/oder NetBIOS Name Server

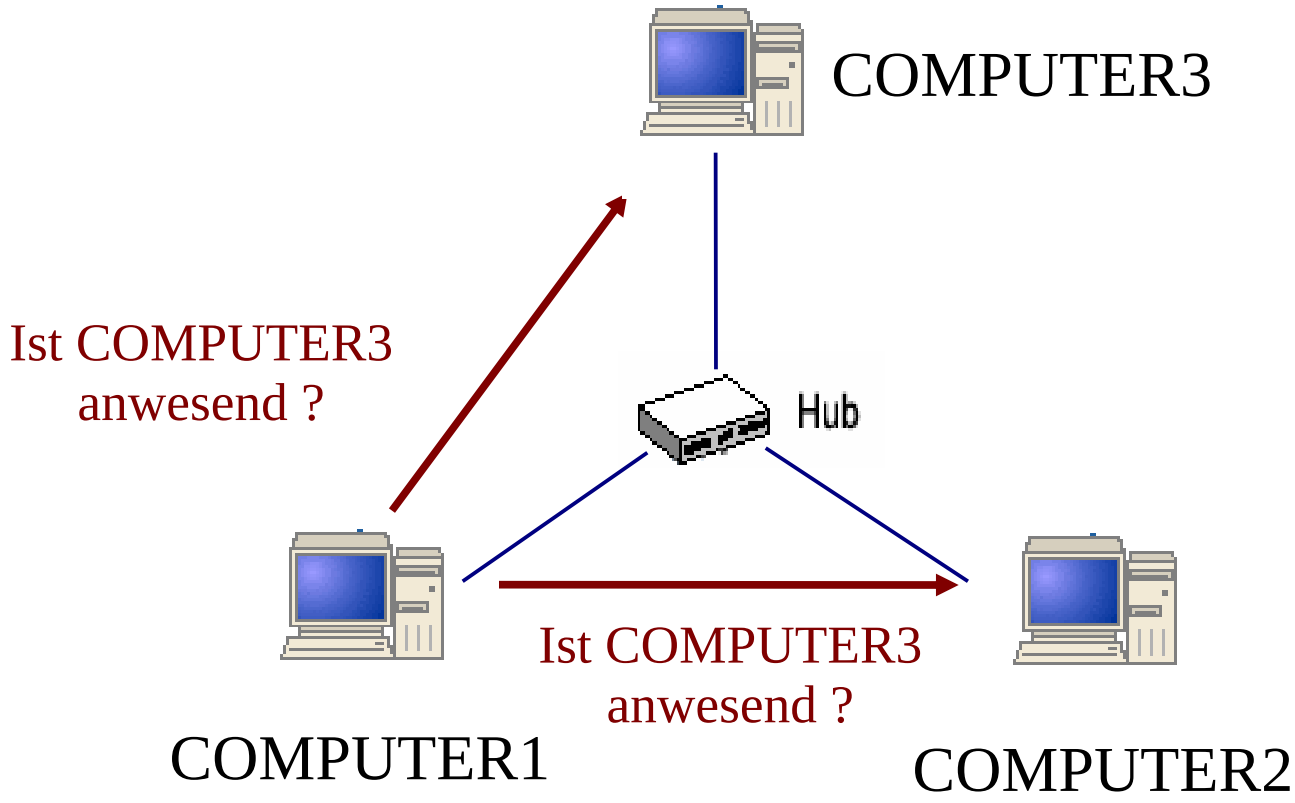
Klassisches SMB Protokoll

Registrierung durch Broadcast



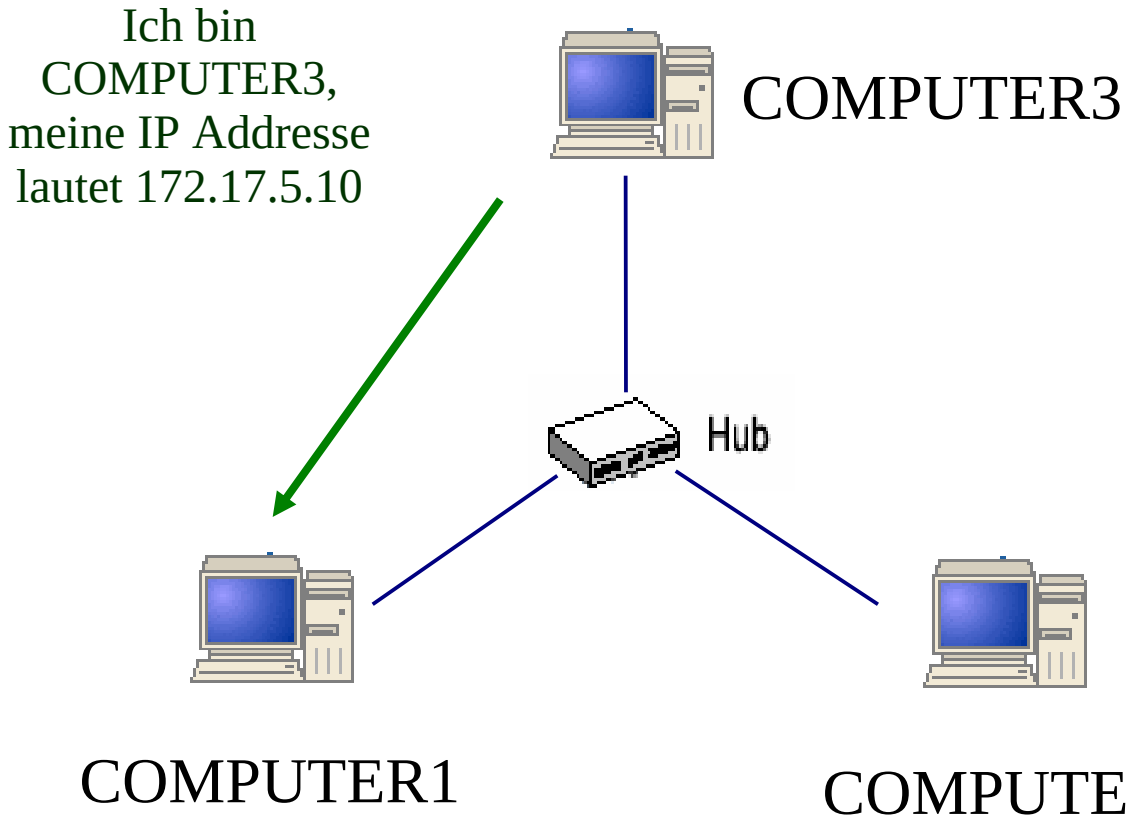
Klassisches SMB Protokoll

Namensabfrage durch Broadcast



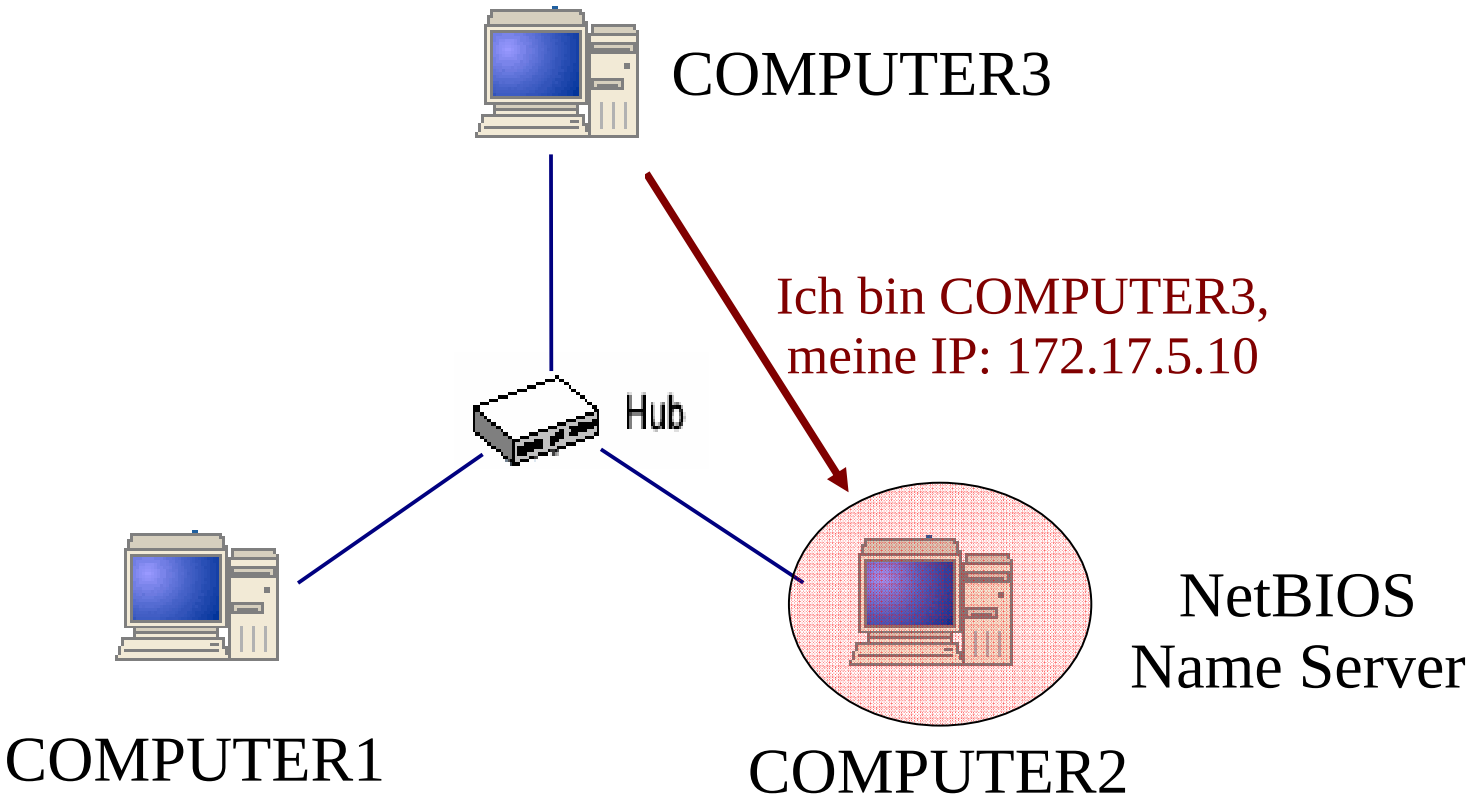
Klassisches SMB Protokoll

Namensabfrage durch Broadcast (2)



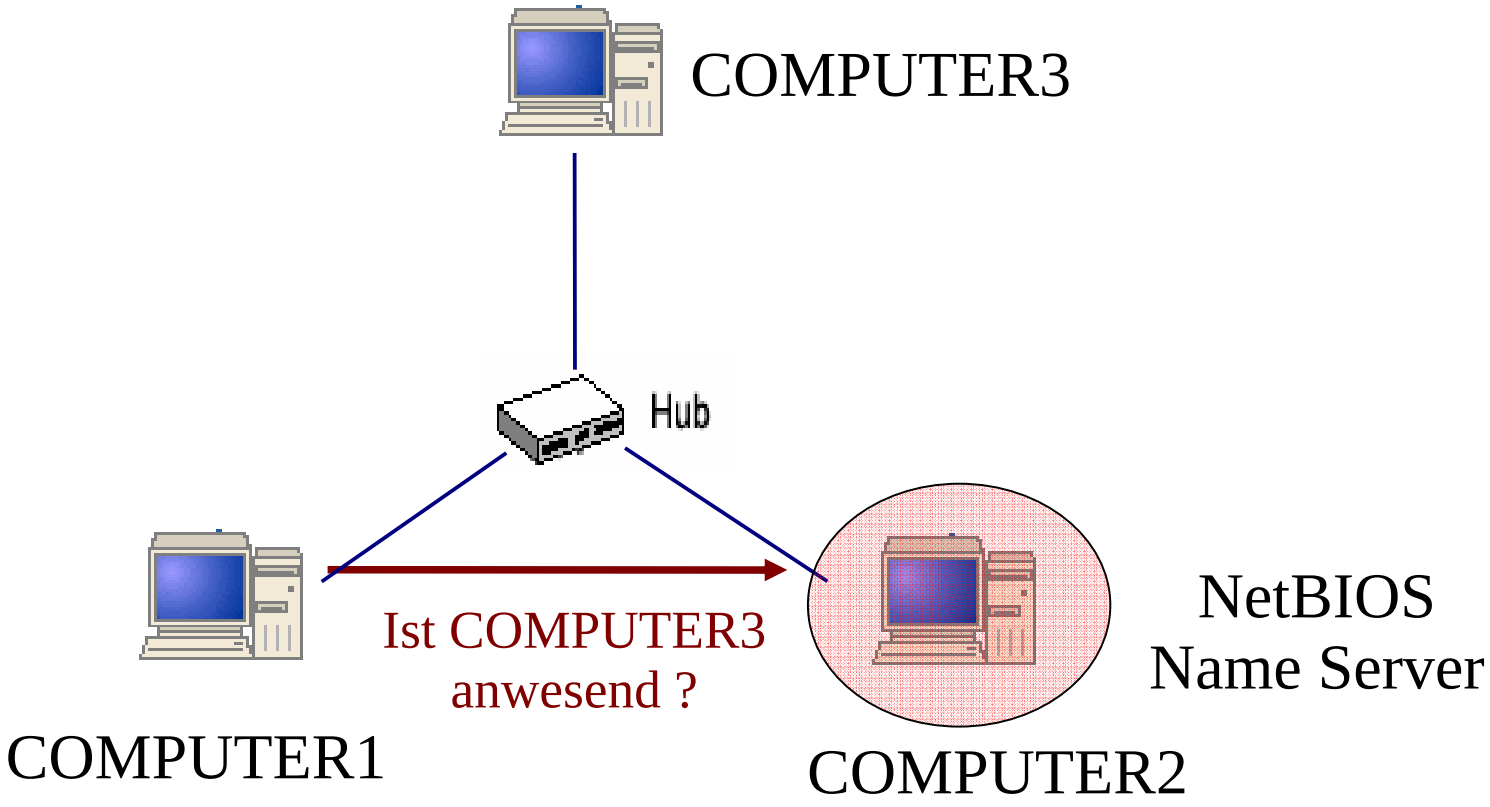
Klassisches SMB Protokoll

Registrierung durch NetBIOS Name Server



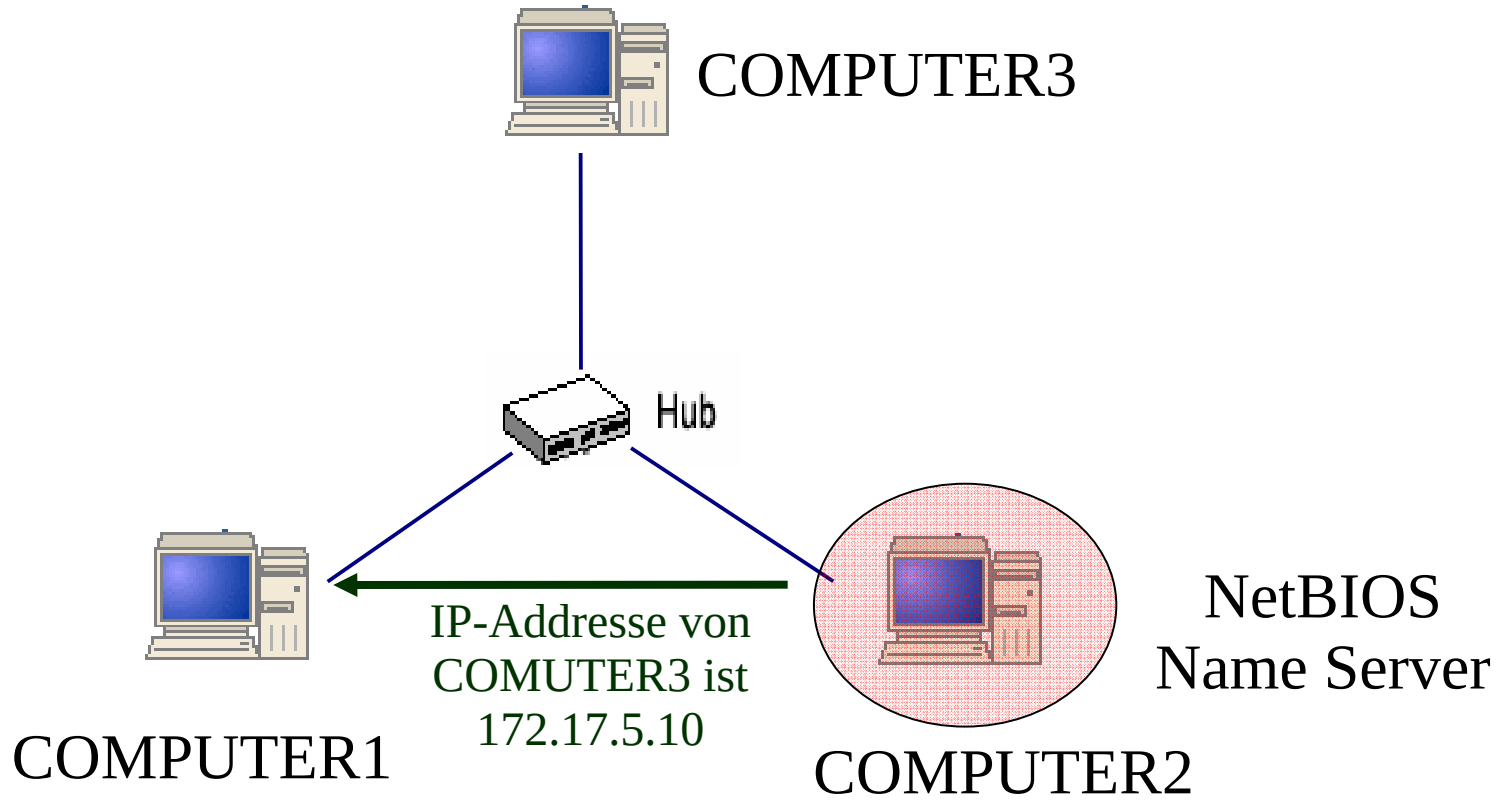
Klassisches SMB Protokoll

Namensabfrage durch NetBIOS Name Server



Klassisches SMB Protokoll

Namensabfrage durch NetBIOS Name Server(2)



Klassisches SMB Protokoll

GEORG-SIMON-OHM FACHHOCHSCHULE NÜRNBERG

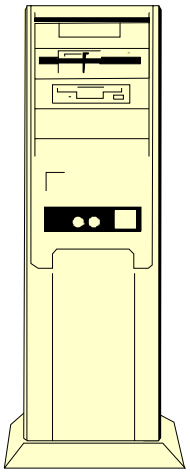
SMB Sicherheitsmodelle

- Freigabeebene
- Benutzerebene
- Zugriff durch Passwort
  - Unverschlüsselt
  - Challenge and Response Verfahren

Klassisches SMB Protokoll

Challenge and Response Verfahren

Server



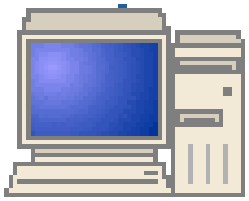
Verbindungsanforderung

Senden einer Challenge

Antwort mit der verschlüsselten Challenge

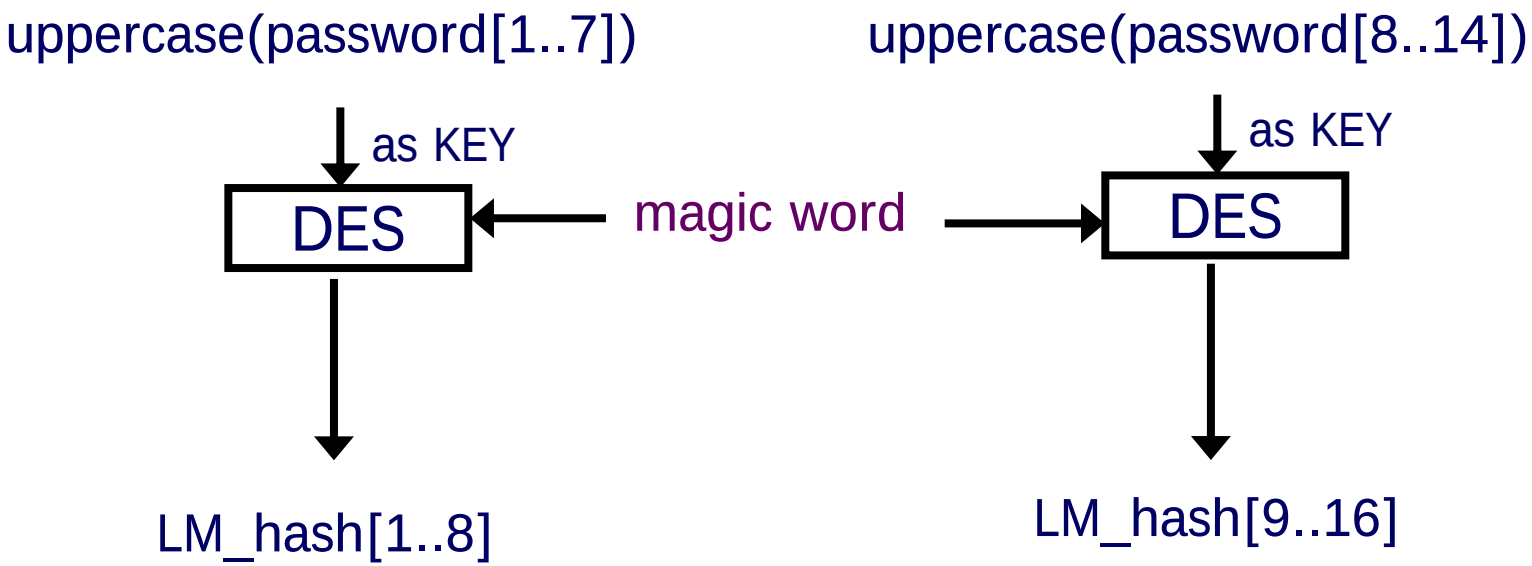
Meldung des Authentisierungsergebnisses

Client



Klassisches SMB Protokoll

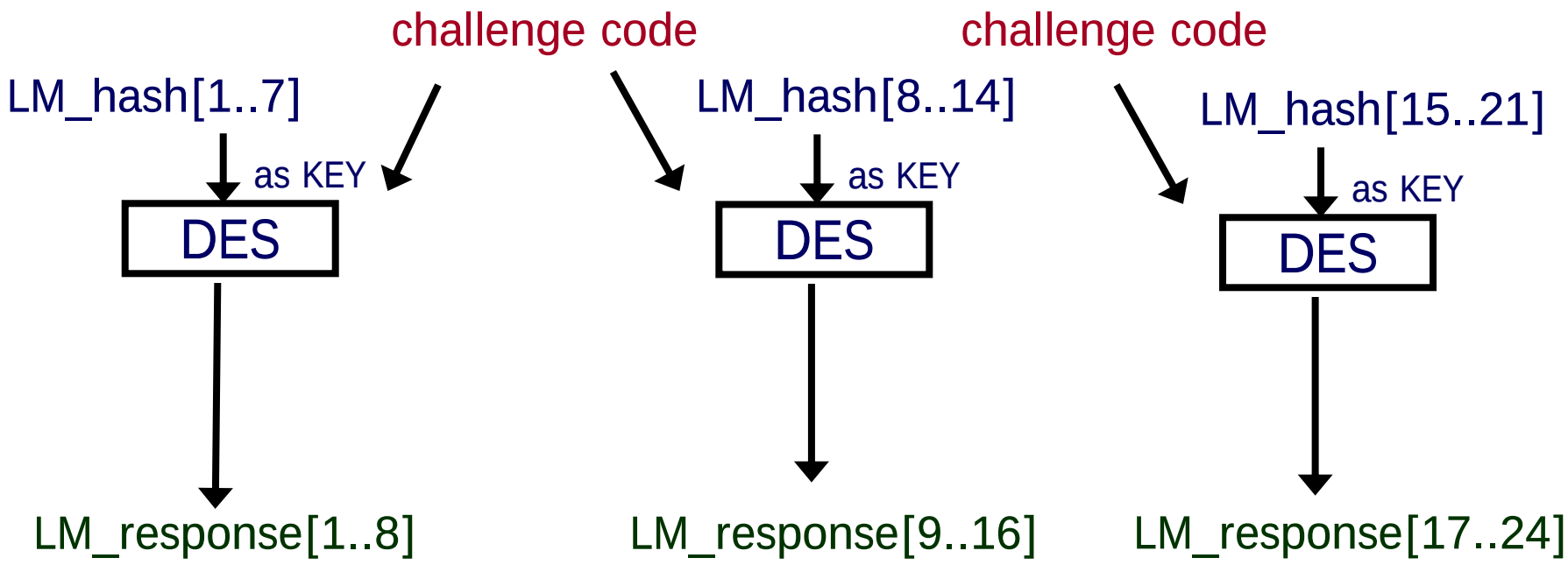
LAN Manager (LM) Challenge and Response



LM_hash[17..21] = 00 00 00 00 00

Klassisches SMB Protokoll

LAN Manager (LM) Challenge and Response (2)



Klassisches SMB Protokoll

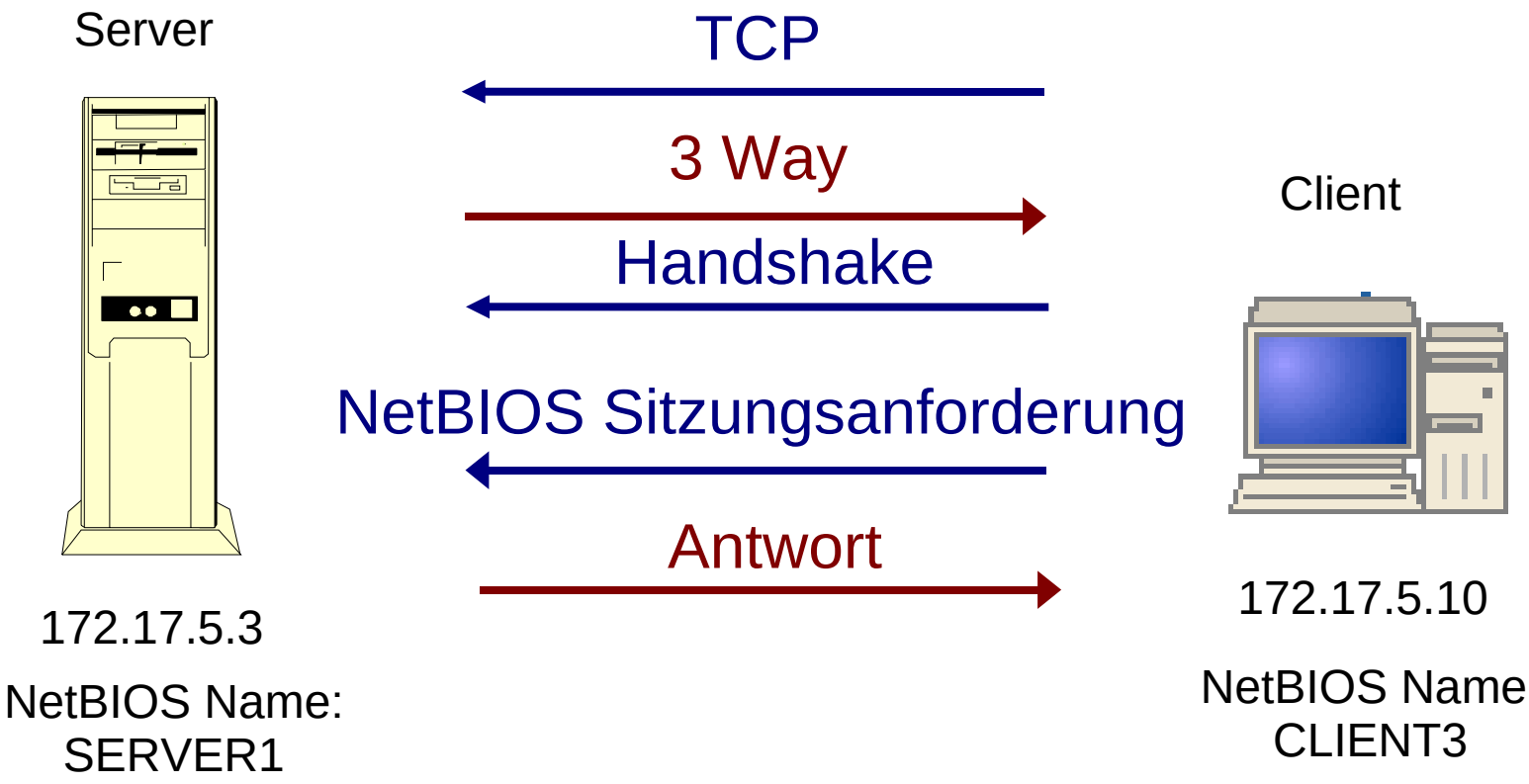
GEORG-SIMON-OHM FACHHOCHSCHULE NÜRNBERG

Challenge and Response Erweiterungen

- NT LAN Manager (NTLM)
  - Keine Konvertierung in Großbuchstaben
  - MD4 Hash-Algorithmus
- NT LAN Manager v2 (NTLMv2)
  - Keine Konvertierung in Großbuchstaben
  - MD4 Hash- & MD5 Verschlüsselungs-Algorithmus

Klassisches SMB Protokoll

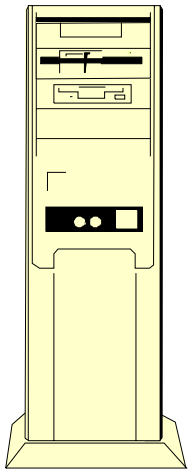
SMB Sitzungsaufbau



Klassisches SMB Protokoll

SMB Sitzungsaufbau (2)

Server



172.17.5.3

NetBIOS Name:
SERVER1

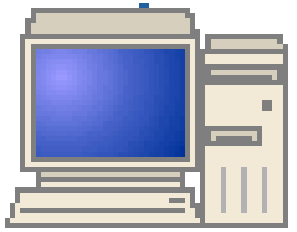
SMB Dialekte vorschlagen

Einen Dialekt auswählen
Optional: 8 Byte Challenge

SMB Session Setup
Benutzername,Passwort

Ergebnis der
Authentisierung mitteilen

Client



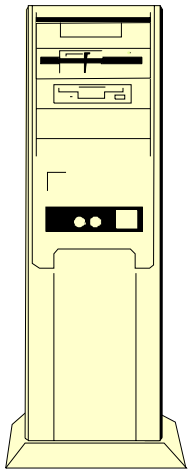
172.17.5.10

NetBIOS Name:
CLIENT3

Klassisches SMB Protokoll

Zugriff auf SMB Freigaben

Server



172.17.5.3

NetBIOS Name:
SERVER1

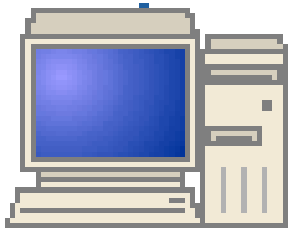
IPC$ Verbindungsanf.

Ergebnis der Anforderung

Ausführen einer Transaktion

Ergebnis der Transaktion

Client



172.17.5.10

NetBIOS Name:
CLIENT3

GEORG-SIMON-OHM FACHHOCHSCHULE NÜRNBERG

4. Erweiterungen in CIFS

Erweiterungen in CIFS

Common **I**nternet **F**ile **S**ystem

- SMB über TCP/IP (Port 445)
- DNS Namensauflösung
- General Security Service Provider
- Signieren von SMB Paketen

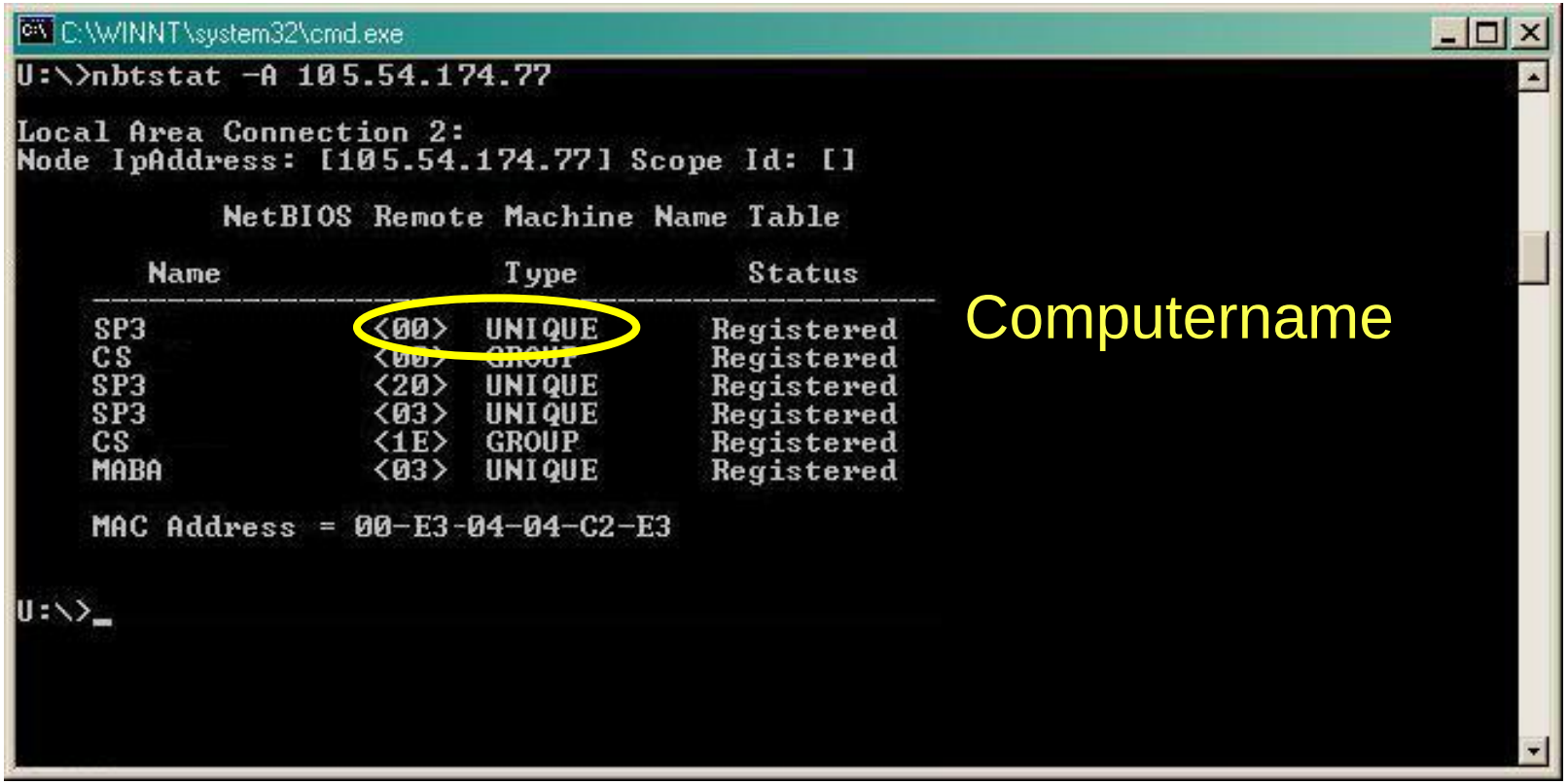
GEORG-SIMON-OHM FACHHOCHSCHULE NÜRNBERG

5. Sicherheitsrisiken

- NetBIOS über TCP/IP
- Authentisierungmechanismus
- Protokolldesign
- Implementierung
- Windows Standardeinstellungen

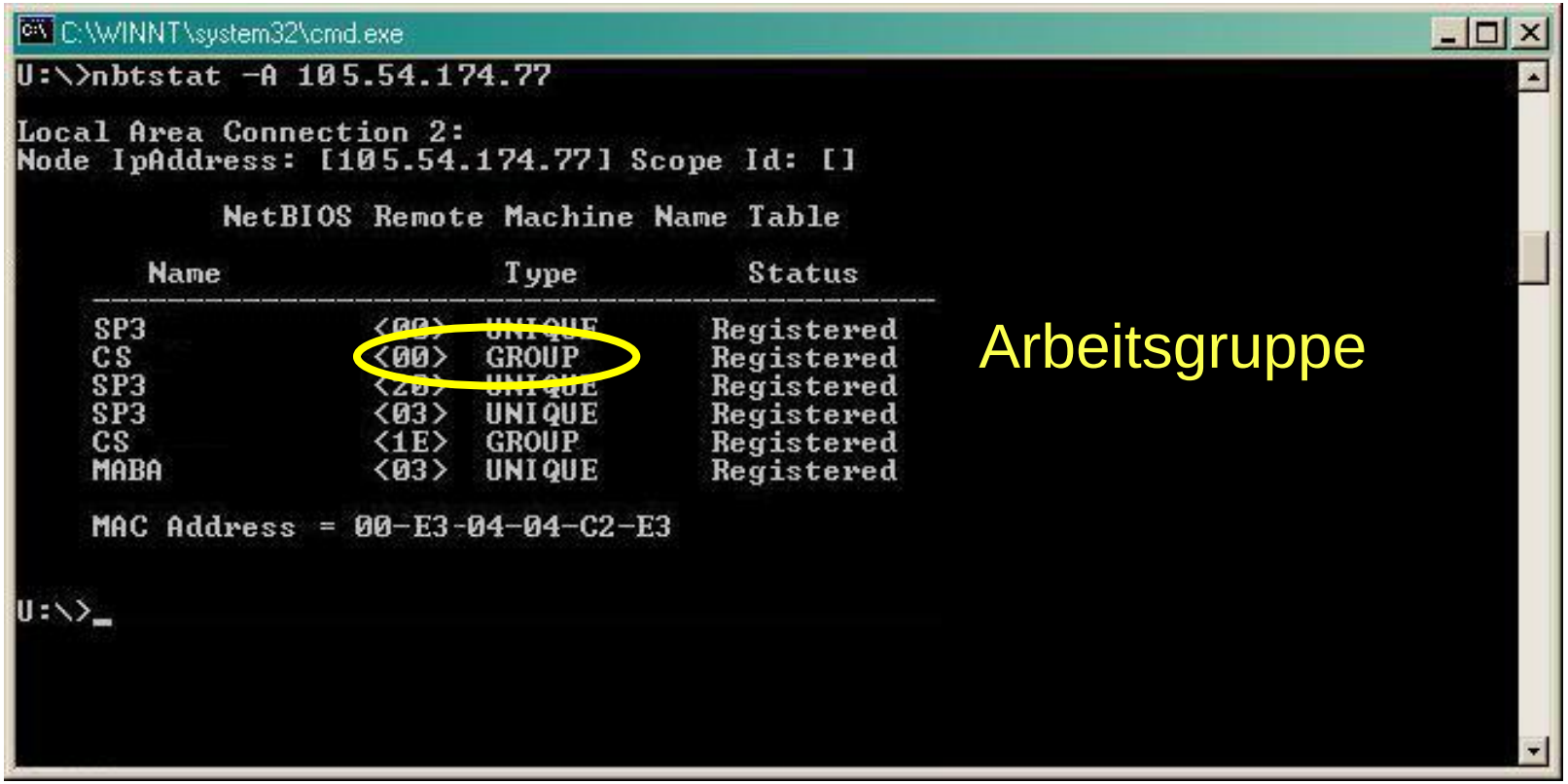
Sicherheitsrisiken

NetBIOS über TCP/IP



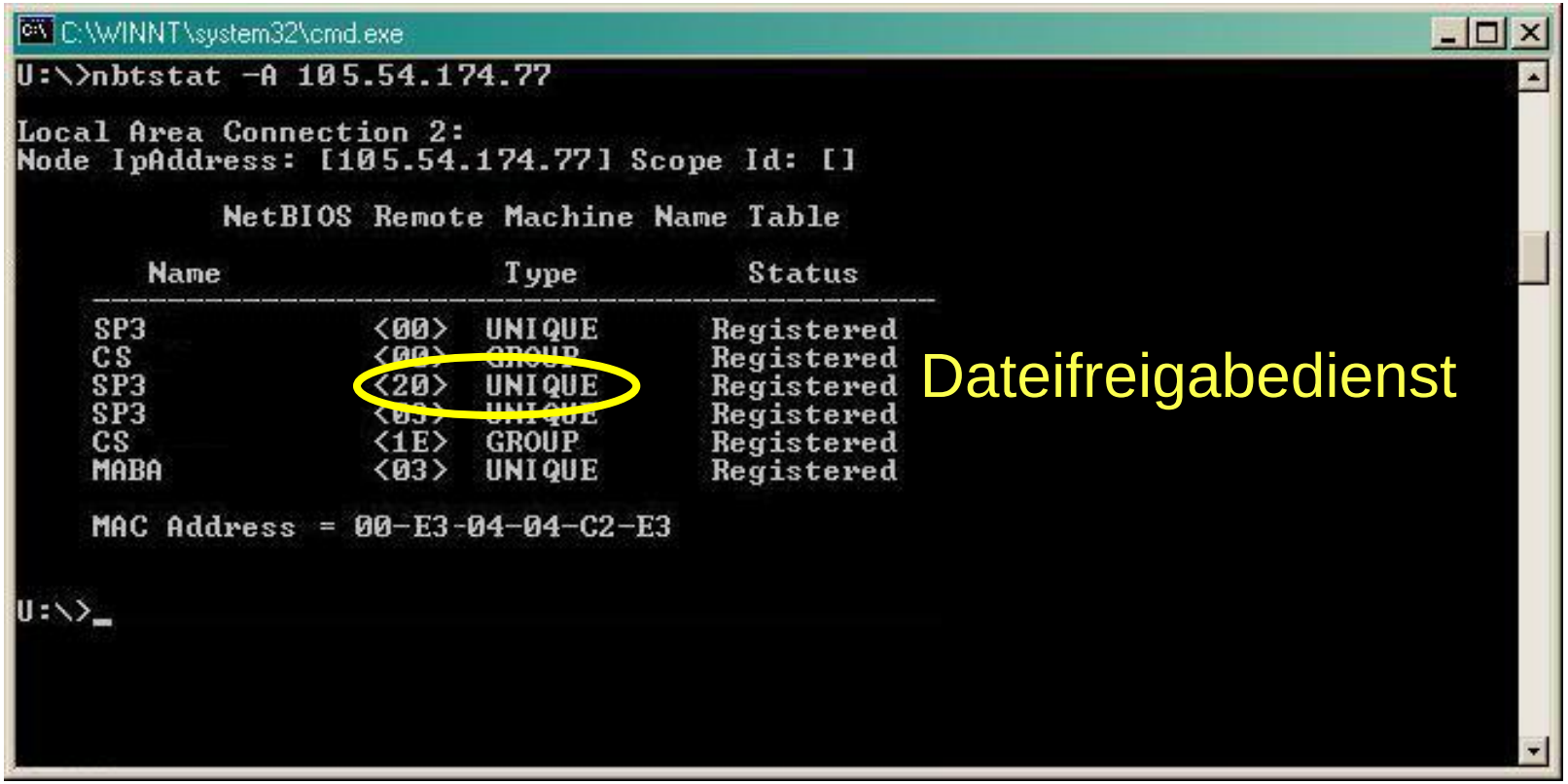
Sicherheitsrisiken

NetBIOS über TCP/IP (2)



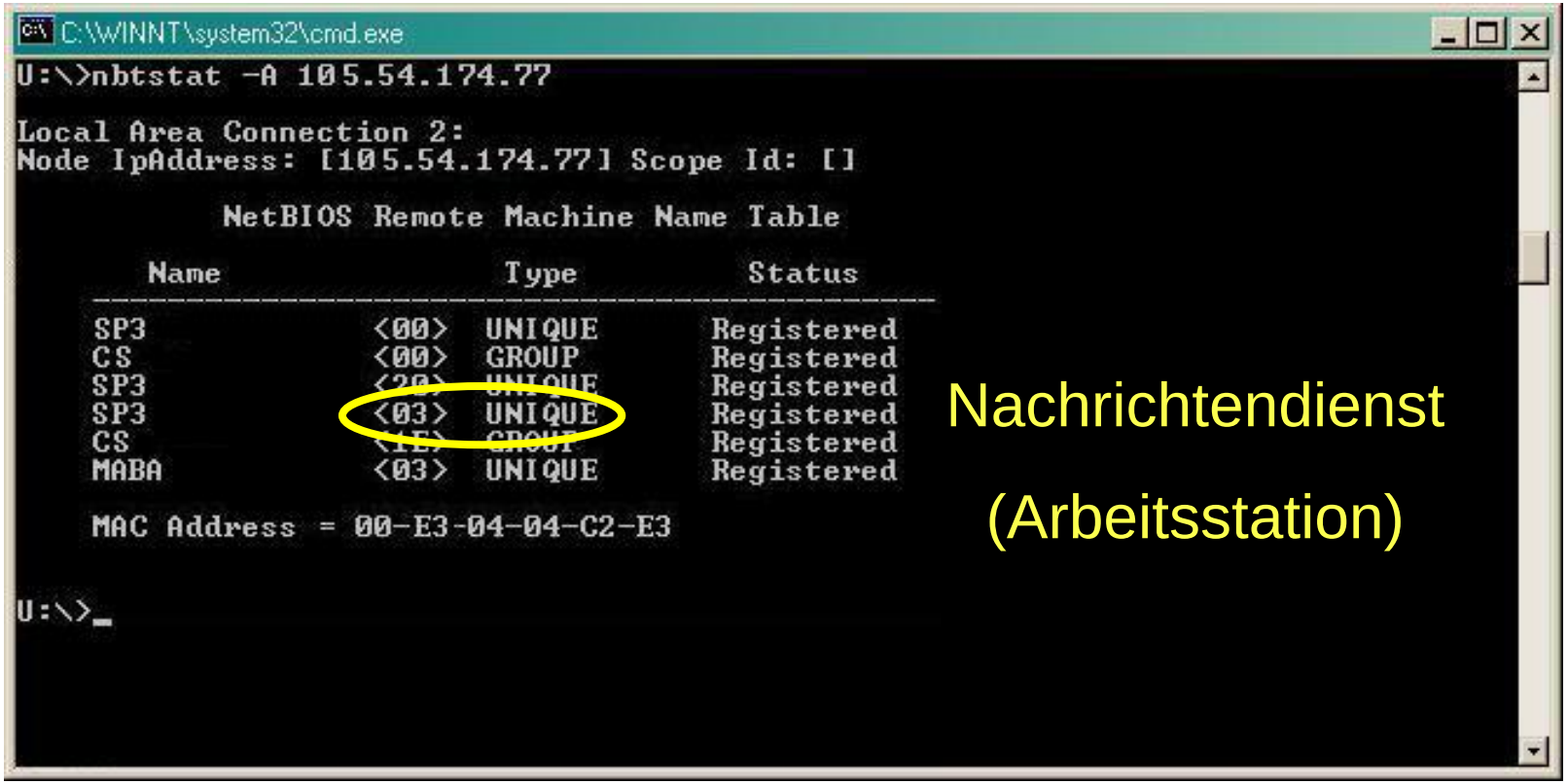
Sicherheitsrisiken

NetBIOS über TCP/IP (3)



Sicherheitsrisiken

NetBIOS über TCP/IP (4)

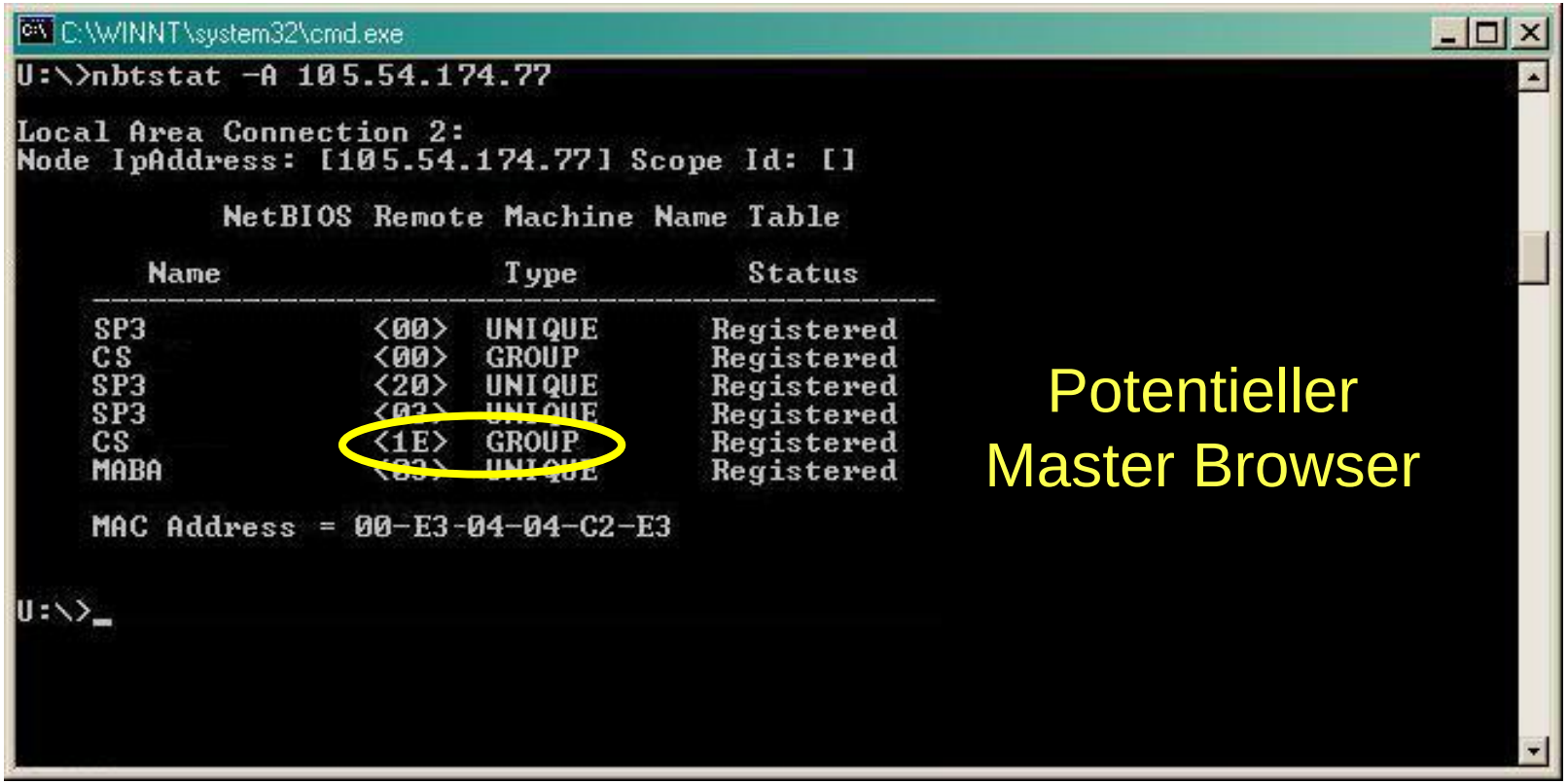


Nachrichtendienst

(Arbeitsstation)

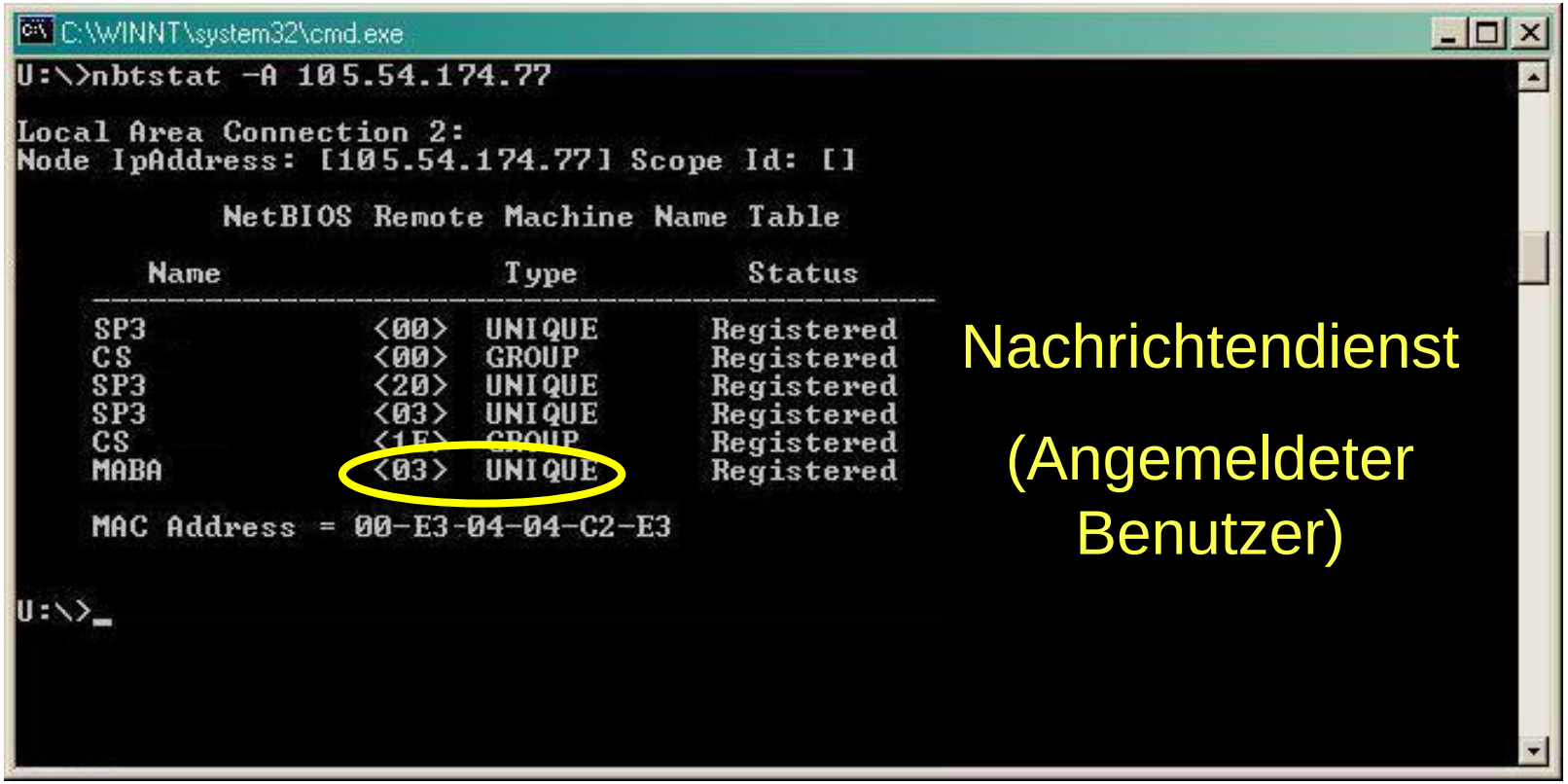
Sicherheitsrisiken

NetBIOS über TCP/IP (5)



Sicherheitsrisiken

NetBIOS über TCP/IP (6)



Nachrichtendienst

(Angemeldeter Benutzer)

Sicherheitsrisiken

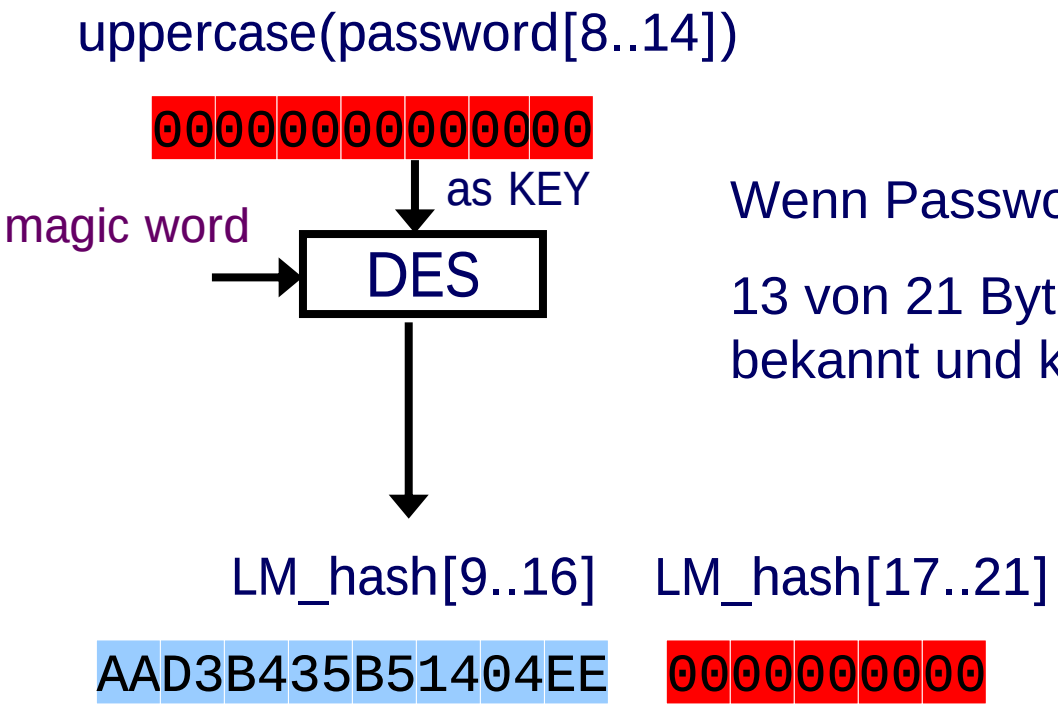
GEORG-SIMON-OHM FACHHOCHSCHULE NÜRNBERG

Schwächen von LM

- Passwort in Großbuchstaben
- Bruteforce Angriff wird durch Teilung des LM Hashwertes erleichtert

Sicherheitsrisiken

Schwächen von LM (2)

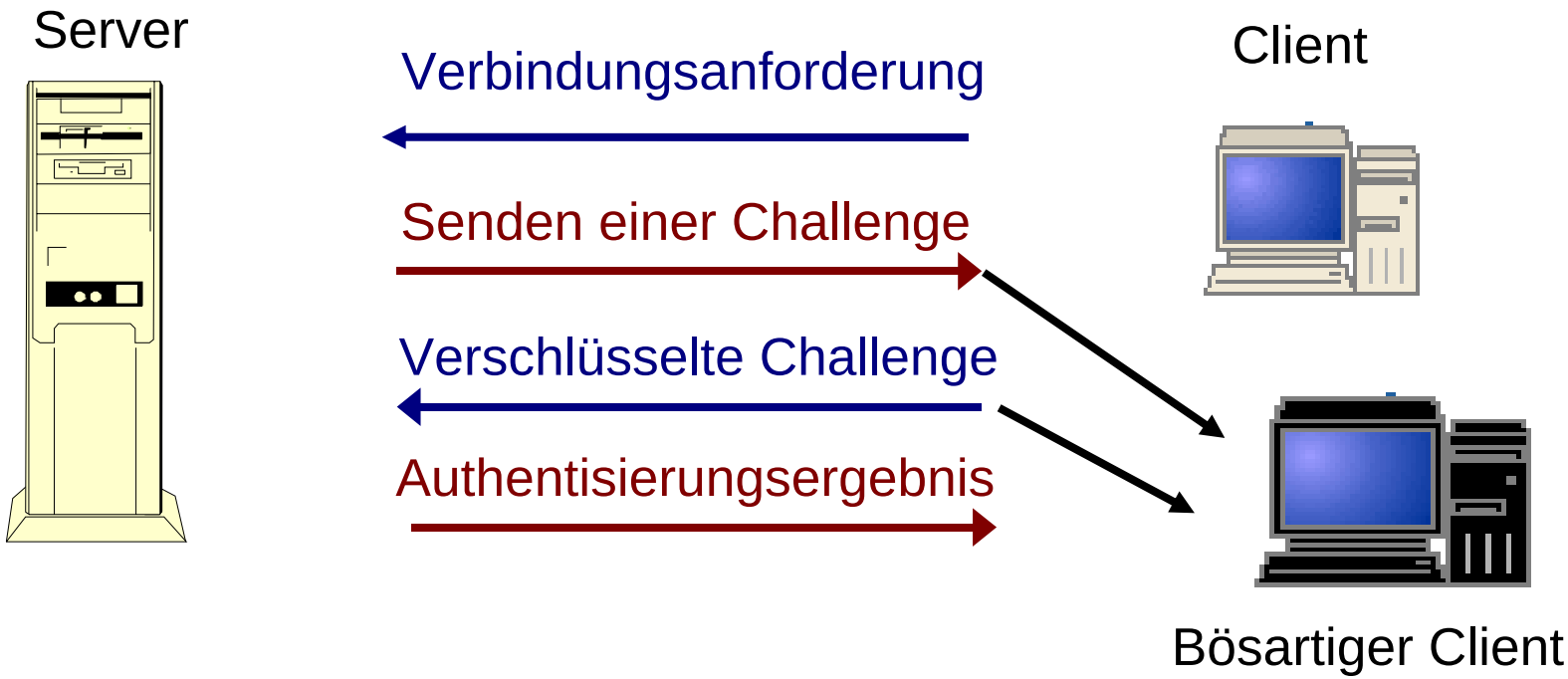


Wenn Passwort kürzer als 8 Zeichen ist:

13 von 21 Bytes der LM Hash sind bekannt und konstant

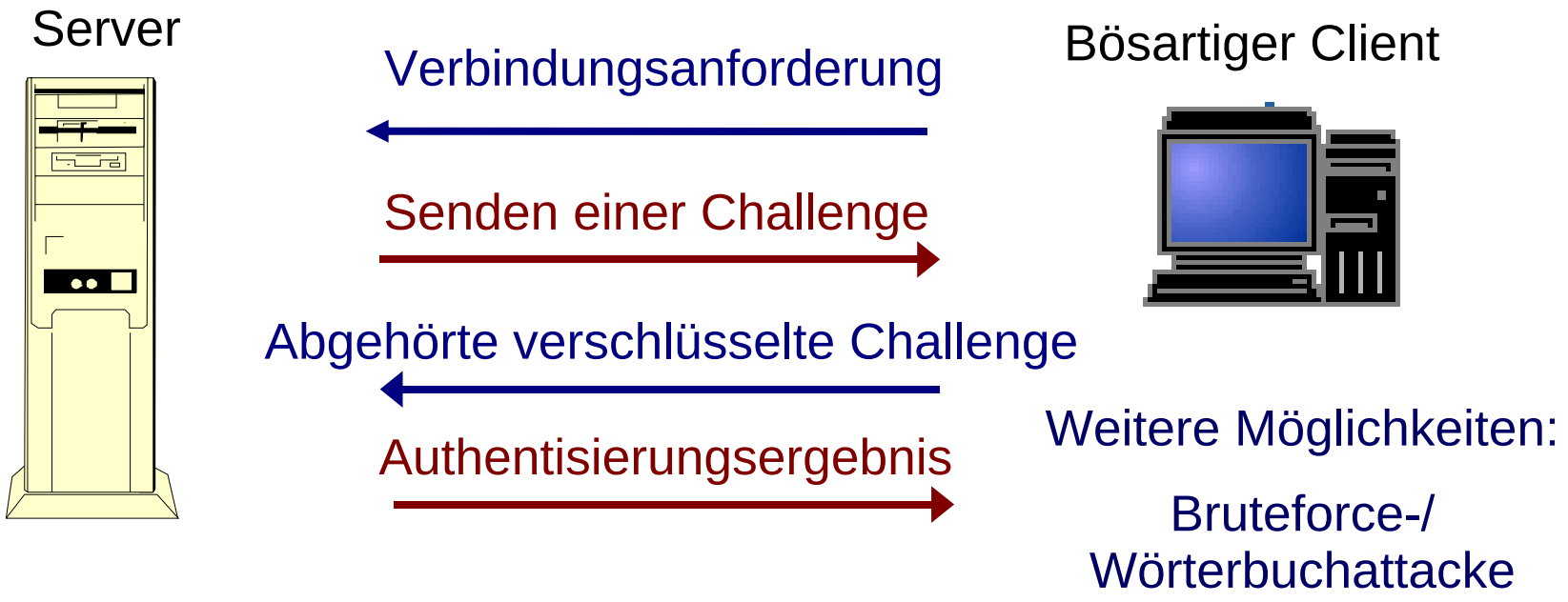
Sicherheitsrisiken

Replay-Attacke



Sicherheitsrisiken

Replay-Attacke (2)



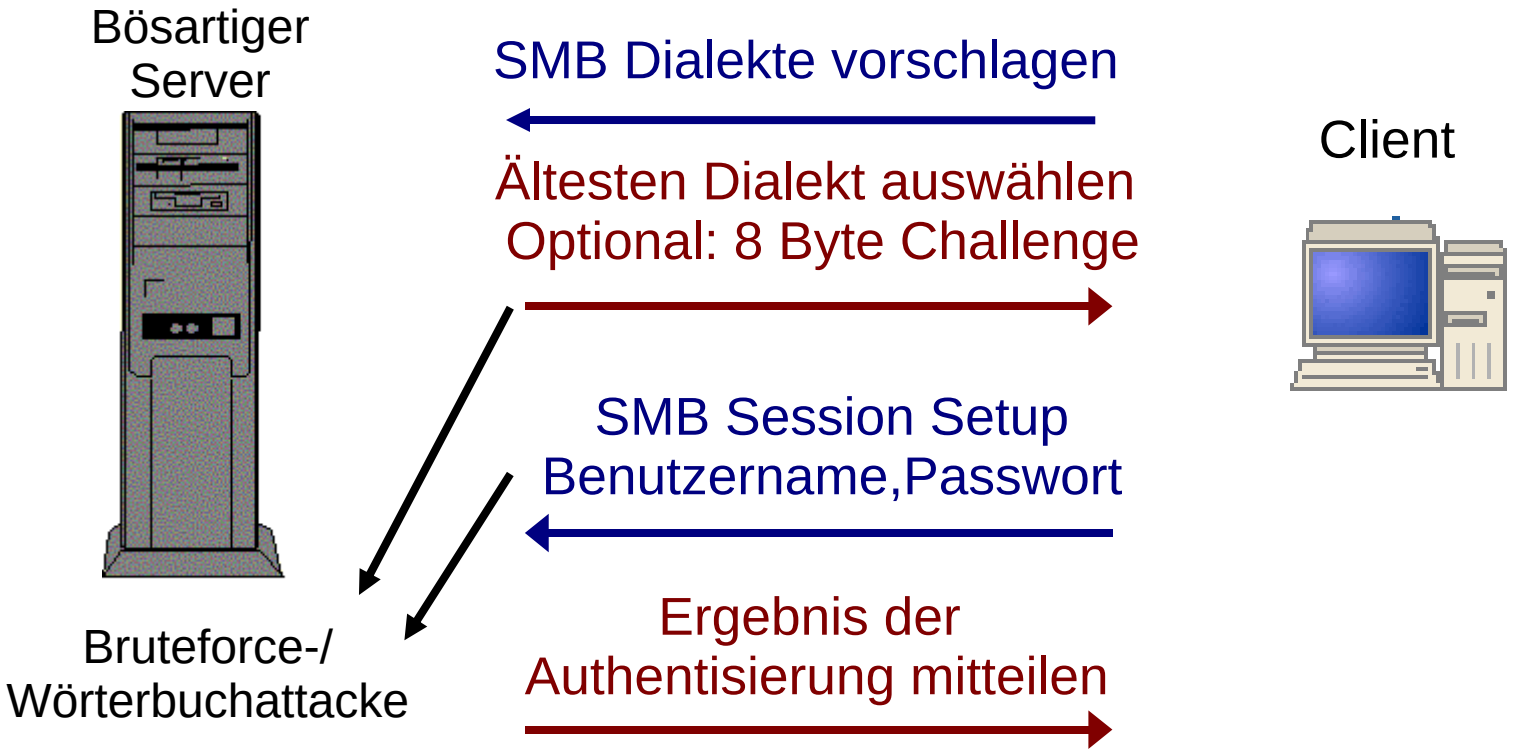
Sicherheitsrisiken

Protokolldesign

- “Anonymer Zugriff” auf „IPC$“ ermöglicht **alle** Freigaben und Benutzerkonten zu erfahren
- Kein Aushandeln der Authentisierungsmethode
- Hashwert ist Passwortäquivalent
- Downgrade Attacke

Sicherheitsrisiken

Downgrade Attacke



Sicherheitsrisiken

Implementierung

- Freigaben mit $-Endung sind **nicht** unsichtbar !
- SMB Pakete des Servers enthalten sensible Daten
  - Systemzeit und Zeitzone
  - Betriebssystemversion
  - Evtl. verwendetes Dateisystem
  - Evtl. Name der Computerdomäne
- Implementierungsfehler

Sicherheitsrisiken

Implementierung (2)

```
mambo:~> smbclient -L FROSCH
Password:
Domain=[FROSCH] OS=[Windows 5.0] Server=[Windows 2000 LAN Manager]

        Sharename       Type      Comment
        ---------       ----      -------
        IPC$            IPC       Remote-IPC
        ADMIN$          Disk      Remoteadmin
        C$              Disk      Standardfreigabe

        Server               Comment
        ---------            -------

        Workgroup            Master
        ---------            -------
mambo:~>
```

Sicherheitsrisiken

"To maintain compatibility with existing Server Message Block (SMB)-based products (for example, Microsoft Windows NT 3.x and 4.0, Microsoft Windows 95) […]"

Quelle: Microsoft Knowledge Base

Sicherheitsrisiken

Windows Standardeinstellungen

- Authentisierung erfolgt standardmäßig mit LM & NTLM verschlüsselter Challenge
- „Netcrawling“ von Windows is aktiviert
- Speichern der LM & NTLM Hashes in der Registry
- Administrative Freigaben (C$, ADMIN$) vorhanden
- Kein Administrator Passwort vorhanden (XP Home)
- NetBT Aktiviert

Sicherheitsrisiken

GEORG-SIMON-OHM FACHHOCHSCHULE NÜRNBERG

Top Schwachstellen in Windows Systemen (Stand 10/2003)

1. Internet Information Services (IIS)
2. Microsoft SQL Server (MSSQL)
3. Windows Authentcation
4. Internet Explorer (IE)
5. Windows Remote Access Services
6. Microsoft Data Access Components (MDAC)
7. Windows Scripting Host (WSH)
8. Microsoft Outlook / Outlook Express
9. Windows Peer to Peer File Sharing (P2P)
10. Simple Network Management Protocol (SNMP)

Quelle: www.sans.org

6. Gegenmaßnahmen

Gegenmaßnahmen

GEORG-SIMON-OHM FACHHOCHSCHULE NÜRNBERG

Empfohlene Maßnahmen

- “Netcrawling” deaktivieren
- Beschränkung der „NULL Session“
- Abschalten von NetBT
- Verwendung von Kerberos
- Nutzung einer Firewall

Verweise

Sans Institute, http://www.sans.org

Computer Emergency Response Team, http://www.cert.org

MS Knowledge Base, http://support.microsoft.com/default.aspx

Internet Engineering Task Force, http://www.ietf.org

Samba Homepage, http://www.samba.org

Schluß

GEORG-SIMON-OHM FACHHOCHSCHULE NÜRNBERG

Vielen Dank

für ihre Aufmerksamkeit !