Öffentliche Netzzugänge an der Uni Hamburg

Dr. Carsten Benecke
Regionales Rechenzentrum
Universität Hamburg

10. Workshop „Sicherheit in vernetzten Systemen“

25./26. Februar 2003 in Hamburg

Inhalt

- Motivation
- Anforderungen an öffentliche Netzzugänge
- Lösungsansätze
- Technische Umsetzung an der Uni Hamburg
- Erweiterungsmöglichkeiten
- Zusammenfassung

Motivation

- Dramatische Zunahme mobiler Rechner (Laptops)
- Zugriff auf Netzressourcen der Uni erwünscht:
  + Arbeitserleichterung für Studenten
  + Arbeitserleichterung für PC-Pool-Personal
  + Flächenversorgung mit Arbeitsplätzen
- Aber: z.Z. keine (offiziellen) Netzzugänge für private Rechner ⇒ „öffentliche Netzzugänge“

Motivation

„Öffentlicher Netzzugang“, was ist das?

- Neuer Dienst an öffentlichen Orten der Uni
  - Bibliotheken, Eingangsbereiche, Hörsäle
- Für Studierende und MitarbeiterInnen
- Kabel-basierter und kabelloser (WLAN) Zugang
- Anschluß eigener Geräte mit eigener Hardware (Schnittstellen werden nicht bereitgestellt!)

Anforderungen an öffentliche Netzzugänge

- Universitätsübergreifende Lösung
  - Unabhängig von der dezentralen Campusstruktur
  - Unabhängig von der jeweiligen Fachbereichsstruktur
- „Skalierbarkeit“
  - Potentiell hohe Anzahl von Benutzern
  - Ständig wechselnde BenutzerInnen
    - Neueinschreibungen
    - Exmatrikulation
    - Hohe Mitarbeiterfluktuation (z.B. befristete Stellen)

Anforderungen an öffentliche Netzzugänge

- Unabhängigkeit von der Netztechnologie
  - Zugangsbereich („Access-Bereich“):
    - Kabel-basierte Zugänge
      - Strukturierte Verkabelung
      - „Legacy“-LANs (BNC/„CheaperNet“)
    - Kabellose Zugänge (Funkzugänge)
      - Wireless LAN (z.Z. IEEE 802.11b)
  - Kernnetz („Backbone“)
    - Subnetz-Routing vs. „VLAN-Switching“

Anforderungen an öffentliche Netzzugänge

- Kontrollierter Zugriff auf das Internet
  - Zugriff erst nach erfolgreicher Authentifikation
    - Nur für Studierende und MitarbeiterInnen
  - Zugriff nur auf bestimmte Dienste
    - Sicherheitsaspekte beachten
      - Z.B. keine „Filesharing“-Protokolle“
    - Leistungsengpässe vermeiden
      - Z.B. keine „P2P“-Protokolle

Anforderungen an öffentliche Netzzugänge

- Aufwandsarme Administration
  - Vorhandene Benutzerdatenbanken benutzen
    - Vermeiden von zusätzlicher Verwaltung
  - Einfaches Authentifikationsverfahren
    - Vermeiden von Beratungsaufwand
  - Unkomplizierte Technik(en) verwenden
    - Vermeiden von Spezialwissen
    - Erhöhen der Robustheit der Infrastruktur

Anforderungen an öffentliche Netzzugänge

- Kosteneffizienz
  - Kosten pro Anschluß müssen gering sein
  - Beschaffungskosten
  - Installationskosten
    - WLAN vs. Kabel
    - „Vermessen vs. Verlegen“
  - Betriebskosten
  - Migrationskosten

Anforderungen an öffentliche Netzzugänge

- Herstellerunabhängigkeit
  - Vermeiden von proprietären Lösungen
  - Vermeiden der Präjudiz durch Erstbeschaffung
  - Vermeiden von Vorgaben für die Anwender
  - Offenbleiben für neue Standards/Technologien

⇨ Gewichtung aus Sicht des Betreibers

  - Aufwandsarme Administration
  - Sichere Authentifikation, Herstellerunabhängigk.

Lösungsansätze (für Authentifikation)

- Medium-spezifische Authentifikation
  - WEP-Verschlüsselung (Schlüsselkenntnis)
  - IEEE 802.1x (z.B. Radius-Abfrage)
- VPN-Techniken
  - RAS, L2TP, PPTP, IPSec
- Authentifikation auf der Anwendungsebene
  - WEB-basierte Authentifikation am Firewall

Medium-spezifische Authentifikation

- Hauptnachteil: Mehrere Techniken erforderlich!
- WEP ist unsicher
  - Schwache Verschlüsselung
  - Symmetrischer Schlüssel für alle Benutzer?
  - Proprietäre Ansätze unbrauchbar
- IEEE 802.1x nur für strukturierte Verkabelung
  - Keine Verschlüsselung
  - Was tun bei „shared Medium“ LANs ?

VPN-Techniken

- Häufig proprietär (PPTP und RAS)
  - Funktioniert (gut) mit Windows
  - Was tun wir mit Mac- und Unix-Benutzern?
- Erheblicher Verwaltungsaufwand
  - IPSec erfordert PKI
    - viel Arbeit für Inbetriebnahme (PKI-Konzept)
    - viel Arbeit im laufenden Betrieb (Zertifikate)
- \+ IPSec: „unschlagbare Sicherheit“

VPN-Techniken

- Erheblicher Aufwand für VPN-Gateways
  - Neue/unbekannte aktive Komponenten
    - „Kryptoboxen“ für Ver-/Entschlüsselung
    - Verzeichnisdienste (Zertifikate verwalten)
  - Zusätzliche Komponenten (Portpreise!)
    - Spezialhardware („Appliances“) ist teuer
    - Management der neuen Komponenten

Authentifikation auf Anwendungsebene

+ Geringer Administrationsaufwand
  + Keine Benutzerzertifikate
  + Verwendet vorhandene Benutzerdatenbanken
+ Abstrahiert von Netzeigenschaften
  + Geeignet für WLAN und kabel-basierte Zugänge
  + Geeignet für „shared“ und strukturierte Netze

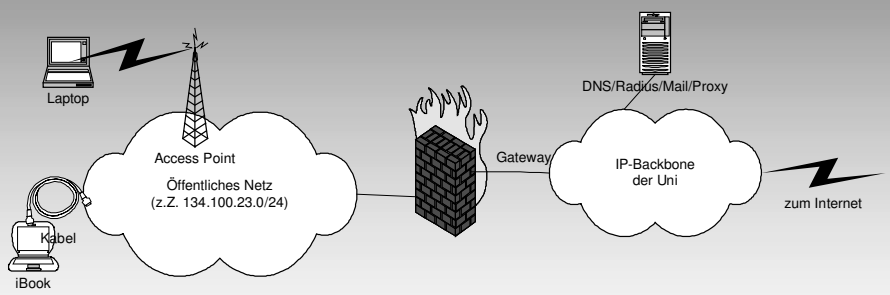
Authentifikation auf Anwendungsebene

+ Geringe Kosten
  + Spezialisierte Hardware ist nicht erforderlich
  + Herkömmliche FWL-Technik auf Universal-HW
  + Leicht zu skalieren (Neue Universal-HW)
+ Alternative Authentifikationsverfahren (freie SW!)
  + „WWW-Authentifikation“
  + „SSH-Authentifikation“

Authentifikation auf Anwendungsebene

- – Ambivalente Sicherheit
  - – Schutzniveau ist abhängig von Anwendung
  - – Einsatz unsicherer Dienste/Protokolle?
  - – Nicht alle Dienste/Protokolle verwendbar
- \+ Möglicher Ausweg
  - \+ STunnel für beliebte Dienste (z.B. Druckdienst)
  - ± Dienstangebot abhängig vom Medium?

Authentifikation auf Anwendungsebene



10. Workshop „Sicherheit in vernetzten Systemen“
Universität Hamburg Regionales Rechenzentrum

Authentifikation auf Anwendungsebene

Gründe für Authentifikation auf Anwendungsebene

+ Plattformunabhängigkeit, Mediumunabhängigkeit
+ Herstellerunabhängigkeit
+ Geringe Kosten
  + Universalhardware für Authentifikation/Gateway
  + Freie Software (OpenSSH, PAM-Radius, s.u.)
+ Gute Skalierbarkeit, Erweiterbarkeit, Migrationsfähigkeit
  + Software liegt im Quellcode vor (auch das OS!)
  + Hardware (Universalrechner) „wird von alleine schneller“

Authentifikation auf Anwendungsebene

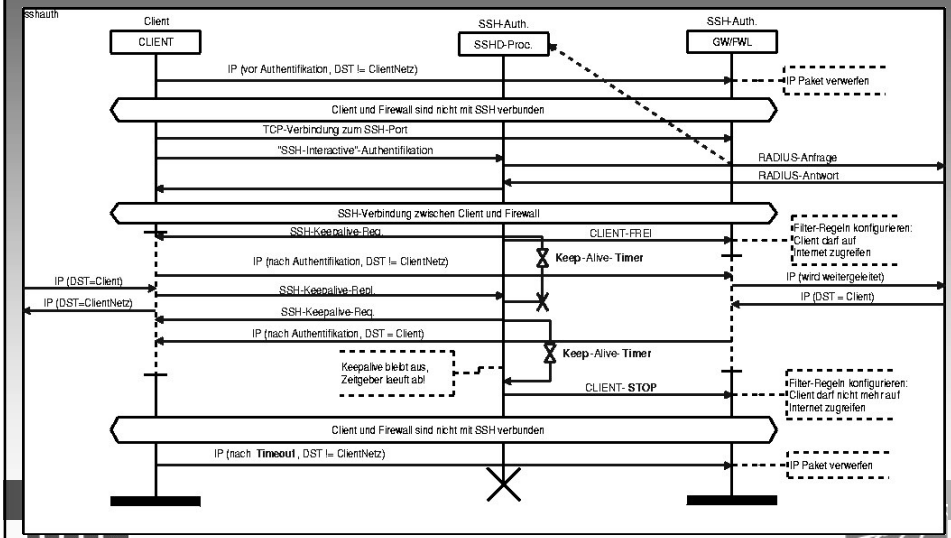
Grundsätzlich gilt:

– Benutzer verbindet sich mit dem Gateway
– Gateway befragt vorhandene Benutzerdatenbank
– Bei gültigem Namen/Passwort:
  – Gateway autorisiert IP-Adresse des Benutzers
  – Gateway überprüft Erreichbarkeit des Benutzers
  – Gateway hebt ggf. Autorisation wieder auf

Technische Umsetzung an der UHH

- Zu lösende Probleme
  - Plattformunabhängigkeit (WIN, MAC, UNIX)
  - Zugriff auf vorhandene Benutzerdatenbank
  - Sicherer Authentifikation
  - Autorisation (kontrollierte Dienstfreigabe)
  - Universitätsübergreifende Lösung
  - Vermeiden von administrativem Aufwand
  - Migrationstransparenz

Technische Umsetzung an der UHH



Technische Umsetzung an der UHH

Benutzer schließt das Gerät an

- Bereiche sind durch Plakate markiert
- Blau markierte Dosen ⇨ Öffentliche Anschlüsse
  + Einheitliche Markierung
- SSID: UHH-<ort>-<raum> ⇨ AP der UHH
  + Einheitliche Namenskonvention
- Netzkonfiguration mittels DHCP
  + Ortsunabhängigkeit

Technische Umsetzung an der UHH

Benutzer baut SSH-Verbindung auf

- Gateway mit zusätzlicher privater Adresse
  + Kennung und Passwort werden gesichert (trotz Funk oder anderer Broadcast-Medien)
  + Einheitliche Adresse (VLAN vs. Routing)
  + Identisches Zertifikat
  ⇨Ortsunabhängige Einstellungen beim Benutzer (trotz potentiell multipler Gateways)

Technische Umsetzung an der UHH

PAM verwaltet Benutzerauthentifikation

- Modular aufgebaut
  - + Modul für „nologin“-Semantik (alle sperren)
  - + Modul für Sperrliste (Individuen sperren)
  - + Module für LDAP- und andere Formate
  - + Modul für Radius-Anfrage und –Accounting
- Zur Laufzeit adaptierbar!

⇨ Flexibilität bei allen „AAA“-Aufgaben

Technische Umsetzung an der UHH

Shell für Autorisation und Interaktion

- Automatisiert die Autorisation
- Interagiert mit dem Benutzer (individuell oder alle)
  - – Bei geglückter Anmeldung (individuell)
  - – Bei manueller Abmeldung (individuell)
  - – Bei administrativer Vorgabe (individuell oder alle)
- Zeigt sich beim „ps“-Kommando mit
  - – Benutzerkennung und zugewiesener IP-Adresse

⇨ Erleichtert die Administration

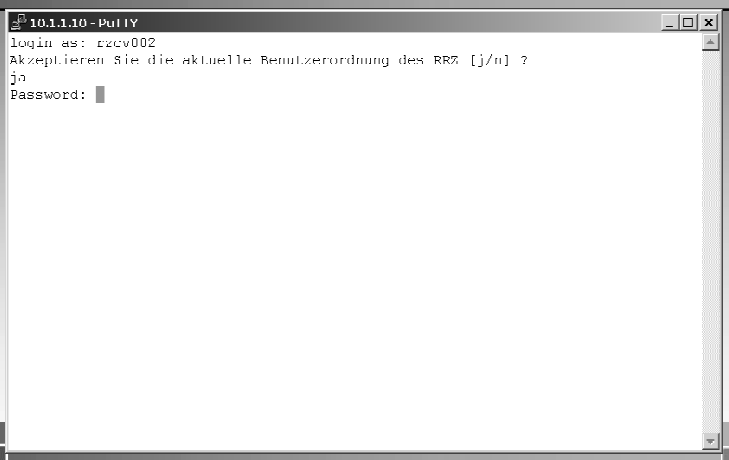
Technische Umsetzung an der UHH

Zugriffskontrolle mit Firewall-Techniken

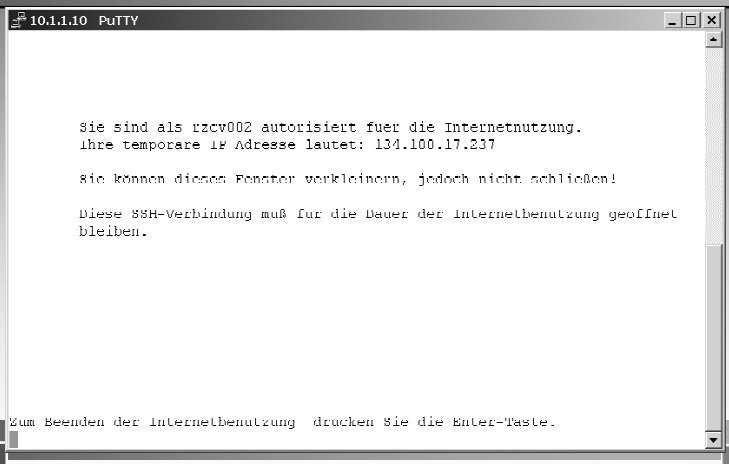
+ Aufwandsarme, gut verstandene Technik
- Allgemeine Filterregeln und Client-spezifische Filterregeln
  - Universell für alle konfiguriert
    - DHCP, DNS, Zugriff auf WWW-Proxy mit HTTP(s), SSH ins Internet, Zugriff auf Mail-Server der UHH (nur SSL-Ports: IMAPs, POPs, SMTPs)
  - Individuell durch Shell für jeweiligen Client konfiguriert
    - Aktuelle IP-Adresse des autorisierten Benutzers

⇨ Flexibilität beim Dienstangebot, gute Skalierbarkeit

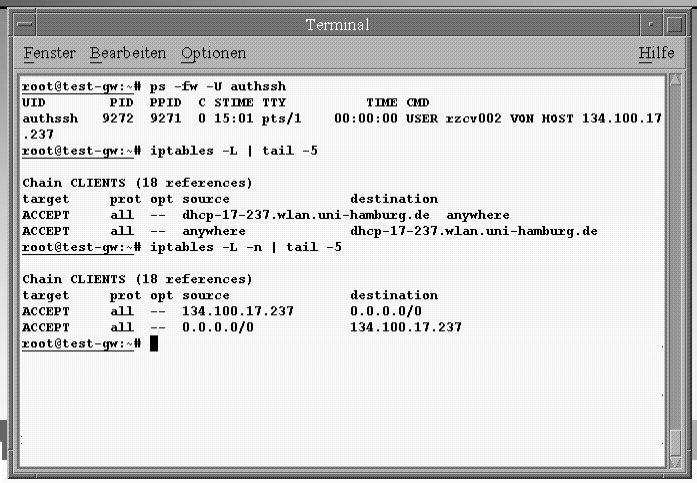
Beispiel/Anmeldung 1/4



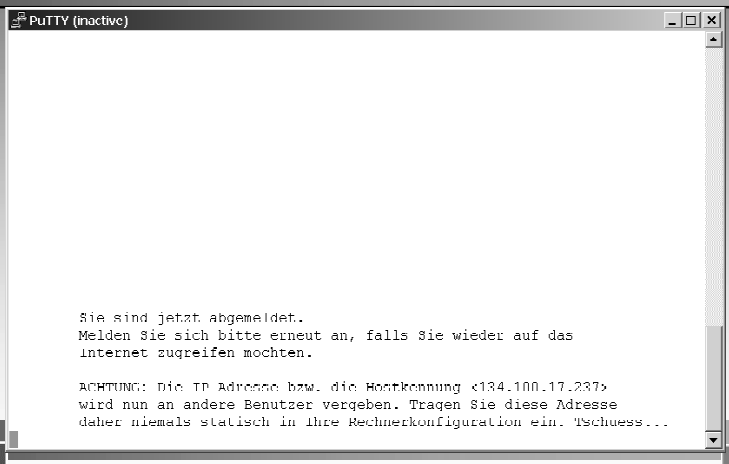
Beispiel/Anmeldung 2/4



Beispiel/Anmeldung 3/4



Beispiel/Anmeldung 4/4



Erweiterungsmöglichkeiten

- Weitere Dienste freischalten
  - Unkritische Dienste direkt freischalten
  - Kritische Dienste z.B. über „STunnel“
- Verhindern von Client<->Client-Kommunikation (UHH soll nicht zur Spieleplattform werden!)
- Einführen von Flusskontrolle (Intranet vs. Internet)?
- Einführen von Audit-Funktionen
  - Bald vom Gesetzgeber vorgegeben?
  - Zum Auffinden von Problemen/Hackern?

Zusammenfassung

- „Öffentliche Netzzugänge“ an der UHH sind:
  + Ein neuer Dienst für Studierende und MAs
  + Unabhängig von der Übertragungstechnik
  + Universitätsübergreifend realisierbar
  + Kostengünstig und pflegeleicht
- Nur sichere oder öffentliche Anwendungen erlaubt
  + Zugriffskontrolle mit Firewall-Techniken
  ± Freischalten von sicheren Anwendungen

Zusammenfassung

- Einsatz von SSH ermöglicht:
  + Unabhängigkeit von Client-Zertifikaten
  + Sichere Passwort-Abfrage über unsichere Netze
  + Nachrichtenversand an die Benutzer
- Einsatz von PAM ermöglicht:
  + Flexible Konfiguration von „AAA“-Aktionen
  + Zugriff auf vorhandene Benutzerdatenbanken