

Netzicherheit Architekturen und Protokolle



Dr. Marcus Schöller



Zur Person: Marcus Schöller

eMail: marcus.schoeller@nw.neclab.eu

Post-Doc: Lancaster
University

- Resilient Networking

Derzeit: Research Scientist
bei NEC Network Laboratories Heidelberg

- Autonomic Networking Architecture
- ResumeNet
- 3G Femto Networks

Studium:

- Uni Erlangen-Nürnberg
- Uni Karlsruhe
 - Fachschaft Info
 - GI
- Universitet Uppsalla

Promotion: Uni Karlsruhe

- Programmierbare Netze
- Internetökonomie
- IPsec-AG
- VL Netzicherheit



1

Was erwartet ihr von der Vorlesung „Netzicherheit“?

- Spaß
 - Fragen von euch
 - Diskussionen mit euch
- Interesse
 - Selbst ausprobieren
 - Kritische Auseinandersetzung mit dem Thema Sicherheit
- Wissen
 - Konzepte
 - Mechanismen
 - Protokolle
 - Standards
- Einbindung in die Vorlesung





Das Buch zur Vorlesung:

„Sichere Netzwerkkommunikation“,
Bless, Blaß, Conrad, Hof, Kutzner,
Mink, Schöller, Springer,
ISBN 3540218459

UB Karlsruhe:

Fachgruppe: inf 2.57
Signatur: 2005 A 8165

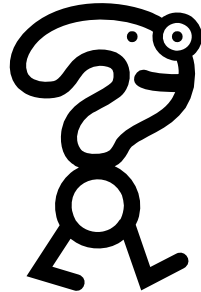
Bibliothek der Fakultät für Informatik:

Signatur: B.Sic(47794)
Inventar-Nr.: 2005/991

Netzicherheit Architekturen und Protokolle 0. Einführung



- Wer hat bereits VoIP verwendet?
- Wer hat Skype verwendet?



- Ist die Verbindung abhörbar?
 - Für den Betreiber fast immer.
 - ▶ Abhörschnittstellen gibt es wahrscheinlich noch zusätzlich
 - Für Dritte nicht so einfach... ?
- Skype.com: Skype verwendet AES!
 - Aber auch richtig? Schlecht nachvollziehbar.
- Skype.com: Es wird ein 256bit Session Key genutzt
 - Aber woher kommt der?
- Einige kleinere Schwachstellen in Skype gefunden:
 - Paper: „Blackhat Europe 2006“
 - ▶ von Philippe Biondi und Fabrice Desclaux (EADS)
- Und aktuell: Kann man dem Skype Client vertrauen?

- Wer hatte schon mal einen Wurm?



- Fehlerhafte Software
 - Buffer Overflow
 - Formatstring Schwachstellen
 - Parsen von Metazeichen
 - ...
- Kein Problem der Netzwerkprotokolle



- **Botnetze**
 - Ausbreitung über Würmer
 - große Menge von fernsteuerbaren infiltrierten Rechnern
 - fortgeschrittene Organisation (z.B. *Storm* Botnetz P2P-Organisation) und Nachladen von Modulen
- **Verwendung von Botnetzen**
 - **Distributed Denial of Service (DDoS) Angriffe**
 - ▶ 3-stündige Nichterreichbarkeit von Yahoo Anfang 2000 verursachte Schaden von ~500.000\$
 - **Spam** versenden
 - Beispiel *Srizbi* Botnetz
 - ▶ geschätzte **315.000 Bots**
 - ▶ **60 Milliarden Spam-E-mails pro Tag**
- **Anmieten von Botnetzen**
 - Botnetz mit 11.000 Rechnern: ab 125\$ pro Stunde
 - einzelner Rechner: 0.10\$ pro Stunde
 - Auktionswebseiten → *Software-as-a-Service* der anderen Art ...

Quelle zu Botnet: Studie von Peter Troxler für McAfee, entnommen einem Bericht bei Spiegel
Online: <http://www.spiegel.de/netzwelt/politik/0,1518,341665,00.html>

Quelle zu einzelner Rechner:

- Wer hat diesen Monat schon Phishing-Mails erhalten?





Die Technische Abteilung der Deutsche Postbank führt zur Zeit eine vorgesehene Software-Aktualisierung durch, um die Qualität des Online-Banking-Service zu verbessern.

Wir möchten Sie bitten, unten auf den Link zu klicken und Ihre Kundendaten zu bestätigen.

http://banking.postbank.de/app/cust_details_confirmation_page.do

Wir bitten Sie, eventuelle Unannehmlichkeiten zu entschuldigen, und danken Ihnen für Ihre Mithilfe.

© 2006 Deutsche Postbank AG

Erfolgreiches Phishing zeigt die Grenze sicherer Protokolle

- Wo die Technik nicht angreifbar ist, wird der Mensch angegriffen
- Phishing als eine Form des „Social Engineering“
- Ausgefeiltere Varianten existieren, nicht nur im Internet

- Beispiel:

Wer hat schon jemandem im RZ oder hier im Gebäude außerhalb der allgemeinen Öffnungszeiten die Tür aufgehalten?



- Wer hat ein WLAN zuhause?
- Wie ist das gesichert?
 - MAC-Filter?
 - DHCP-Filter?
 - Hidden SSID?
 - WEP?
 - WPA?
 - WPA2? 802.11i?
 - gar nicht?

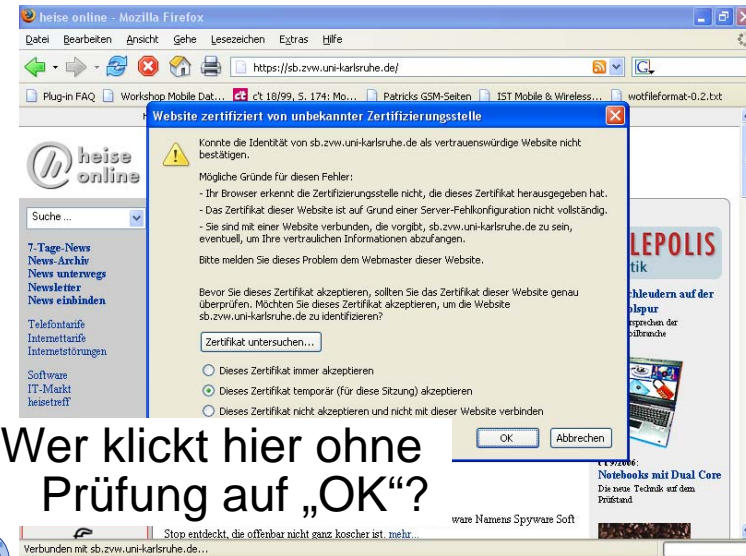


- Welcher Schutz hiervon wie sicher ist, wollen wir unter anderen in dieser Vorlesung klären.
 - Kapitel: Zugangskontrolle/Infrastrukturschutz
- Nebenbei: MAC-Filter, DHCP-Filter, Hidden SSID bieten (nahezu) keinen Schutz
 - Mithören reicht für die Angriffsvorbereitung aus
 - ▶ MAC fälschen / IP wählen

• Exkurs: „Hidden SSID“

- Wurde angelegt als Sicherheitsfunktion
- Klient muss zuerst den Namen eines WLANs anfragen, erst dann kann er sich mit diesem verbinden
- Ablauf:
 - ▶ Klient: „Hallo, ist hier mein Heimnetz mit dem Namen ABC?“
 - ▶ AP: „Ja! Da du mich kennst, darfst du das Netz ABC betreten.“
- Offensichtlicher Angriff:
 - ▶ Klient: „Hallo, ist hier mein Heimnetz mit dem Namen ABC?“
 - ▶ Angreifer: „Na klar, komm ruhig her“ ;-)
- Problem: Der Klient fragt immer, weil Hidden SSID möglich...

16



Wer klickt hier ohne
Prüfung auf „OK“?

17

- Vertrauen in Zertifikate ist für viele Sicherheitsprotokolle notwendige Voraussetzung
- Prüfung aber oft vernachlässigt
- Gängige Browser enthalten viele Root-Zertifikate
 - Wer hat diese schon einmal selbst überprüft?
- Auch „echte“ Zertifizierungsstellen machen Fehler
- Mehr dazu in der Vorlesung



Farcus

by David Weissglass
Gordon Coulthart



"It's our new computer security system!"

A CRYPTO NERD'S IMAGINATION:

HIS LAPTOP'S ENCRYPTED.
LET'S BUILD A MILLION-DOLLAR
CLUSTER TO CRACK IT.

NO GOOD! IT'S
4096-BIT RSA!

BLAST! OUR
EVIL PLAN
IS FOILED!

