Lehrveranstaltung:IAM 2006:Tunnel und verdeckte Kanäle in Netzen

Wechseln zu:Navigation, Suche

Diese Lehrveranstaltung wird nicht mehr angeboten.

Studiengang	Interaktive Medien (IAM 2006)
Studienabschnitt	Vertiefungsphase
Modul	Wahlpflichtfach Informatik
Name	Tunnel und verdeckte Kanäle in Netzen
Name (englisch)	Tunneling and Network Steganography
Kürzel	TUNN2.WP
Voraussetzungen	Es müssen mindestens 80 Credits in den Studienabschnitten Grundlagen- und Orientierungsphase und Aufbauphase erworben worden sein.
Wird gehalten:	veraltet
Semester	IAM 7
Lehrformen	Vorlesung
Credits	2,5
SWS	2 (Lehre: 2, Teaching Points: 2)
Workload	Präsenzstudium: 30 h (durchschnittlich 2 h pro Woche) Eigenstudium: 45 h (durchschnittlich 3 h pro Woche)
Notengebung	Kommanote (1,0; 1,3; 1,7; 2,0, 2,3; 2,7; 3,0; 3,3; 3,7; 4,0; 5,0)
Gewichtung (Modulnote):	50 %
Verantwortliche(r)	Nik Klever
Lehrende(r)	Steffen Wendzel
Homepage	https://www.hs-augsburg.de/fakultaet/informatik/studium/wahlpflichtveranstaltung/tunnel und verdeckte kanaele/index.html

1 Inhalte

Die Vorlesung verbindet die Themen Tunneling und Netzwerksteganografie. In beiden Fällen werden, vereinfacht dargestellt, Netzwerkdaten innerhalb anderer Netzwerkdaten übertragen. Im Falle des Tunnelings erfolgt dies meist legitim, im Falle der Netzwerksteganografie hingegen nicht:

Das Senden von Netzwerkdaten innerhalb anderer Netzwerkdaten ist ein Grundprinzip des heutigen

Internets. Ob im bisherigen Internet Protocol (IPv4) oder in der neuen Version (IPv6), in virtuellen privaten Netzwerken (VPNs), Transport- und Anwendungsprotokollen: ohne Tunneling ist ein Betrieb von modernen Netzwerken nur eingeschränkt möglich. Know-how im Bereich des Netzwerktunnelings ist ein Zugang zu zentralen Bereichen der Netzwerkadministration und etwa bei der Umstellung auf IPv6 und beim Verbinden von Gebäude-Netzen über das Internet von elementarer Bedeutung.

Verdeckte Kanäle bzw. Netzwerksteganografie spielen nicht nur für die Wissenschaft, sondern zunehmend für die Öffentlichkeit, eine Rolle: Möchten Journalisten oder die politische Opposition regimekritische Informationen in überwachten Netzwerken übertragen oder sollen Botnetze koordiniert werden, so genügt eine reine Datenverschlüsselung nicht. Wird eine Kommunikation nur verschlüsselt, ist sie für eine überwachende Instanz sichtbar. Mit Netzwerksteganografie hingegen lässt sich die Existenz einer Datenübertragung verbergen. Gleichzeitig soll in der Vorlesung auch die Detektion und Vermeidung steganografischer Kommunikation erläutert werden.

Insbesondere werden die folgenden Themen in der Vorlesung behandelt:

(Wiederholung der) Grundlagen von TCP/IP
Netzwerktunneling (Grundlagen; Anwendungsgebiete; Tunneling für die Umstellung von IPv4 auf IPv6; Tunneling für Gebäude-Netze mit BACnet/IP und KNX/IP; weitere Protokolle: IPIP; IP-in-IP; General Routing Encapsulation; L2TP; Teredo; IPSec; PPTP; Socks)
Verdeckte Kanäle und Netzwerksteganografie (Anwendungsgebiete; Schadpotential; Terminologie; Historische Entwicklung; Zeitkanäle, Speicherkanäle, Verfahren zur Erstellung verdeckter Kanäle; Detektion, Limitierung und Prävention verdeckter Kanäle; Fortgeschrittene Themen für verdeckte Kanäle).

2 Literatur

S. Wendzel: Tunnel und verdeckte Kanäle im Netz, Springer-Vieweg, 2012.

3 Prüfungen

Nummer	Prüfer	Zweitprüfer	Prüfung	Prüfungsart	Prüfungsdetails	Hilfsmittel
1930386	Steffen Wendzel		nicht mehr angeboten	Leistungsnachweis		

Kategorie:
Lehrveranstaltung