Universität Hamburg
DER FORSCHUNG | DER LEHRE | DER BILDUNG

Aufgabenstellung für die Bachelorarbeit: Funktionsweise, Angriffe und Abwehrmechanismen von SSL/TLS

Zielsetzung:

Die Protokollfamilie SSL/TLS umfasst Techniken zum Schutz von Kommunikationsdaten in IP-basierten Netzen. Ihre weite Verbreitung und Wichtigkeit für die IT-Sicherheit ist historisch gewachsen, und ihr Einsatz erstreckt sich über mittlerweile weit mehr Protokolle der Anwendungsschicht, als nur das ursprünglich anvisierte HTTP. Diese weite Verbreitung hat zwei wesentliche Konsequenzen. Zum einen wurden sowohl die Spezifikation der Protokollfamilie als auch praktische Implementierungen von SSL/TLS Gegenstand zahlreicher Angriffe. Zum zweiten sind ein grundlegendes Verständnis der Funktionsweise von SSL/TLS und der erwähnten Angriffe obligatorisch bei der Entwicklung und Implementierung von verteilter Software, Internetdiensten und Protokollimplementierungen auf der Anwendungsschicht, die mittels SSL/TLS abgesichert werden sollen.

In dieser Bachelorarbeit soll unter Einbeziehung aktueller Entwicklungen und Forschungsergebnisse die Funktionsweise von SSL/TLS, bedeutende Angriffe auf diese Protokollfamilie sowie daraus erarbeitete Anpassungen der Protokollspezifikation und Abwehrmechanismen erläutert und speziell für den Einsatz in der Hochschullehre aufbereitet werden. Darüber hinaus soll ein modular aufgebautes Tool zur Veranschaulichung der SSL/TLS-Funktionsweise sowie deren Angriffe und Abwehrmechanismen entwickelt und prototypisch umgesetzt werden. Der Fokus des Tools liegt in der Demonstration von SSL/TLS und dessen Schwächen mit beliebiger Verständnisvertiefung, sollte allerdings auch um weitere IT-Sicherheitsprotokolle erweiterbar sein.

Bearbeiter:	Tom Petersen
Matrikelnummer:	6359640
Studiengang:	Informatik
Betreuer:	Dipl.-Inf. Ephraim Zimmer
Erstgutachter:	Prof. Dr. Hannes Federrath
Zweitgutachter:	
Beginn am:	01.07.2015
Bearbeitungsdauer:	5 Monate

Der Fachbereich Informatik behält ein unentgeltliches nichtausschließliches Nutzungsrecht an Schutzrechten und Urheberrechten an der Bachelorarbeit für seine satzungsgemäßen Zwecke. Die am Arbeitsbereich geltenden Hinweise für Abschlussarbeiten sind zu beachten.

Prof. Dr. Hannes Federrath
Verantwortlicher Hochschullehrer

Dipl.-Inf. Ephraim Zimmer
Betreuer

Tom Petersen
Bearbeiter/in