VSDB

Verschlüsselung

DES
Diffie-Hellman

Daniel Dimtrijevic Thomas Traxler

28. Februar 2014

5AHITT

Inhaltsverzeichnis

1 Aufgabenstellung

Kommunikation [12Pkt] Programmieren Sie eine Kommunikationsschnittstelle zwischen zwei Programmen (Sockets; Übertragung von Strings). Implementieren Sie dabei eine unsichere (plainText) und eine sichere (secure-connection) Übertragung.

Bei der secure-connection sollen Sie eine hybride Übertragung nachbilden. D.h. generieren Sie auf einer Seite einen privaten sowie einen öffentlichen Schlüssel, die zur Sessionkey Generierung verwendet werden. Übertragen Sie den öffentlichen Schlüssel auf die andere Seite, wo ein gemeinsamer Schlüssel für eine synchrone Verschlüsselung erzeugt wird. Der gemeinsame Schlüssel wird mit dem öffentlichen Schlüssel verschlüsselt und übertragen. Die andere Seite kann mit Hilfe des privaten Schlüssels die Nachricht entschlüsseln und erhält den gemeinsamen Schlüssel.

Sniffer [4Pkt] Schreiben Sie ein Sniffer-Programm (Bsp. mithilfe der jpcap-Library http://jpcap.sourceforge.net oder jNetPcap-Library http://jnetpcap.com/), welches die plainText-Übertragung abfangen und in einer Datei speichern kann. Versuchen Sie mit diesem Sniffer ebenfalls die secure-connection anzuzeigen.

Info Gruppengröße: 2 Mitglieder Punkte: 16

Erzeugen von Schlüsseln: 4 Punkte Verschlüsselte Übertragung: 4 Punkte Entschlüsseln der Nachricht: 4 Punkte Sniffer: 4 Punkte

2 Designüberlegungen

3 Arbeitsaufteilung

Name	Arbeitssegment	Time Estimated	Time Spent
Thomas Traxler	Chat	1h	0.5h
Daniel Dimitrijevic	En-/Decrypt	2h	2h
Thomas Traxler	En-/Decrypt	1h	1h
Walter Klaus	Diffie-Hellman	1h	2h
Daniel Dimitrijevic	Sniffing	1h	2h
Gesamt		6h	7.5h

4 Arbeitsdurchführung

5 Testbericht

6 Quellen