GSS-Übungsblatt 1

Chamier, Eickhoff, Gäde, Hölzen, Jarsembinski · SoSe 2016

Aufgabe 2: Schutzziele

Abgrenzung I:
a)
Anonymität heißt, dass der Sender für den Empfänger, oder etwaige Dritte, unkenntlich ist. Im Gegensatz dazu wirkt Pseudonymität wie eine Verkleidung, das heißt, die Verkehrsdaten des Senders werden durch einen vertraulichen Dritten verschleiert. Für den Empfänger sind also nur die Daten des Dritten sichtbar und nicht die des Senders direkt. Wird der gesamte Vorgang verschleiert und nicht die Daten der Beteiligten spricht man von Unbeobachtbarkeit.

b)
Der Unterschied zwischen Vertraulichkeit und Verdecktheit besteht darin, dass bei letzterem die Existenz des Datenaustauschs verschleiert wird, wohingegen bei Vertraulichkeit die Daten verschlüsselt werden, um sie vor Angreifern zu schützen. Dies ist zu vergleichen mit dem Unterschied von Steganographie zu Kryptographie.

Abgrenzung II:
a)
Ist eine Nachricht integer, bedeutet das, dass eventuelle Beschädigungen oder andere Modifikationen vom Empfänger erkannt werden können, während Zurechenbarkeit meint, dass der Absender tatsächlich derjenige ist, für den er sich ausgibt. Dies wird zum Beispiel durch digitale Signaturen gewährleistet.

b)
Ein Dienst ist verfügbar, wenn er zu einem gewünschten Zeitpunkt genutzt werden kann, wohingegen er auch erreichbar sein kann ohne die gewünschte Fuktion bereitzustellen.

Techniken:
Anonymität: Fraglich im Internet mit IPs, Lokal vllt. ohne Benutzerkonto Pseudonymität: Proxy Vertraulichkeit: Verschlüsselung (z.B. RSA, AES, WhatsApp-Ende-zu-Ende-Verschlüsselung) Verdecktheit: Steganographie (Nachrichten in JPEGs o.Ä.) Integrität: Hashsummen, Paritätsbits Zurechenbarkeit: Digitale Signatur Verfügbarkeit: Cloud Erreichbarkeit: Lokal,Internet,Infrarot

Aufgabe 3: Angreifermodell

2.
Rolle: Außenstehender(nur mit karte oder nur mit pin), andere Benutzer des Automaten Verbreitung: Ablesen an Tastatur, Aufsätze am Automaten, Diebstahl Verhalten: Ablesen(beobachtend), Aufsätze(aktiv), Diebstahl(Aktiv) Rechenkapazität: Ablesen(0), Aufsätze(0),Diebstahl(nur karte - enorm)

Aufgabe 5: Passwortsicherheit

Brute-Force-Angriff: $62^8 \div 1000000 \div 60 \div 60 \div 24 = 2527,1$ Tage

Bei beliebiger Passwortlänge mit Zahlen: $(10^1 + ... + 10^{16}) \div 1000000 \div 3600 \div 24 = 128601$ Tage