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.

c)

Anonymität: Anonymität ist schwer bis gar nicht im Internet zu erreichen. Da jede Internetverbindung über IP-Adressen und Protokolle aufgebaut wird, ist es so gut wie unmöglich keine eigenen Daten im Netz zu hinterlassen. Eine Möglichkeit quasi Anonym zu sein, wäre einen eigenen Server zu benutzen, um sich über diesen im Netz zu bewegen. So würden keine Verbindungsdaten an einen Drittanbieter eines Proxy-Servers weitergegeben. Die Verbindungsdaten des Servers sind jedoch trotzdem im Internet verbreitet, man ist also nur quasi anonym.

Pseudonymität: Pseudonymität kann zum Beispiel über Proxy-Server oder VPN-Verbindungen erlangt werden. Der Anbieter des Proxy-Servers kennt zwar die Verbindungsdaten des Senders, gibt diese jedoch nicht weiter. Trotzdem können an die Pseudonymsdaten Nachrichten gesandt werden, die über dem Server wieder beim Nutzer landen.

Vertraulichkeit: Vertraulichkeit kann z.B. über das Verschlüsseln des gesendeten Inhaltes erreicht werden. Verfahren hierfür wären RSA, AES, etc..

Verdecktheit: Um seine gesendeten Inhalte verdeckt zu halten, kann man z.B. Stganographie in verschiedenen Formen anwenden. Daten lassen sich in Bildern (JPEG, Gif, ...) oder auch in Sound-Dateien (MP3, WMA, ...) einbetten und sind so quasi unsichtbar für Angreifer. Dies gilt natürlich nur wenn der Angreifer nicht vermutet, dass überhaupt Daten versteckt sind.

Integrität: Die Integrität von gesendeten Daten kann z.B. durch Mitsenden von Paritätsbits oder der Hashsumme der Orginaldatei erreicht werden. Wurden die Daten manipuliert, so werden die Paritätsbits oder die Hashsumme dieser Daten nicht mit dem Original übereinstimmen. Dieser Prüfung ist nur bedingt zuverlässig, da natürlich die Daten so manipuliert werden können, das die Hashsumme und die Paritätsbits den Originalen entsprechen obwohl es sich nicht um die selben Daten handelt. Besonders bei Hashcodierung sind solche Kollisionsattacken verbreitet.

Zurechenbarkeit: Die Zurechenbarkeit von Daten kann mittels digitaler Signatur überprüft werden. Hierzu werden aus einem privatem Schlüssel und der Nachricht eine Signatur erstellt. Diese Signatur kann, dann mittels öffentlichen Schlüssel und Verifikationsalgorithmus auf ihre Authentizität überprüft werden.

Verfügbarkeit: Die Verfügbarkeit von Internetdiensten kann z.B. durch Backup-Server gewährleistet werden. Im Fall einer DDos Attacke, könnte dann der Backup-Server genutzt werden, während der Hauptserver wieder hochgefahren wird. Physischer Schutz gegen z.B. einen Stromausfall wäre ein Backup-Generator, der den Betrieb des Servers gewährleistet.

Erreichbarkeit: Um die Erreichbarkeit eines Webdienstes oder Servers gegen Angriffe auf die Verbindung der Rechner abzusichern, kann man den Dienst auf mehreren Servern laufen lassen, um die Chance zu erhöhen, dass noch mindestens einer erreichbar ist. Um eine ständige Erreichbarkeit zu gewährleisten, müsste man ausschließlich mit lokalen, physisch verbundenen Systemen arbeiten.

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)

In unserem Angreifermodell für das Abheben von Geld mittels einer EC-Karte kann der Angreifer entweder die Rolle eines Außenstehenden sein, der entweder eine EC-Karte oder eine PIN unrechtmäßig erlangt hat, oder die Rolle eines anderen Nutzers, der versucht Geld von einem anderen

Konto abzuheben. Der außenstehende Angreifer hat die Möglichkeit entweder die PIN eines Benutzers passiv zu erspähen oder aktiv mittels Aufsatz oder ähnlichem Abzutasten. Ausserdem kann der Angreifer sich der EC-Karte eines Kunden bemächtigen. Solange der Angreifer nur die PIN oder die EC-Karte besitzt, ist das System vor einem Angriff sicher. Wenn der Angreife jedoch beides besitzt, versagt das Sicherheitssystem. Es wäre dem Angreifer auch möglich die fehlende PIN mittels Bruteforce versuch zu ermitteln, was viel Rechenkapazität benötigt und einem nur drei Versuche bietet, oder eine Kopie einer EC-Karte anzufertig, was wiederum enorme Rechenleistung benötigen würde. Gegen einen Angriff eines Benutzer, der versucht Geld von einem fremden Konto abzuheben, ist das System geschützt, da EC-Karte und PIN nur Zugriff auf ein bestimmtes Konto erlauben. Natürlich könnten auch Entwickler oder Hersteller potenzielle Angreifer sein. In diesem Fall jedoch, könnte bereits in der Entwicklung eine Hintertür ins System eingebaut worden sein, womit das System schon in der Konstruktion nicht sicher wäre. Dies ist bei jedem System möglich und sollte im seltensten Fall in Betracht gezogen werden.

Aufgabe 5: Passwortsicherheit

3. Brute-Force-Angriff

Alphanumerisch mit genau 8 Zeichen: $62^8 \div 1000000 \div 60 \div 60 \div 24 = 2527,1$ Tage

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

Wie in obigen Berechnungen zu sehen ist, hat die Länge des Passworts eine stärkere Auswirkung auf die Rechenzeit als die Komplexität. Dies gilt jedoch nur solange es sich um einen Brute-Force Angriff handelt. Bei einem Wörterbuch-Angriff kann die Komplexität einen größeren Einfluss auf die Berechenbarkeit als die Länge machen, wenn das längere Passwort nur ein einfaches Wort ist.