Aufgabe 2: Schutzziele

Alexander Hildebrandt, Jan-Thomas Riemenschneider

Abgrenzung I

a) Anonymität bedeutet, dass man Ressourcen und Dienste benutzen kann, ohne die eigene Identität zu offenbaren. Pseudonymität schreibt dagegen vor, dass Nutzer statt anonym zu bleiben ein Pseudonym benutzen müssen. Beide Varianten gewähren dem Nutzer Schutz vor dem Preisgeben des echten Namens, aber Pseudonymität gibt dem Anbieter von Ressourcen und Diensten mehr Kontrolle und Sicherheit, da alle Zugriffe und Änderungen zu einem Pseudonym zugeordnet werden können. Unbeobachbarkeit bedeutet, dass Nutzer beim Benutzen von Ressourcen und Diensten nicht von Dritten beobachtet werden können. D.h. Unbeobachtbarkeit ist jeweils zusammen mit Anonymität oder Pseudonymität realisierbar, aber Anonymität und Pseudonymität sind exklusiv.

b) Vertraulichkeit besagt, dass Daten beim Übertragen geheim gehalten werden, während Verdecktheit die Übertragung von Daten an sich geheim hält. D.h. beide Schutzziele wollen das Übertragen von Daten davor schützen, von Dritten gesehen zu werden. Vertraulichkeit ist für den normalen Nutzer durchaus relevant, da man sich von Diensten wie Emails und Messengers wünscht, dass Dritte nicht mitlesen. Verdecktheit ist z.B. für illegale Geschäfte relevanter, da es dabei wichtig ist, gar nicht erst miteinander in Verbindung gebracht zu werden.

Abgrenzung II

a) Integrität bedeutet, dass jegliche Modifikationen eines Inhaltes erkannt werden können, sobald sie beim Empfänger ankommen, während Zurechenbarkeit bedeutet, dass das Senden und Empfangen von Inhalten bewiesen werden kann. Ersteres ist relevant, um die Intention des Senders sicherzustellen (egal, ob es um den Inhalt der Nachricht oder um den Namen des Senders selbst geht), während letzteres bei vertraglichen Abkommen wichtig ist. Z.B. könnte eine Firma verpflichtet sein, eine Mahnung zu verschicken, bevor sie eine Geldstrafe an einen Nutzer schicken. Zurecenbarkeit würde dann dafür sorgen, dass die Firma einen Beweis hat, dass die Mahnung angekommen ist, bevor sie die Geldstrafe veranlassen.

b) Verfügbarkeit besagt, dass Nutzer wann sie wollen auf Dienste und Ressourcen zugreifen können, während Erreichbarkeit bedeutet, dass man Kontakt mit einem Nutzer oder einer Maschine aufnehemen kann, wann man will. Erreichbarkeit setzt Verfügbarkeit voraus, aber das Gleiche gilt nicht umgekehrt. Verfügbarkeit beschäftigt sich eher mit dem Vorhandensein eines Elementes, während Erreichbarkeit impliziert, dass das Element tatsächlich greifbar ist.

Techniken

Anonymität ist automatisch gegeben, wenn ein Online-Forum, Chatroom oder ähnliches keine Form von Anmeldung benötigt, um einen Beitrag zu schreiben.

Pseudonymität ist umsetzbar, indem man Beiträge auf einer Online-Platform nur erlaubt, wenn man einen festen Nickname wählt, der mit allen Beiträgen assoziiert wird.

Unbeobachtbarkeit ist umsetzbar, indem man den Zugriff auf eine Datei sperrt, sobald ein Nutzer an dieser Datei arbeitet und erst nach der Bearbeitung wieder freigeschaltet wird.

Vertraulichkeit ist durch jegliche Form von Verschlüsselung umsetzbar.

Verdecktheit ist umsetzbar, indem man Daten auf einem physikalischem Medium an einen Empfänger überreicht.

Integrität ist umsetzbar, indem zusammen mit seiner Nachricht einen Code verschickt, der vom Inhalt der Nachricht abhängig ist. Der Empfänger muss das System kennen, durch das der Code erzeugt wurde. Dadurch kann er den Code mit dem Inhalt der Nachricht abgleichen und Unstimmigkeiten erkennen.

Zurechenbarkeit ist umsetzbar, indem man eine Lesebestätigung mit seiner Email sendet. Die Email kann wahlweise nur lesbar gemacht werden, falls die Bestätigung vom Empfänger angenommen wird.

Verfügbarkeit ist umsetzbar, indem man nach jeder Modifikation an einer Datei gezwungen wird, Tests auszuführen. Der Anbieter der Datei übernimmt die Modifikationen erst, sobald die Datei alle Tests besteht.

Erreichbarkeit ist umsetzbar, indem man regelmäßig die Verbindung eines Servers überprüft und Backups erzeugt. Anders als die restlichen Schutzziele ist die Erreichbarkeit eher reaktiv zu gewährleisten, indem man z.B. eine unterbrochene Internetverbindung so schnell wie möglich wiederherstellt. Es ist sehr viel schwerer einen direkten Schutz vor der Unterbrechung von Erreichbarkeit zu erstellen, wie es z.B. bei der Verfügbarkeit möglich ist.

Aufgabe 3.2

Angreifermodell am Beispiel des Geldautomaten

An einem Geldautomaten wird von einem Kunden Geld in folgenden Schritten abgehoben: Einführung der Karte, Eingabe des Sicherheitspins, Auswahl des abzuhebenden Betrages, Entnahme der Karte, Auszahlung des Bargeldes. Die trivialste Rolle, die ein Angreifer einnehmen kann, wäre möglicherweise die in Form eines “Scheinbenutzers”, der bei der Pineingabe des Opfers mit gezielten Blicken die Passwortkombination herausfindet und somit bereits eines der Schutzziele, das Schutzziel der Vertraulichkeit, verletzte. Eine andere Möglichkeit wäre, dass sich der Angreifer, aus welchen Gründen auch immer (Mitarbeiterzugriff, als Außenstehender) ggf. unerlaubten Zugriff zum Bank- bzw. Automatensystem verschafft und gezielt Systemzustände zu seinen Gunsten verändert oder auch nötige Informationen gewinnt. Das führe zu Verletzung zweier Schutzziele, sowohl dem Schutzziel der Vertraulichkeit als auch dem Schutzziel der Integrität. Das Verhalten des Angreifers kann man im ersten Fall als beobachtend-passiv beschreiben, im zweiten Fall hingegen als aktiv-veränderend. Die Rechenkapazität ist im Falle eines Nicht-Mitarbeiterzugriffs auf das System als komplexitätstheoretisch anzusehen, im Falle eines Mitarbeiterzugriffs sicherlich als informationstheoretisch. Der Nicht-Mitarbeiter könnte ggf. Gezwungen sein per Brute-Force-Methode sich Zugriff auf Daten zu verschaffen, bei einem Mitarbeiter ist das entsprechend weniger wahrscheinlich.

Aufgabe 5.3

Brute-Force-Angriff

- Acht Passwort Stellen
- Eine Million Passwörter pro Sekunde prüfen
- Passwort besteht aus alphanumerischen Zeichen

Vs

- Keine Kennwortlängeneinschränkung
- Passwort besteht aus 16 Zahlen

Lösung 1 (Alphanumerisch, achtstelliges Passwort):

Möglichkeiten pro Stelle = Alphabet (groß und klein) + Zahlen

= 26 große Buchstaben + 26 kleine Buchstaben + 10 Zahlen = 62 Möglichkeiten pro Stelle

Anwendung der Formel "(Anzahl der Möglichkeiten pro Stelle) ^ Passwortlänge"

Daraus ergeben sich 62^8 (218.340.105.584.896) Passwortmöglichkeiten.

Geteilt durch eine Million geprüfte Passwörter pro Sekunde kommt man auf die nötigen Sekunden, die zur Passwortfindung führen.

218.340.105.584.896 / 1.000.000 = 218340105,6 Sekunden

218340105,6 / 60 = 3639001,76 Minuten

3639001,76 / 60 = ca. 60650 Stunden

60650 / 24 = 2527 Tage

2527 / 365 = ca. 6,9 Jahre

Es dauert also maximal **6,9 Jahre** bis das Passwort gefunden wird.

Lösung 2 (Numerisch, sechzehnstelliges Passwort):

Möglichkeiten pro Stelle: Zahlen = 10

Anwendung der Formel "(Anzahl der Möglichkeiten pro Stelle) ^ Passwortlänge"

10^16 = 10.000.000.000.000.000

Geteilt durch eine Million geprüfte Passwörter pro Sekunde kommt man auf die nötigen Sekunden, die zur Passwortfindung führen.

10.000.000.000.000.000 / 1.000.000 = 10.000.000.000 Sekunden

10.000.000.000 / 60 = ca. 166.666.666 Minuten

166.666.666 / 60 = ca. 2.777.777 Stunden

2.777.777 / 24 = ca. 115.740 Tage

115.740 / 365 = 317 Jahre

Es dauert also **317 Jahre** bis das Passwort gefunden wird.