Aufgabe auf Seite 429.

2-2 (Un)Abhängigkeit von Vertraulichkeit, Integrität, Verfügbarkeit am Beispiel Identifikation

Es sind keine „sicheren" IT-Systeme zu erwarten, für die auch nur bzgl. eines der drei Schutzziele keinerlei Anforderungen bestehen:

- Bestehen keinerlei Anforderungen bzgl. *Verfügbarkeit*, dann braucht überhaupt kein IT-System realisiert zu werden. Damit sind dann alle seine (vorhandenen) Informationen integer und vertraulich.
- Bestehen keinerlei Anforderungen bzgl. *Integrität*, dann kann das IT-System Menschen nicht unterscheiden, da seine zu ihrer Unterscheidung nötige Information unbefugt modifiziert werden kann. Gleiches gilt für die Information zur Unterscheidung anderer IT-Systeme.
- Bestehen keinerlei Anforderungen bzgl. *Vertraulichkeit*, dann kann sich das IT-System anderen Instanzen gegenüber nicht als es selbst ausweisen, denn Angreifer könnten alle dafür nötige Information vom IT-System erhalten. (Die umgekehrte Argumentation geht nicht so glatt durch: "Da das IT-System keinerlei Information vertraulich halten kann, kann es andere Instanzen nicht erkennen, denn Angreifer könnten alle Information erhalten, anhand derer das IT-System andere Instanzen unterscheiden will."Die Argumentation scheint zwar schlüssig zu sein, jedoch könnte das IT-System die Information, die es von der anderen Instanz erwartet, vor dem Abspeichern einer kollisionsresistenten Hashfunktion (vgl. §3.6.4 und §3.8.3) unterwerfen und nur das Ergebnis dieser Hashfunktion abspeichern und später mit dem entsprechend berechneten Wert der Eingabe vergleichen.)

Aufgabe auf Seite 430.

2-3 Sende Zufallszahl, erwarte Verschlüsselung - geht's auch umgekehrt?

Der Unterschied ist subtil:

In der normalen Variante muß über die Zufallszahlenerzeugung nur angenommen werden, daß sich Zufallszahlen nicht (mit relevanter Wahrscheinlichkeit) wiederholen.

In der umgekehrten Variante muß *zusätzlich* angenommen werden, daß die Zufallszahlenerzeugung für Angreifer unvorhersagbar ist. Das sollte zwar bei Zufallszahlenerzeugung, wie der Name suggeriert, der Fall sein, aber Vorsicht ist die Mutter der Porzelankiste.

Der Unterschied wird an einem extremen Beispiel am deutlichsten: Die normale Variante ist sicher, wenn als Zufallsgenerator einfach ein Zähler genommen wird, der nach jeder „Zufallszahl" inkrementiert wird. Mit dieser Implementierung der Zufallszahlenerzeugung wäre die umgekehrte Variante des Protokolls vollkommen unsicher.

Für Interessierte: In [NeKe_99] finden Sie neben einer ausführlicheren Erklärung dieses Beispiels auch eine lesenswerte Einführung in einen Formalismus (BAN-Logik), mit dem solche Protokolle untersucht werden können.

Aufgabe auf Seite 430.