Prinzipien der Kyptographie

Das Kerckhoffsche Prinzip

Wenn man ein geheimes Dokument irgendwo zuhause versteckt, dann hat das ziemlich wenig mit Sicherheit zu tun. Mögliche Angreifer (wir nehmen an, der Angreifer ist die National Security Agency [NSA] höchstpersönlich) würden selbstverständlich das Haus durchsuchen. Selbst wenn das Dokument an einem geheimen Ort versteckt ist, wird es nach genügend langem Suchen gefunden werden. Man könnte dich ausspionieren, Freunde ausfragen usw. Außerdem muss man möglicherweise auch an den geheimen Ort zurückkommen, um das Dokument wiederzuholen. Verstecken ist also nicht besonders effektiv.

Wenn ich das Dokument jedoch in den Safe lege, den Angreifern noch sämtliche Entwicklungspläne dieses Safes und noch hundert anderer mitsamt ihren Kombinationen gebe, so dass alle neugierigen Menschen den Mechanismus ausgiebig studieren können, aber immer noch nicht in der Lage sind, den Safe zu öffnen, dann ist das Sicherheit.

Das Bild des Safes ist eine schönes Beispiel für Kryptographie, das übrigens von Bruce Schneier stammt. Wenn wir das Ganze auf ein Verschlüsselungs-System übertragen, ist der Safe das Verschlüsselungs-Verfahren. Dieses Verfahren sollte auch noch dann sicher sein, wenn es von den weltbesten Kryptographen untersucht wurde.

Die Sicherheit eines kryptographischen Systems darf ausschließlich von der Geheimhaltung des Schlüssels abhängen, nicht von der Geheimhaltung des Verfahrens (Kerckhoffs’sches Prinzip)

Die eigene Verschlüsselungsmethode

In den meisten Fällen stellt es ein nicht unlösbares Problem dar, an das verwendete Verfahren zu gelangen. Und kennt man es erstmal, kann man selber Tests daran durchführen und es möglicherweise knacken. Vielleicht kann die verschlüsselte Nachricht auch ohne Kenntnis des benutzten Verfahrens geknackt werden, falls ein außerordentlich schlechtes benutzt wurde. Beim Beispiel des Safes könnte der Schlüssel eine bestimmte Zahlenkombination sein. Natürlich muss auch der Schlüssel ausreichende Sicherheit bieten, wenn ich z. B. eine nur zweistellige Kombination wähle, ist ein Safe ziemlich witzlos.

Aktuelle kryptographische Verfahren werden von ausgewiesenen Experten implementiert und für gewöhnlich in öffentlichen Wettbewerben und Prozessen auf ihre Tauglichkeit überprüft.

Wenn man selbst Software programmiert, die kryptographische Funktionen implementiert, sollte man dazu stets auf entsprechende, erprobte Bibliotheken zurückgreifen. Kurz: **Man erfindet keine eigene Verschlüsselung**.