Einführung in Kryptographie und Datensicherheit Übung 2

Tilman Bender Matrikelnummer: 108011247244

29. Oktober 2011

Aufgabe 2

a)

Die Chancen stehen günstiger für den Angreifer, da er lediglich einen ausnutzbaren Fehler finden muss. Der Verteidiger dagegen muss sein System gegen alle bekannten Angriffe absichern.

b)

Kryptographie kann Sicherheitsziele nur bis zu dem Punkt schützen, ab dem es einfacher ist sich die Informationen auf einem Anderen weg als dem direkten Knacken des Systems zu besorgen. Hier kommt wieder das Angreifermodell zum Tragen: Eine Festplattenverschlüsselung kann die Vertraulichkeit und Integrität der gespeicherten Informationen nur so lange gewähren, bis der Benutzer (z.B. durch Beugehaft) gezwungen wird sein Passwort zu verraten.

c)

> there's no test possible that can prove the absence of flaws

Systeme werden meist nur auf Funktionalität hin überprüft (d.h. ob das System das tut, was gefordert wird). Um die Abwesenheit von Fehlern zu attestieren müsste man allerdings sicherstellen, das das System für alle möglichen Eingaben nur das geforderte tut. Da dies nicht möglich ist, kann man lediglich prüfen ob das System für einen bestimmten bekannten Angriff anfällig ist. Selbst wenn ein System allen zur Zeit der Erstellung bekannten Angriffen standhält, heißt das nicht dass das System auf Dauer sicher bleibt.

d)

Ein gutes kryptographisches System muss vom Design (Mathematik), über die Implementierung (Elektrotechnik, Programmierung) bis hin zur Installation und Benutzung den Anforderungen entsprechend umgesetzt werden. Die Sicherheit eines (kryptographischen) Systems stellt also eine Kette da, bei der das schwächste Glied darüber entscheidet ob das System sicher ist oder nicht. Die Tatsache, dass bei den einzelnen Gliedern verschiedenes Wissen über die Problemstellung vorliegt, macht das Unterfangen umso schwieriger.

Bereits beim Entwurf des System sollte darauf geachtet werden, dass Folgende Fragen beantwortet werden:

- **Was** soll das System schützen?
- **Vor wem** soll das System schützen?
  - Motivation
  - Ressourcen (Zeit, Geld, Hardware, Software, Know-How)
- **Wie lange** soll das System schützen?
- **Wer** wird das System einsetzen?
- **Wie** wird der Benutzer das System einsetzen?

e)

Durch die Politik das Versagen von Sicherheitssystemen unter den Teppich zu kehren wird den zukünftigen Machern neuer Systeme die Möglichkeit verwehrt aus den Fehlern voriger Generationen zu lernen. Sie können ihre Systeme nicht gegen einen Angriff absichern, der nie publiziert wurde.

f)

Neben der Beantwortung der in d) aufgeführten fragen, sollten die Macher künftiger kryptographischer Systeme, immer davon ausgehen dass der Angreifer mächtiger ist und über mehr Ressourcen verfügt als erwartet. Das entworfene System sollte also auch fragen Standhalten wie: Was wäre, wenn der Angreifer ein vielfaches an Speicherplatz/Rechenleistung/ etc. zur Verfügung hat? Ein gutes kryptographisches System zieht heute bereits die Angreifer von morgen in Betracht.