Was schert uns Verschlüsselung?

Reinhard Wobst

Datenspuren 2007, 5.5.07

Über den Autor:

- Spezialist für Kryptografie ("Abenteuer Kryptologie", Addison-Wesley)
- verdient Geld u.a. mit Angsterzeugung, bietet Kryptografie als Lösung an
- beschädigt mit diesem Vortrag systematisch eine seiner Lebensgrundlagen, indem er die Bedeutung der Kryptografie stark herabsetzt

Anliegen des Vortrags:

- Aufräumen mit den Mythen
  - von geknackten Algorithmen
  - von alles mitlesenden Geheimdiensten
  - Unsicherheit wegen "nur" 128 Bit langer Schlüssel ...
  - oder Hintertüren in guten Algorithmen
- will die wirklich gefährlichen Schwachstellen aufzeigen
- will einige Lösungen anbieten:
  - Key handling
  - Sicherheitskonzepte
  - gesunden Menschenverstand entwickeln

- "echte" Spionage vorstellen (Ex-NSA-Mitarbeiter)

Der Mythos knackbarer Algorithmen

"256 Bit lange Schlüssel sind sicherer als 128 Bit", "Schlüssel durchprobieren ist eine Frage finanzieller Ressourcen"

Bei Star Trek - ja. Grobe Rechnung:

$2^{128} \approx 3.4 * 10^{38}$. Bei 100 Milliarden Dechiffrierungen pro Sekunde (reine Utopie!) und 10 Millionen Computern weltweit würde das Durchprobieren aller Schlüssel

$$3.4 * 10^{38} * 10^{-11} * 10^{-7} = 3.4 * 10^{20} \text{ sec}$$

dauern; ein Jahr hat ca. 31 Millionen Sekunden, macht rund 10^{13} Jahre ... möglicherweise ist unser Universum jünger.
Energieverbrauch, Siliziumbedarf.
Noch besser: Bei 256 Bit und utopisch schnellen CPUs kann man zwar einen Rechner bauen, der in einem Jahr alle Schlüssel durchprobiert, aber der bildet dann wegen seiner riesigen Masse ein schwarzes Loch, d.h. man kann das Ergebnis nicht mehr verwerten.

"Die Geheimdienste können alle Algorithmen knacken"

- Bis heute keine Schwachstelle bei DES gefunden (obwohl man immer eine NSA-Hintertür vermutete - inzwischen sind aber die Designkriterien bekannt), nur gibt es inzwischen Hardware, die 56-Bit-Schlüssel durchprobieren kann (Deep Crack, oder Copacobana: www.copacobana.de) - wenige Tage (immerhin!).
- AES wurde von den führenden Köpfen weltweit über Jahre hinweg geprüft und ständig untersucht. Schwachstelle nicht auszuschließen, doch anzunehmen, dass gerade die

NSA diese kennt, ist einfach Paranoia - auch dort braucht man sichere Algorithmen und greift auf öffentliche Forschung zurück!

Key Handling: Schwachpunkt!

Das Erzeugen, Speichern und Verwalten von Schlüsseln ist viel kritischer als der Algorithmus selbst - in der Praxis.

Für Interessenten: Mein Artikel "Geheimniskrämerei" in der iX 1/07, S.110-114.

Schlüsselerzeugung:

- schlechteste Methode: Passwort als Schlüssel. Starr, unsicher, fehleranfällig. *Es ist ein schwerer Designfehler, die Verantwortung für Sicherheit auf den Endnutzer abzuladen!*

Beispiel: cryptfs, Passwort nicht auswechselbar. Unzählige Anwendungen ...

Wenn schon, dann *Passphrase* ("Mir sitsn heutahmd zusammn/un quatschn Mist?") - für Tippkünstler, oder abgeleitet darauf: **Mshz/uqM?**

- Richtig: Sitzungsschlüssel zufällig erzeugen, diesen mit Passphrase verschlüsseln. Kryptografischer Zufall = nicht vorhersagbarer Zufall; statistische Eigenschaften viel weniger interessant (einmal durch MD5/SHA-1 jagen ...)

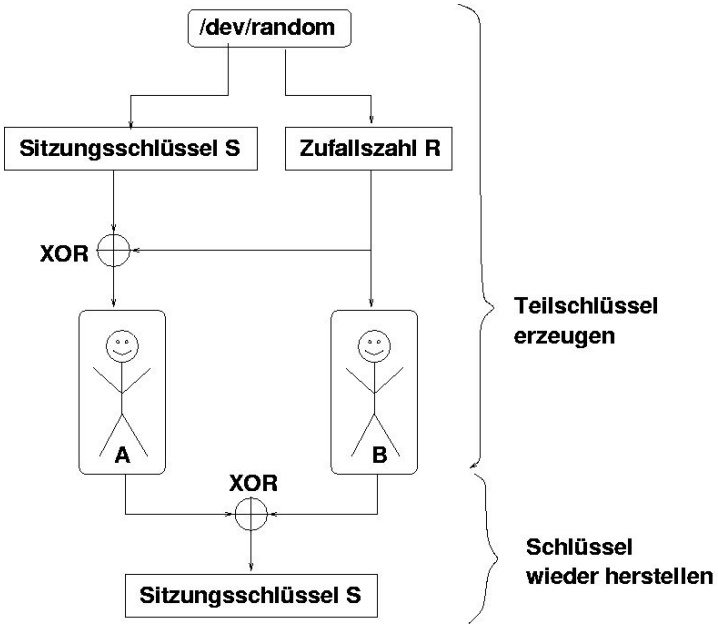
Schlüssel anwenden

- Minimum: Salting + Stretching (vgl.a. Ferguson/Schneier, Practical Cryptography, Wiley 2003, ISBN 0-471-22357-3, oder auch Wikipedia) - schon beim UNIX-Login der 70er Jahre, immer noch nicht bei einigen Windows-Anwendungen

Schlüssel speichern

- Problem **Mitarbeiter-Kündigung:** Alles neu verschlüsseln? Ausweg: Sitzungsschlüssel
- Problem **Vertrauen** (single point of failure, Schlüssel kann gestohlen werden):

- Speichern in **Hardware** - **Zwei-Faktor-Authentifizierung** z.B. (Kosten, vergessen, Kompatibilität)
- Schlüssel teilen: **Secret Splitting** (Vier-Augen-Prinzip):



Nachteil: Wenn Alice oder Bob vergesslich sind, ist alles verloren

- **Secret Sharing:** "beliebige zwei von drei Personen können den Schlüssel wiederherstellen" (Beispiel eines nutzbaren Python-Skripts: http://home.wtal.de/rwobst/addenda/secshare.zip
  Damit lässt sich das "Kündigungsproblem" lösen.
- **Gretchenfrage:** Einfach zu implementieren - aber wer wendet das alles an? (EFS bei Windows: Suche Schlüssel auf der Platte!)

Fazit:

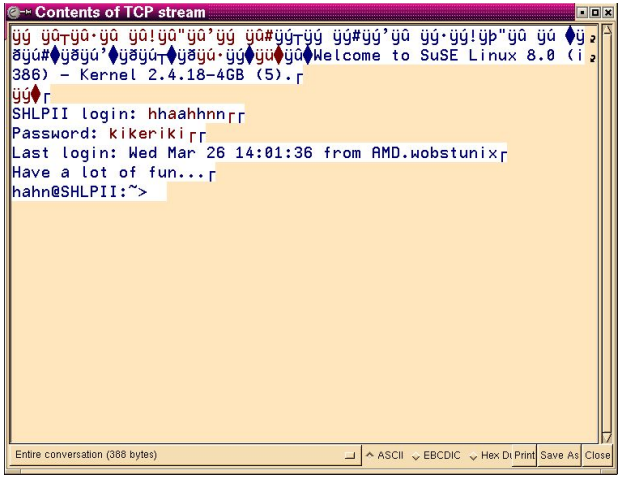
Ohne Grundkenntnisse der Kryptografie bitte NICHTS implementieren!

Schöne Theorie ... der Spion denkt anders

Grundsatz: Ein Angreifer sucht immer die schwächste Stelle und versucht immer, möglichst billig zum Ziel zu kommen:

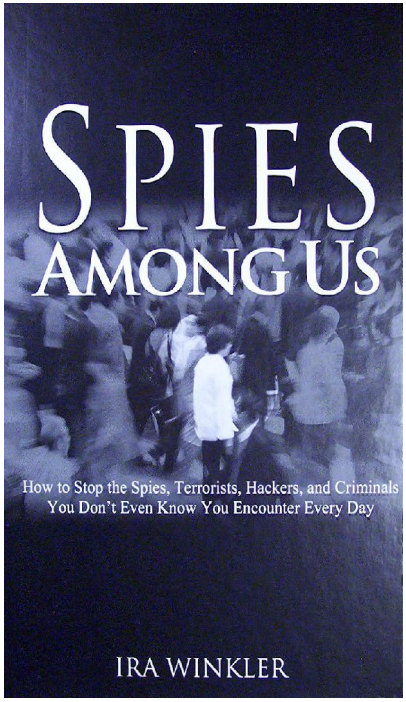
- Wenn GnuPG/PGP richtig angewendet wird, baut man in lohnenden Einzelfällen eben einen Hardware-Keylogger ein (hilft auch bei Knoppix nicht mehr) - aus der Praxis
- Ansonsten tut es auch ein Bundestrojaner (oder ein guter Trojaner von wirklich fähigen Diensten ☺)
- Social Engineering (aber: Handarbeit, teuer)

- Warten, bis Info ungeschützt über das Netz geht (Beispiel aus Mailingliste - an einer Stelle zufällig Familienname doch verraten, und schon hat man sie binnen 10 Minuten ergoogelt/eryahoot/erpresst)
  Hilfreiche Tools hierzu: telnet (hallo, liebe Windows-Nutzer!). Beispiel für User "hahn", Passwort "kikeriki":



- Data Mining - die Waffe des 21. Jahrhunderts (http://www.c3d2.de/datenspuren/2005/vortraege/Keynote.pdf)

Wie der Profi vorgeht



(Wiley 2005, ISBN 0-7645-8468-5)

- Ira Winkler ist Ex-NSA-Mitarbeiter (und darf das sagen)
- Spionage im Auftrag der betroffenen Firmen ("Universalhacker")
- erste 30 Seiten Pflichtlektüre für alle, die Geheimdienste interessiert: Wie wird dort gearbeitet? (Die Stasi war zwar brutal, aber sowas von rückständig ...)
- Mehr dazu in einem Artikel der LanLine Spezial diesen Mai - oder im Buch!

Spektakulärster Auftrag: Diebstahl von Konstruktionsunterlagen von Kernreaktoren binnen einer Woche

Wie macht man das?

- Man beginnt an einer Nebenniederlassung im Fischrestaurant.
- Dort steht ein Gefäß für Visitenkarten, unter denen ein freies Mittagessen ausgelost wird. Natürlich wirft dort jeder seine Karte ein. (Merke: Ein guter Spion kennt vor allem menschliche Schwächen.)
- Kellnerin ablenken, eine Karte stehlen.

- Mit der Karte zum Einlass der Nebenstelle fahren: "Ich habe mein Badge verloren, hier ist meine Visitenkarte." - "OK, melden Sie sich ..." (keine Kontrolle, unpraktisch) - ich kenne es besser!
- Von der Tiefgarage aus konnte man ins Innere des Gebäudes gelangen (ich kenne Besseres! - obwohl man üblicherweise hinter jemandem durchschlüpft; James Bond machte es vor, so geht das auch in der Praxis)
- Vom Innern des Gebäudes kommend, erregt man keinen Verdacht, wenn man fragt, wo man einen Badge erhält

- beide Eindringlinge unterschrieben ihre Anträge gegenseitig als Vorgesetzte
- mit dem Badge fuhren sie tags darauf zur Hauptniederlassung
- Badge war gar nicht nötig, weil zweite Autospur nicht kontrolliert wurde (kenne ich besser!) - dafür aber die Auftraggeber!
- Unerwartet fragte man sich zur Grafikabteilung durch, weil dort die Angebote gespeichert werden. (Merke: Schwachstelle gesucht, wie die Wetterschiffe der Wehrmacht beim Enigma-Knacken)

- Gaben sich als Firmenleitung aus und fragten nach verwendeten Textverarbeitungen (rein technisch, also unverdächtig - damit waren Dateiformate und -namen bekannt)
- "Zur Prüfung" bat er, eine Zeile eintippen zu können:
  `cat /etc/hosts`
  (die Sekretärin verstand natürlich nichts - Psychologie und Einfühlungsvermögen ...)
- Damit waren Rechnernamen und IP-Adressen bekannt. So sieht der Netzwerkangriff eines Profis aus!

- Eindringen in Hochsicherheitsbereich mit Vereinzelungsanlage ... auf Frage nach Auftraggeber gab er den Namen eines der Auftraggeber an, der in einer Sitzung saß ... also warten.
- Ein Sysadmin kam vorbei und freute sich über das technische Interesse. Bereitwillig führte er ihn durch den Serverraum, wo IP-Adressen UND Rechnernamen aufgeklebt waren.
- Der Rest war Routine: Der Partner, ein Ex-KGB-Hacker, drang mittels der Standardpasswörter (nie verändert) sofort in alle Bereiche ein. Man schreckte sogar vor der

gewonnenen Datenflut zurück und begnügte sich mit den Konstruktionsunterlagen.

- Aufgabe war binnen eines halben Tages erledigt, Abflug aus der unfreundlichen Wüstengegend, Erholung verdient.

Merke: Das ist harte und riskante Arbeit, die viel Erfahrung und Geschick erfordert. Die Leute werden zu Recht gut bezahlt ☺

Schlussfolgerungen

- Kryptografie ist nur ein ganz kleiner Teil der Sicherheit.
- Trotzdem verschlüsseln und Schlüssel richtig handhaben, denn ohne Kryptografie geht es nicht.
- Immer das gesamte Sicherheitskonzept im Auge haben: Angreifer sucht die schwächste Stelle, schert sich nicht um unsere Einbruchsrichtlinien.
- Immer fragen: Wer ist überhaupt am Angriff interessiert? Lohnt sich der Aufwand?
- Sicherheit darf nicht auf dem Bewusstsein des Anwenders basieren.