Next Generation Privacy - PGP 5.0

Bernd Lehle / Oliver Reutter

Manch einer wird sich fragen, warum denn nun eine neue Version von PGP herauskommt, nachdem die letzte gerade begonnen hat Fuß zu fassen. Es gibt aber viele ge-wichtige Gründe, PGP komplett neu zu überarbeiten. Diese reichen von der Umgehung von patentrechtlichen Problemen über die Anpassung an aufkommende Standards bei der digitalen Signatur bis hin zur Verbesserung der Benutzer-Interfaces. Wie es den Entwicklern diesmal gelang, PGP rechtlich völlig legal aus den USA auszuführen, ist ein weiteres Kabinettstückchen, das wieder eindrucksvoll vor Augen führt, wie sinnlos ein Verbot von starker Kryptographie Ist.

PGP 5.0 ist ein Projekt, das schon seit 1994, kurz nach dem Release der Vorgängerversion 2.6.3 begonnen wurde. Damals sollte es PGP 3.0 heißen, um den deutlichen Versionssprung hervorzuheben. In der Zwischenzeit kam aber ein Programm namens PGP-Mail 4.5 auf den Markt, das ebenfalls noch zur alten Generation von PGP gehörte. Um die Benutzer dann nicht komplett zu verwirren, wurde die neue Version mit der Nummer 5.0 dann über alle anderen gestellt.

Der Source Code ist unterteilt in einen plattformunabhängigen Teil und speziellen Code für Unix, Windows und Macintosh. Zum Erstellen von lauffähigen Versionen werden immer der plattformunabhängige und der jeweils systemspezifische zusammen benötigt. Alle vier Listings wurden als Bücher veröffentlicht. Wozu um alles in der Welt veröffentlicht man Software als Bücher mit insgesamt 6 000 Seiten? Ganz einfach - die amerikanische Verfassung schützt die Verbreitung, und damit die Ausfuhr, von Büchern im Rahmen der freien Meinungsäußerung. Somit konnte der Source Code legal die USA verlassen. Zwei Tage nach dem offiziellen Release von PGP 5.0 in den USA, am 16. Juni 1997, lagen die Bücher in Norwegen und wurden Seite für Seite eingescannt.

Die holländischen Hacker von HackTic wollten nicht solange warten und hatten über unbekannte Kanäle die US-Originalsoftware als Executable ebenfalls zwei Tage nach Veröffentlichung besorgt und auf http://www.utopia.hacktic.nl/ bereitgestellt. Das amerikanische Wirtschaftsministerium zeigte sich von der schnellen Verbreitung der exportbeschränkten Software überrascht.

Am 11. August 1997 gab es das erste beta-Release der internationalen Unix-Version. Drei Monate später kam eine Version für DOS sowie Win95/NT heraus. Die Mac-Version wird sicher bis 1998 dauern.

Was ist neu an PGP 5.0 ?

Die Neuerungen erstrecken sich sowohl auf die mathematischen Innereien von PGP als auch auf das Benutzerinterface. Die Innereien sind bei allen Versionen gleich, das Interface unterscheidet sich verständlicherweise. Daher sollen die einzelnen Neuerungen gesondert betrachtet werden. Die wichtigen und plattformübergreifenden mathematischen Innereien kommen zuerst.

Mathematische Neuerungen

Alle bisher in PGP verwendeten Algorithmen hatten ihre kleinen Probleme:

1. **Public Key Algorithmus**: Hier wurde bisher RSA verwendet. RSA ist in den USA patentiert. Das Patent läuft am 20. September 2000 aus. Für PGP durfte in den USA daher nur die proprieläre RSAREF-Implementierung benutzt werden. Außerhalb der USA war das kein Problem.
2. **Hash Function**: Die für die digitalen Unterschriften benötigte One Way Hash Function war bisher MD5. In diesem Algorithmus wurden in letzter Zeit einige Schwächen gefunden, die ihn als nicht so sicher erscheinen ließen, wie bisher vermutet.
3. **Symmetrischer Verschlüsselungsalgorithmus**: Für den hier zum Einsatz kommenden Algorithmus IDEA existiert ein Patent der schweizer Firma Ascom. Damit mußte PGP bisher für den gewerblichen Gebrauch lizensiert werden.

All diese Probleme haben den Benutzern von PGP bisher ziemliches Kopfzerbrechen bereitet. Insbesondere die IDEA-Lizenz ist für Anwender u.U. teuer (US$ 15 pro Mitarbeiter in kleineren Firmen), wenn sie gewerblich PGP verwenden. Um all diese Probleme aus dem Weg zu räumen, wurde PGP 5.0 so programmiert, daß keine laufen-den Patente berührt werden.

Als Public Key Algorithmus wird nun EIGamal verwendet. Dieser Algorithmus ist an sich nicht patentiert. Er beruht aber signifikant auf der ersten veröffentlichten Public Key-Verfahren von Diffie und Hellman. Dieses wurde aber schon 1977, ein Jahr nach seiner Veröffentlichung patentiert, damit lief das Patent am 29. April 1997 aus und EIGamal ist damit frei verwendbar. Aus Kompatibilitätsgründen ist RSA weiterhin in PGP 5.0 enthalten.

Anders als bei den früheren Versionen von PGP, bei denen mit RSA sowohl verschlüsselt als auch unterschrieben wurde, kommen bei PGP 5.0 unterschiedliche Verfahren zum Einsatz. Zum Unterschreiben wird der DSA (Digital Signature Algorithm) verwendet. DSA ist eine Variante des Schnorr/EIGamal Signaturalgorithmus [4]. Mit ihm sind nur digitale Unterschriften aber keine Verschlüsselungen möglich. Dieser Algorithmus wurde in einem umfangreichen Proposal unter dem Namen DSS (Digital Signature Standard) 1991 standardisiert.

Ein anderer Bestandteil von DSS ist der Secure Hash Algodthm SHA. Dieser Algorithmus basiert zum Teil auf MD5 und weist bisher keine Schwächen auf. Statt den 128 bit von MD5 erzeugt er eine 160 bit lange Prüfsumme.

Als symmetrische Verschlüsselungsverfahren werden CAST und Triple-DES verwendet. CAST ist eine neuere kanadische Entwicklung mit variabler Schlüsseilänge, Triple-DES ist das altbekannte DES dreimal hintereinander mit verschiedenen Schlüsseln ausgeführt, was zu einer effektiven Schlüssellänge von 112 bit führt. Für CAST verwendet PGP 5.0 128 bit Schlüssellänge. Aus Kompatibilitätsgründen versteht PGP 5.0 auch noch IDEA. Offenbar verursacht das aber keine patentrechtlichen Probleme mehr.

Neuerungen Im Kommandozellen-lnterface (Unix und MS-DOS)

Bisher war PGP ein einheitliches Programm und wurde aus der Kommandozeile zu jedem Zweck mit anderen Optionen aufgerufen. Bei PGP 5.0 wurde dies in vier Kommandos auseinandergezogen, die den bisherigen vier Hauptoptionen entsprechen. So gibt es zum Schlüssel verwalten das Programm `pgpk` (bisher `pgp -k ...`), zum Verschlüsseln `pgpe` (bisher `pgp -e ...`), zum Unterschreiben `pgps` (bisher `pgp -s...`) und zum Überprüfen von Unterschriften, bzw. zum Entschlüsseln `pgpv` (bisher `pgp v...` oder einfach nur `pgp`). Technisch existieren allerdings nur zwei Programme, `pgp` und `pgpk`. Die anderen, `pgpe`, `pgps` und `pgpv` sind symbolische Links (Unix) oder Kopien (DOS) des Programms `pgp`, das, wenn es alleine aufgerufen wird, nur eine

Benutzungsmeldung ausdruckt und nicht verwendbar ist.

Als Eselsbrücke kann man sich merken, daß die wichtigste Option nun Teil des Programmnamens geworden ist und die anderen Optionen einfach angehängt werden. Schlüssel wurden früher mit `pgp -kg` erzeugt, nun geht es mit `pgpk -g`. Ausnahmen gibt es natürlich auch. So kann man sich seine Schlüsselringe nicht mehr mit `pgpk -v` (früher `pgp -kv`) anschauen, sondern mit `pgpk -i`. Alle Mailprogramme, die bisher auf diese Weise PGP als Backend benutzt haben, müssen natürlich auf PGP 5.0 neu angepaßt werden.

Die Prozedur, wie die zwei neuen Schlüsselpaare (eins zum Verschlüsseln, eins zum Unterschreiben) erzeugt werden, ist mit der bisherigen vergleichbar und hat eine verständliche Benutzerführung. Neu ist dabei die Geltungsdauer, die man einem Schiüssel mitgeben kann.

Zu erwähnen ist vielleicht noch der Speicher-Manager DOS4GW, der bei der DOS-Version mitgeliefert wird und ohne den PGP dort nicht läuft. Die Verwendung ist etwas seltsam, aber wenigstens gut dokumentiert.

Neuerungen Im Windows-Interface (Windows NT, Windows 95)

Da es bisher überhaupt kein Interface für Windows gab, sondern nur eine DOS-Version, die von Plug-Ins diverser Mailprogramme aufgerufen wurde, ist es quasi keine Neuerung, sondern eine Neuentwicklung.

Die Windows-Version ist binär als zip-Files erhältlich, das ausgepackt und dann installiert werden muß. Das Paket enthält ein schönes Key Management-Programm (PGP Keys), das auch automatisch mit einem Key Server kommunizieren kann kann. Die Schlüsselerzeugung läuft gut steuerbar und unter Begleitung einer hübschen Animation. Leider ist die Erzeugung von herkömmlichen RSA-Schlüssein noch nicht implementiert.

Die Schlüssel sind dann als Dateien vorhanden, die durch auffällige Icons gut sichtbar sind. Ebenfalls wird eine Verknüpfung für alle PGP-relevanten Dateiformate erzeugt, so daß bei Doppelklick auf signierte oder verschlüsseite Files sofort die entsprechenden Anwendungen gestartet werden. Verschlüsseite Dateien haben auch eigene Icons. Wird auf eine Datei mit der rechten Maustaste geklickt, gibt es einen Menüpunkt PGP, der dann alle anwendbaren Funktionen enthält. Was bisher noch fehlt, ist die Möglichkeit konventionell, d.h. nur symmetrisch, zu verschlüsseln.

Dem Paket sind auch Plugins für Exchange und Eudora beigefügt. Exchange stand uns zum Test nicht zur Verfügung, das Eudora-Plugin ist noch nicht implementiert, daher können wir zu den Plugins keine Aussagen machen.

Ein lästiges Problem bei unserem Test war lediglich, daß die Windows-Version keine Schlüssel der amerikanischen Linux-Version akzeptieren wollte und umgekehrt. Auch innerhalb der amerikanischen Versionen klappte der Schlüsselaustausch nicht. Dazu ist nach unserem Wissen bisher keine tragbare Lösung gefunden. Innerhalb der bisher verfügbaren internationalen Versionen klappt der Schlüsselaustausch.

Und wie geht es nun weiter ?

Eigentlich stünde einer schönen neuen PGP-Welt nichts mehr im Wege. Man muß nur abwarten, bis der ganze Papierberg gescannt ist und die neue Generation der Verschlüsselung steht bereit.

Leider funktioniert das nicht so einfach. Die Lizenz, die PGP Inc. an seine Papierberge koppelte,

erlaubt nur das Scannen des Quelltextes und dessen Verbreitung. Es erlaubt NICHT dessen Veränderung (Nachzulesen beim Punkt Noncommercial Distribution). Daß diese Veränderung aber dringend notwendig ist, zeigte sich sofort nach Ausprobieren der ersten Unix-Versionen. Glücklich konnten sich die Benutzer schätzen, unter deren Unix-Dialekt der Source Code überhaupt fehlerfrei kompilierte. Noch glücklicher waren die, bei denen die Executabies hinterher ohne sofortigen Absturz liefen. Aber selbst bei dem System, wo die wenigsten Fehler auftraten - bei Linux - waren die Programme hinterher so instabil, daß an ein effektives Arbeiten nicht zu denken war. Sinnige Fehlermeldungen wie `cannot write to /dev/null` überraschen den Benutzer an allen möglichen Stellen. Auch die Windows-Versionen haben so ihre Fallstricke. Die Unmöglichkeit des Schlüsselaustausches mit und innerhalb der amerikanischen Version hatten wir ja schon erwähnt. Unter diesen Voraussetzungen ist PGP 5.0 in der frei erhältlichen Version nicht im geforderten Maß von Poriabilität, Sicherheit und Zuverlässigkeit einsetzbar.

Im Herbst 1997 fand daraufhin in München eine Konferenz der Internet Engineering Task Force (IETF) statt. Der Beschluß über einen einheitlichen Verschlüsselungsstandard im Internet stand zur Debatte. Als Kandidaten standen PGP und S/MIME zur Wahl. S/MIME wird vom Netscape Navigator und vom Microsoft lnternet Explorer in zwei nicht kompatiblen und nicht offengelegten Versionen verwendet. Dadurch, daß PGP nun offiziell offen engelegt wurde, wie es sich für einen Internet-Standard gehört, gewann es natürlich das Rennen gegen S/MIME. Gleichzeitig stellte das Gremium allerdings fest, daß der einzige Weg zu einer neuen Generation von PGP, OpenPGP ge-tauft, nur über ein komplettes Reengineering der PGP 5.0 Sourcen laufen kann. Der Aufwand dafür wird auf drei bis vier Mannjahre geschätzt. Im Klartext heißt das, daß es vor Mitte 1998 keine stabil verwendbare und plattformübergreifende Version von PGP 5.Oi geben wird.

Allen, die weiterhin auf eine vertrauliche Kommunikation Wert legen, können wir daher nur die Verwendung von PGP 2.6.3i empfehlen. Von der kommerziellen amerikanischen Version von PGP 5.0 können wir ebenfalls nur abraten. Die Benutzung außerhalb der USA ist zwar nicht verboten, wenn sie einmal exportiert wurde, aber sie enthält Schnittstellen für Nachschlüssel. Diese Schnittstellen sind normalerweise zwar nicht aktiv, können aber aktiviert werden, wenn dies z.B. in einer Benutzergruppe gewünscht wird. Ob die Freeware Version diese Schnittstelle auch enthält, ist bisher nicht bekannt. Da sich die internationale Version nur im Namen und im primär kontaktierten Key Server unterscheidet, könnten diese Schnittstellen dort auch vorhanden sein.

Die Nicht-Amerikaner lehnen Nachschlüsei für Open-PGP bisher strikt ab. Daher kann man erst bei Verfügbarkeit dieses Standards guten Gewissens den Schritt auf 5.0 wagen.

Latest News

Ganz kurz vor der Drucklegung kam noch folgende Meldung über den Ticker:

Pretty Good Privacy Incorporated wurde am 01.12.1997 von der Firma McAffee aufgekauft, die Marktführer im Bereich Anti-Viren-Software ist. Die gemeinsame Firma wird Network Associates Incorporated heißen. Was diese Entscheidung für die Zukunft von PGP bedeutet, ist bis jetzt noch völlig unklar...

Literatur

[1] Garfinkel, S., PGP, O'Reilly and Associates

[2] International PGP Homepage: http://www.pgpi.com/

[3] Deutsche PGP-Anleitung: http://www.hkn.de/user/raven/pgpan ltg.htm

[4] Schneier, B., Applied Cryptography, Wiley and Sons

Ansprechpartner in sicherheitsrelevanten Fragen

- sneakers@rus.uni-stuttgart.de
- dfncert-request@cert.dfn.de

Bernd Lehle, NA-5531 (bis 31.12.1997)
E-Mail: lehle@rus.uni-stuttgart.de

Oliver Reutter, NA-4513

E-Mail: oliver.Reutter@rus.uni-stuttgart.de
