DuD
Datenschutz und Datensicherheit

PGP, quo vadis?

Die Zukunft von PGP, GnuPG und OpenPGP

Rainer W. Gerling, Stefan Kelm

Seit nunmehr einem Jahrzehnt gilt das Programm PGP („Pretty Good Privacy“) als der Standard für E-Mail- und Datei-Verschlüsselung, insbesondere unter Internet-Benutzern. Seit der allerersten Version der Software hat sich jedoch vieles verändert, und noch immer wird an der Verbesserung von PGP gearbeitet – gelegentlich auch, weil ein versteckter Fehler gefunden wird.[1] Dieser Beitrag stellt den aktuellen Stand aus der Sicht zweier langjähriger PGP-Benutzer dar.

Dr.
Rainer W. Gerling

Datenschutzbeauftragter der Max-Planck-Gesellschaft, Lehrbeauftragter für Datensicherheit an der FH München.
Studium der Physik an der Universität Dortmund. Promotion und Habilitation an der Universität Erlangen-Nürnberg.
E-Mail: rgerling@gmx.de

Stefan Kelm

Secorvo Security Consulting GmbH.
Arbeitsschwerpunkt: Public Key Infrastrukturen, digitale Signaturen, Rechner- und Netzwerksicherheit
E-Mail: kelm@secorvo.de

[1] Zu Fehlern in PGP siehe auch Senderek, DuD 10/2000, S. 603-608 und Knobloch, in diesem Heft.

1 Einleitung

Die erste Version von PGP beginnt Phil Zimmermann unter dem Eindruck der US Senate Bill 266 im Jahre 1991 zu schreiben. Dieser Gesetzentwurf verlangte, dass jedes Verschlüsselungsprodukt eine Hintertür für die Strafverfolgungsbehörden enthalten soll. Phil Zimmermanns Idee war, PGP vor Inkrafttreten des Gesetzes so weit zu verbreiten, dass das Gesetz ins Leere laufen würde. Zum Glück ist der Entwurf nie geltendes Recht geworden. Aber trotzdem veröffentlicht Phil Zimmermann noch im gleichen Jahr PGP 1.0 mit den Algorithmen RSA und MD4[2] sowie dem selbst entwickelten Base-O-Matic. Schon im nächsten Jahr allerdings wird PGP 2.0 mit den Algorithmen IDEA, RSA und MD5 veröffentlicht.

Den „Ritterschlag“ erhält Phil Zimmermann aber 1993, als die US-amerikanische Regierung gegen ihn wegen illegalen Waffenexports zu ermitteln beginnt. Nach dem damals geltenden amerikanischem Recht ist Verschlüsselungssoftware eine Kriegswaffe,[3] für deren Export eine entsprechende Lizenz erforderlich ist. Da in der Zwischenzeit frei verfügbare Versionen von PGP rund um den Globus aufgetaucht waren, wurden entsprechende Ermittlungen gegen Zimmermann eingeleitet.

Parallel dazu wird PGP von verschiedenen Seiten angegriffen, da der RSA-Algorithmus vom MIT in den USA patentiert ist[4] und eine Firma namens Public Key Partners[5] das alleinige Recht zur Vermarktung dieses Patents hat. Da PGP das RSA Verfahren verwendet, verletzt es die Lizenzrechte von Public Key Partners. In den USA und Europa ist außerdem der IDEA Algorithmus patentiert.[6] Somit ist außerhalb der USA PGP nur für nicht kommerzielle Zwecke kostenlos verwendbar. Für kommerzielle Anwendungen dagegen wird eine IDEA-Lizenz benötigt. In den USA ist keine legale Anwendung (auch keine nichtkommerzielle) ohne RSA-Lizenz möglich. Auf Druck des MIT entsteht daher im Jahre 1994 mit PGP 2.5 eine Version, die für den nichtkommerziellen Gebrauch durch Verwendung des Toolkits RSAREF in den USA legal eingesetzt werden kann. Außerhalb der USA stört das RSA-Patent indes niemanden, da es nur in den USA gilt.

Die Verbreitung der PGP Version 2.5 wird jedoch durch diese rechtlichen Auseinandersetzungen nicht gebremst, ganz im Gegenteil: Tausende von FTP-Servern weltweit bieten mittlerweile PGP zum freien Download an; insbesondere im universitären Umfeld gewinnen PGP-verschlüsselte E-Mails schnell an Bedeutung.

Schnell entsteht durch Fehlerkorrekturen noch im Jahr 1994 die Version 2.6.2, die bei vielen als die klassische und „einzig wahre“ PGP-Version gilt. Von dem Norweger Stale Schumacher wird eine inoffizielle (aber durch Phil Zimmermann indirekt abgesegnete) internationale Version 2.6.2i erstellt; durch kleine Verbesserungen entsteht nur wenig später die letzte der kommandozeilen-orientierten PGP-Versionen 2.6.3i.

In den USA vertreibt die Firma ViaCrypt eine kommerzielle Version von PGP unter den Versionsnummern 2.7, 4.0 und 4.5.

[2] R.W. Gerling, *Kryptographie* DuD, **21** 197-202 (1997); R.W. Gerling, *Verschlüsselung im betrieblichen Einsatz*, Datakontext Verlag Frechen 2000.

[3] Die „International Traffic in Arms Regulations“ (ITAR, section 121.1) stellten kryptographische Software Panzern, Artillerie und Massenvernichtungswaffen gleich...

[4] U.S. Patent Nr. 4405829, erteilt am 20. September 1983, ausgelaufen im September 2000

[5] Diese Firma bestand aus RSA Data Security Inc. und Caro Kahn Inc. der Muttergesellschaft von Cylink Inc. Sie existiert nicht mehr.

[6] http://www.ascom.ch/infosec/idea.html

In mittlerweile existierenden Internetforen kursieren Gerüchte über ein PGP 3, das Phil Zimmermann und andere[7] nach der Beendigung des Ermittlungsverfahrens herausbringen wollen. Nachdem 1996 das Verfahren eingestellt wird, gründet Zimmermann die Firma PGP, Inc. und kauft ViaCrypt auf. Endlich erscheint dann 1997 PGP 5 (das langerwartete PGP 3 bekam die Versionsnummer 5) als erste Programmversion mit grafischer Benutzeroberfläche unter Windows. Der gesamte Quellcode von PGP 5 und einigen Nachfolgeversionen wird in Buchform[8] publiziert, da Bücher im Gegensatz zur Software legal aus den USA exportiert werden dürfen. In Norwegen, Holland und in der Schweiz wird der Quelltext von kleinen Teams eingescannt, überprüft und neu compiliert, so dass es jetzt eine legale PGP Version außerhalb der USA gibt.

2 PGP heute

Im November 1999 erhält NAI, die in der Zwischenzeit PGP, Inc. übernommen haben, von den US-amerikanischen Behörden eine Export-Lizenz für PGP. Damit ist der komplizierte Export des Quellcodes in Büchern und die damit verbundene Veröffentlichung nicht mehr erforderlich und wird nach wenigen Programm-Updates voraussichtlich endgültig eingestellt.

Phil Zimmermann wiederum ist bei NAI als „Senior Fellow" eingestellt, sein tatsächlicher Einfluss auf die weitere Entwicklung von PGP scheint aber immer mehr zu schwinden. Gleichzeitig veröffentlicht NAI immer schneller neue Versionen von PGP mit immer neuen Funktionalitäten: Heute verfügbare Versionen beinhalten eine Vielzahl unterschiedlicher Features, die mit der ursprünglichen Verschlüsselung von Dateien und E-Mails nur noch wenig gemeinsam haben. All dies führt dazu, dass immer häufiger Kritik sowohl an PGP selbst als auch an NAI laut wird; viele eingeschworene PGP-Benutzer weigern sich wegen mangelnden Vertrauens, immer neue Programmversionen zu installieren.

Ende September 2000 stellt NAI im deutschen Museum in München PGP 7 vor, die auch für Geschäftskunden recht schnell in englisch verfügbar ist. Im Februar 2001 erscheint eine englische Freeware Version von PGP 7,[9] die allerdings nicht mehr von Aktivisten kompiliert, sondern als Binärversion direkt von NAI herausgegeben wird. Im April 2001 folgt dann die deutschsprachige Version für Geschäftskunden.

Die bislang verfügbare Retailversion („Personal Privacy") scheint bisher nicht mehr zu existieren. Damit ist es einer Privatperson nicht mehr möglich, die Zusatzfunktionen PGPdisk, PGPnet (inkl. Firewall und Intrusion Detection System) zu nutzen, da diese Funktionen in der Freeware Version nicht enthalten sind und die Version „PGP Desktop Security" nur mit minimal 25 Lizenzen gekauft werden kann.

Seit einiger Zeit bereits gibt es keinerlei Anzeichen dafür, dass der PGP-Quellcode von NAI noch veröffentlicht werden wird. Der Quellcode zu Tools wie PGPdisk und PGPnet wird wohl in Zukunft definitiv nicht mehr verfügbar sein. Ob die eigentliche Kernfunktionalität, also E-Mail und Dateiverschlüsselung, irgendwann wieder einmal als Quellcode vorliegen und damit potenziell überprüfbar wird, bleibt zum jetzigen Zeitpunkt mehr als fraglich.

Wer seine Software bisher mit Plugins von Drittherstellern PGP-fähig gemacht hat, ist darauf angewiesen, noch bei PGP 6.5 zu bleiben, da NAI bisher (Mai 2001) den Software Development Kit für PGP 7 nicht publiziert hat. Viele Entwickler von kostenlosen Plugins müssen jetzt passen. In der Vergangenheit entwickelten sie ihre Software unter Verwendung des Quellcodes, in Zukunft müssen sie den SDK kaufen. Da Freeware kein Geld abwirft, ein schwieriges Problem. Manches wichtige und kostenlose E-Mail-Programm wird mit PGP 7 nicht mehr zusammenarbeiten.

PGP war und ist eine Software, die vor allem durch Privatanwender und Bürgerrechtler groß geworden ist und die ein exzellentes Image hat. Durch den Verkauf von PGP, Inc. an NAI wurde dieses Image erstmalig deutlich angekratzt: einerseits war NAI zu jenem Zeitpunkt aktives Mitglied der amerikanischen „Key Recovery Alliance" (KRA),[10] einem Verbund von Firmen, die Key Recovery-Mechanismen unterstützen.

Darüber hinaus brach die ADK-Funktionalität[11] (von Firmen durchaus gewünscht) und die damit verbundene und von Ralf Senderek aufgedeckte Sicherheitslücke[12] eine weitere Zacke aus der PGP Krone. Im Februar 2001 schreckte die Meldung, dass Philip Zimmermann NAI verlassen hat die Nutzergemeinde auf.[13] Sollte nun noch der von vielen ersehnte PGP Quellcode ausbleiben, wird die „PGP-Gemeinde" ernsthaft verschnupft sein.

NAI begibt sich hier auf ein gefährliches Pflaster: PGP ist derzeit in Firmenkreisen weit weniger fest etabliert als NAI es sich wünschen könnte – einen weiteren Imageverlust unbeschadet zu überstehen, könnte in Anbetracht dieser Fakten schwierig werden. Und das gute Image ist noch immer ein ganz wesentlicher Vorteil von PGP gegenüber anderen Lösungen. Dieser Vorteil darf nicht aus Kurzsichtigkeit verspielt werden!

Die Zukunft von PGP ist dabei sicherlich immer noch recht spannend. Es gibt seit kurzem eine durchaus attraktives PGPwireless für PalmOS (Abb. 1).[14] Im Gegensatz zu der Freeware Version OpenPGP 1.2[15] für den Palm läuft es extrem stabil.

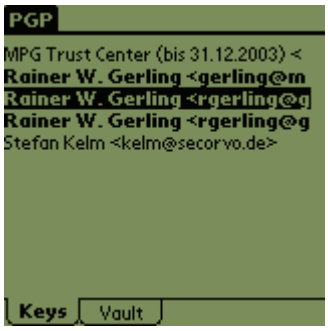

Abb. 1: PGPwireless 1.5 für PalmOS

Das für Spätsommer 2001 angekündigte PGP 7.1 wird erstmalig ein Hardwaredevice (Ikey 2000 von Rainbow[16]) zur Schlüsselgenerierung und zur sicheren Speicherung des privaten Schlüssels unterstützen. Gerüchten zu Folge ist PGP (bzw. Teile davon) auch gerade im Prozess der Evaluierung

[7] Neben Phil Zimmermann haben sich zu diesem Zeitpunkt insbesondere die beiden MIT-Mitarbeiter Derek Atkins und Colin Plumb an der Weiterentwicklung von PGP beteiligt.

[8] Die mehrere Tausend Seiten umfassenden Bücher sind in einem speziellen OCR-Font bedruckt, der das anschliessende Einscannen stark vereinfacht. U.a. werden in den Büchern auch einfache Prüfsummen abgedruckt, die eine automatisierte Fehlerkorrektur der eingescannten Seiten ermöglicht.

[9] http://www.pgpi.org/

[10] Die Mitgliedschaft wurde später – nach Aussagen von NAI – widerrufen.

[11] R.W. Gerling *Company Message Recovery* DuD, 22 38 (1998)

[12] Siehe Senderek, DuD **24** 603-608, 2000

[13] Siehe DuD **25** 245, 2001

[14] Patrik Brauch, Kryptomobil, c't 10/2001, Seite 102.

[15] http://home.foni.net/~mohnhaupt/pilot/pilot-sw.htm#pgp

[16] http://www.rainbow.com/ikey/

und Zertifizierung nach Common Criteria[17] und könnte dann sogar zu bestimmten Sicherheitsniveaus der Europäischen Signaturrichtlinie[18] konform sein. Dies wird aber eine sichere Speicherung des Schlüssels in einem Hardwaredevice voraussetzen.

2.1 pgp.net

Seit den ersten Erfolgen von PGP haben sich auch international betriebene Keyserver für die Verteilung von PGP-Schlüsseln etabliert. Alle diese Keyserver laufen auf UNIX-basierten Workstations; zum Einsatz kommt eine OpenSource-Software, die mehr oder weniger stabil läuft. Die Server synchronisieren sich untereinander per E-Mail, so dass es ausreicht, neue Schlüssel oder Signaturen an einen der Server zu senden.

Zur Vereinfachung der Adressierung wurde bereits vor einigen Jahren die Domain *pgp.net* ins Leben gerufen, unter der alle Keyserver einheitlich erreichbar sein sollen. Da diese jedoch ausnahmslos von Freiwilligen betrieben werden (in Deutschland beispielsweise von den Mitarbeitern der DFN-PCA[19]), kommt es in regelmäßigen Abständen zu Problemen, was in erster Linie mit den riesigen Datenmengen zusammenhängt.[20] Darüber hinaus ist es derzeit nicht möglich, einmal an die Server übermittelte Schlüssel wieder zu löschen.

Problematisch ist ferner die Tatsache, dass die von NAI betriebenen Keyserver (*pgp.com*, *nai.com* bzw. *pgpkeys.mit.edu*) sich nicht an der Synchronisation mit den Servern von *pgp.net* beteiligen. Neue Schlüsselringe werden von NAI nur in sehr unregelmäßigen Abständen zur Verfügung gestellt, so dass hier abweichende Datenbestände existieren.

2.2 OpenPGP

In dem Standard OpenPGP[21] wird das Dateiformat in Anlehnung an PGP definiert, damit unabhängige Implementierungen möglich sind. OpenPGP sieht dabei ein neues Signaturformat mit Sub-Paketen vor. GnuPG erzeugt OpenPGP-kompatible Dateien, während PGP 6.x/7.x nicht hundertprozentig OpenPGP-kompatibel ist.

Die beiden Tschechen Vlastimil Klima und Tomas Rosa publizierten zur CeBit 2001 eine Sicherheitslücke im Format des privaten Schlüsselbundes.[22] Die Ausnutzung dieser Lücke ermöglicht es einem Angreifer u.U., den geheimen Signaturschlüssel eines anderen PGP-Benutzers extrahieren zu können. Eine weitere, jüngst veröffentlichte Schwachstelle beschreibt einen Fehler in der „split key“ Funktionalität von PGP.[23] Beides sind erneut deutliche Zeichen dafür, dass auch etablierte Standards, die von einer Vielzahl von Experten erstellt wurden, nicht vor schwerwiegenden Designfehlern und damit verbundenen Sicherheitslöchern in der Implementation gefeit sind.[24]

2.3 GnuPG

Im September 1999 wird die Version 1.0.0 von GNU Privacy Guard[25] freigegeben. Damit steht ein uneingeschränkt kostenloses Verschlüsselungsprogramm, das OpenPGP konform ist, zur Verfügung. Vom Bedienungskomfort entspricht diese Kommandozeilenversion dem PGP 2.6.3. Es gibt eine Windowsversion, diese wird aber ausdrücklich als ungeeignet für den Produktionseinsatz bezeichnet.

Im Herbst 1999 erzeugt GnuPG aufsehen, als bekannt wird, dass das Bundesministerium für Wirtschaft die GnuPG-Entwicklung mit 318 TDM fördert[26]. Damit beteiligt sich weltweit erstmalig eine Regierung offiziell und aktiv an der Entwicklung von freier Open Source Software. Ein extrem wichtiges politisches Zeichen, welches auch international viel diskutiert wurde.

Die Benutzbarkeit von GnuPG ist jedoch unter Windows derzeit noch nicht gegeben. Es fehlen Plugins für gängige E-Mail Programme. Lediglich für Eudora gibt es eine frühe Version eines Plugins.

Auch die Schlüsselsuche auf Schlüsselservern ist noch nicht benutzerfreundlich, da nach Schlüssel-IDs und nicht nach Namen oder E-Mail Adressen gesucht wird.

Eine grafische Oberfläche mit der wesentlichen Funktionalität von PGPkeys und PGPtray gibt es mit dem GNU Privacy Assistant (GPA). Da auch die Windows Anwendung mit dem Toolkit GTK+[27] erstellt wurde, ist sie für einen Windowsanwender sehr gewöhnungsbedürftig (Abb 2). Dieser Toolkit wurde ursprünglich für die Entwicklung unter X Windows entwickelt. Ein „Windows Look and Feel“ kommt nicht auf.

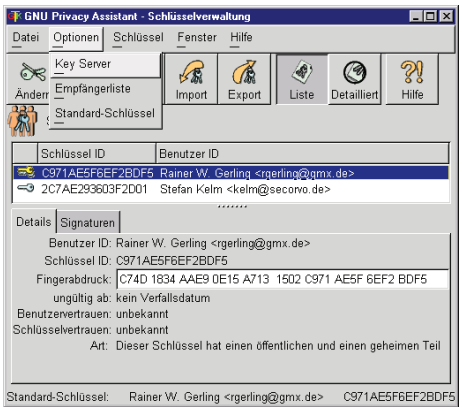

Abb. 2: GNU Privacy Assistent unter Windows NT 4

GnuPG steht erst am Anfang einer hoffentlich erfolgreichen Geschichte. Ein wichtiger Punkt, der entscheidend sein wird für die Zukunft, ist die Verfügbarkeit und Akzeptanz einer guten benutzerfreundlichen Windows-Version sowie entsprechender E-Mail-Clients und Plugins für andere gängige Programme. Nur über Windows kann und wird sich der Erfolg im Massenmarkt einstellen. Die Entscheidung zwischen dem Missionieren der Windows-Benutzer (was nicht unbedingt erfolgreich sein muss) und der Schaffung eines erfolgreichen Produktes muss getroffen werden.

Fazit

PGP und GnuPG stehen an entscheidenden Punkten ihrer Entwicklung. Zur Zeit werden wichtige Weichen für die Zukunft gestellt. Als überzeugte Anwender sehen wir mit einer gewissen Sorge auf diese Entwicklung. Wir wünschen uns, dass die Verantwortlichen die richtigen Entscheidungen treffen und dass wir auch in Zukunft aus Überzeugung hinter diesen Produkten stehen können.

[17] http://www.commoncriteria.org/
[18] Siehe Schwerpunkt in DuD, Heft 2/2000
[19] http://www.cert.dfn.de/dfnpca
[20] Die interne Datenbank der Keyserver hat eine Größe von ca. 1,7 GB, täglich empfängt jeder Server zwischen 20.000 und 30.000 E-Mails.
[21] OpenPGP RFC 2440
[22] Sicherheitslücke in OpenPGP, c't, Heft 8/2001, S. 54 und Knobloch, in diesem Heft.
[23] http://www.securiteam.com/
[24] siehe Knobloch, in diesem Heft
[25] http://www.gnupg.de/
[26] http://www.sicherheit-im-internet.de/
[27] http://www.gtk.org/