Pretty Good Privacy

1. Introduction

1.1. What is cryptography?

Cryptography originates from the Greek word “kryptos” meaning hidden [1]. It is one of the main branches of cryptology which studies methods of securing and authenticating information. Cryptography is concerned with the design of these methods whereas cryptanalysis, the other main branch of cryptology, looks at overcoming them. Cryptography is also described as the science of using mathematics to encrypt and decrypt data for secure transmissions [2 p. 11].

1.2. Why is cryptography important?

The Computer Emergency Response Team (CERT) recorded the total number of computer vulnerabilities from 1995 to 2008 (Q1-Q3) based on reports submitted to them and from other public sources [3]. Security vulnerabilities were included from operating systems on individual machines, routers in networks and other network devices [4 p. 10]. Their statistics show a general trend of the total number of vulnerabilities rising from 171 in 1995 to a peak of 8064 in 2006. Clearly this shows Internet security is a problem albeit a problem which is possibly starting to be tackled more effectively as tenaciously indicated by the decrease in the total number of vulnerabilities from 8064 in 2006 to 6058 in 2008 (Q1-Q3) [3]. Moreover the Internet Architecture Board (IAB) submitted a report in 1994 called “Security in the Internet Architecture” (RFC 1636). The overall conclusion of the report was that “security must be added to the Internet” [5 p. 44] outlining the necessity to secure network infrastructure and traffic by authentication and encryption.

Huge growth percentages between 2000 and 2009 for the number of Internet users [6] indicate more people will use the Internet in the future. Therefore organisations and individuals will rely more and more on the Internet for operations. With more users relying on the Internet with its increasing power and complexity more information will be placed online. Since one of the main motives behind attacking systems is information gathering then cryptography is more important than ever in order to counteract this threat and allow users confidentiality and authentication.

2. Looking at PGP

2.1. What is it?

Pretty Good Privacy (PGP) is a hybrid cryptosystem [2 p. 16]. This means it uses a combination of symmetric and asymmetric cryptographic algorithms [7 p. 1] and contains all the possible keys and protocols that enable it to work. Philip R. Zimmermann is the creator of PGP [2 p. 37] and the founder of PGP Inc. The PGP Corporation claims to be a global leader in data encryption software [8].

2.2. How does it work?

The algorithm PGP uses to transmit a file is as follows. Firstly the file is compressed (if possible) primarily to reduce the chance of cryptanalysis discovering patterns but also to save disk space and transmission time. A private single use session key number is then generated from random movements of a user's mouse and random keystrokes on their keyboard [2 p. 16]. If the user chooses to digitally sign the file then after the private key is generated a cryptographically strong hash function is used on the plaintext (unencrypted file) to produce a fixed length piece of data known as a message digest [2 p. 19]. The private key and message digest can then be used in combination to create a digital signature [2 p. 20] which allows the receiver to verify the information including its origin. PGP can optionally encrypt messages through conventional or symmetric block ciphers (cryptographic algorithms) using the same key (word, number or phrase) to encrypt and decrypt. Three of the block ciphers offered include CAST, Triple-DES and IDEA which work on 64-bit blocks of plaintext and ciphertext (encrypted plaintext). The difference between them is that CAST and IDEA have 128-bit key sizes whereas Triple-DES uses a larger more secure 168-bit key. All three offer cipher block chaining (CBC) and cipher feedback (CFB) modes where PGP uses them in CFB 64-bit mode [2 p. 41]. In CBC mode each block is combined with the previous block in a bitwise exclusive or (XOR) operation ensuring even identical blocks encrypt differently. CFB is similar to CBC except the ciphertext of the previous block is used in the XOR operation instead of its plaintext [9]. If the user opts for encryption then after the plaintext is converted into ciphertext the session key is encrypted to a public key that is

bound to the receiver [2 p. 16]. The receiver then uses their private key from their PGP distribution to recover the temporary session key allowing the ciphertext to be decrypted [2 p. 17].

It should not be taken for granted that a public key belongs to the advertised recipient as an imposter could be acting with their name and ID. There are a variety of ways to authenticate a public key. The simplest and most secure method in terms of confirming user identity would be to ask for it in person. However in most cases this will probably be logistically inefficient. Digital certificates are a commonly used alternative shown by the fact they are used in HTTPS (Hypertext Transfer Protocol Secure) [10 p. 1150]. They usually contain at least three pieces of information pertaining to a person or entity which are a public key, certificate information (such as names, e-mail addresses, etc) and at least one digital signature [2 p. 21].

PGP uses a cumulative (web of) trust model [2 p. 32] although current versions also support a hierarchical model [2 p. 25]. In the cumulative trust model if someone signs a public key certificate they become an introducer of that key whereas in the hierarchical model trust extends from root certificates. There are three levels of certificate validity in the cumulative trust model which are valid, marginally valid and invalid [2 p. 32]. Their assignment depends on how trusted the signatures are. Another user can assign a level of trust to the introducer of a certificate and use the public key they signed for assuming the certificate validates. PGP allows users to assign one of three levels of trust to other users' public keys which are complete trust, marginal trust and no trust [2 p. 32]. To establish a key is valid in PGP it requires either a completely trusted signature or two marginally trusted signatures [2 p. 33]. On top of this PGP allows meta-introducers to be established with numerical assignments above level 0. If you assign level 0 to a user then you trust you have a valid copy of their key. Level 1 is the same as level 0 but you also trust the user to only sign valid keys thus they become a meta-introducer. Level n (where n is a positive integer) is the same as level 0 but you also trust the user only signs keys belonging to people of category n-1 [11 p. 14] again making them a meta-introducer. PGP also supports certificate revocations [2 p. 34] for situations where a private key is lost or stolen and in more recent versions certificate expiration dates [2 p. 24].

2.3. How secure is it?

The two main approaches to attacking a pure version of PGP are theoretical attacks which try to exploit weaknesses of its cryptographic methods and practical attacks which try to exploit the way people use it. Here a pure version of PGP is defined as being compiled from unmodified source code. An impure version could potentially work completely differently with removed, modified and/or added code. For example an attacker could distribute an impure version with malicious code that makes all security related information accessible to them. Without hash checks or similar methods to reliably tell if a distribution is pure or not users would be unaware of this attack.

The RSA algorithm (public key cryptosystem) works using three large numbers, let us call them **P**, **M** and **S** where **P** is the public key, **M** is the modulus of the public key and **S** is the secret key. The message is first interpreted as a number and raised to the power of **P**. **M** is then continuously subtracted from this result until it is less than **M** eventually giving the cryptogram (encrypted message). The recipient performs a similar procedure when they get the encrypted message; they raise the cryptogram to the power of **S** and subtract **M** until the result is smaller than **M** rendering the unencrypted message. **M** must be the product of two prime numbers which, if known, can lead to **P** and **S** being quickly inferred [12]. Therefore an attacker who knows **M** needs only to factorise it to find the primes and from them the keys. However this task proves much more difficult than it sounds because the numbers are so large it is practically impossible to factor them. Overall the extreme difficulties involved in attacking the cryptographic methods of PGP result in attackers focussing on practical attacks.

PGP encrypts a user's private key using a hash of a passphrase they provide [2 p. 35]. If an attacker discovers a user's passphrase and is able to gain access to the computer where their private key is stored then they can obtain that user's private key. Once the private key is obtained if the attacker intercepts that user's messages they can decrypt them. This type of attack is much more likely to be successful compared to attacks on the cryptographic methods because the vulnerability lies not with the system but with the users who are more likely to be fallible. For example a user might write their passphrase down, communicate it and/or be observed whilst entering it. Another way to obtain the passphrase would be for an attacker to infect a user's computer with a virus

or Trojan. The malicious program could log and send to the attacker the keystrokes of the user in the hope that the user would eventually type their passphrase. However all software is subject to this vulnerability thus it should not be the responsibility of PGP to deal with it.

2.4. What are its applications?

The primary use of PGP was originally to encrypt e-mail messages and attachments [2 p. 37] but its applications have since grown due to an increase in features. To name a few it currently supports digital signatures [2 p. 19], disk encryption, file and folder security [13] (specifically on laptops and networks), protection for instant messaging clients [14] and signed and/or encrypted HTTP responses and requests [15]. Since PGP initially solely relied on the cumulative trust model it was not well suited to commercial applications since businesses usually rely on an appointed authority within themselves to confirm information. However since the hierarchical model was added this is no longer a restriction thus expanding its applications.

PGP is useful to anybody who wants to secure their data transmissions or storage and so is applicable to all industries including education, financial services, government, healthcare and retail. Moreover the fact that the source code of PGP was made open to the public [16] for so many years has allowed it to be scrutinized and confirmed. This gives PGP an advantage over its competitors because to the public it appears more trustworthy. On top of this a number of human rights groups have given testimonials to how PGP has benefitted them through letters sent to its creator Philip Zimmerman [17]. These letters make PGP look more ethical and like a product helping to spread democracy. One opposing argument is that the wide availability of PGP or any cryptosystem is a security liability as it could fall into the wrong hands such as those of terrorists. Overall PGP is a tool neither good nor evil with currently widespread applications especially desirable to companies seeking data security.

3. Conclusions

The number of Internet users, vulnerabilities and threats is likely to continue increasing. Although it is conceivable that some users may not be at risk whether the information

they send and/or store is secure or not, this is false in many cases. Securing information is founded on cryptography and for most users is and will probably continue to be automatic and hidden. However the market for cryptosystems will probably grow as more businesses go online and as more users become aware of their advantages and of online threats. PGP is a leading contender in this market with many features aimed at both businesses and individual users. It is based on well understood and theoretically sound principles and although trust seems to have dwindled since its open source days it is still highly regarded around the world.

4. References

1. H.G. Liddell, *A Greek-English lexicon with a revised supplement 1996*. 9th ed. Clarendon: Oxford. 1996. xlv, 320 p.
2. *An Introduction to Cryptography*. Network Associates, Inc. and its Affiliated Companies. 1990-1998. [cited 17 October 2009]; Available from: ftp://ftp.pgpi.org/pub/pgp/6.5/docs/english/IntroToCrypto.pdf.
3. *CERT Statistics (Historical)*. Carnegie Mellon University. 1995-2008. Updated 12th February 2009 [cited 17th October 2009]; Available from: http://www.cert.org/stats/.
4. W. Stallings, *Cryptography and network security : principles and practice*. 4th ed. Pearson/Prentice Hall: Upper Saddle River, N.J. 2006. xvi, 680 p.
5. B. Braden, et al., *Report of IAB Workshop on Security in the Internet Architecture February 8-10, 1994*, ed. B. Braden. RFC 1636. N.W. Group. Internet Architecture Board. 1994. [cited 17th October 2009]. Available from: http://www.faqs.org/ftp/rfc/pdf/rfc1636.txt.pdf.
6. *Internet World Stats Usage and Population Statistics, INTERNET USAGE STATISTICS The Internet Big Picture, World Internet Users and Population Stats*. Miniwatts Marketing Group. 2009. Updated 2009 [cited 17th October 2009]; Available from: http://www.internetworldstats.com/stats.htm.
7. J.J. Benz, *PGP: A Hybrid Solution*. SANS Institute InfoSec Reading Room. 2001. [cited 17th October 2009]. Available from: http://www.sans.org/reading_room/whitepapers/vpns/pgp_a_hybrid_solution_717.

8. *Corporate Overview*. PGP Corporation. [cited 17th October 2009]; Available from: http://www.pgp.com/about_pgp_corporation/corporate_overview/index.html.
9. *Encryption modes used in Crypto Systems' products*. Crypto Systems Incorporated. 2007. [cited 17th October 2009]; Available from: http://crypto-systems.com/modes.html.
10. E. Armstrong, et al. *The J2EE™ 1.4 Tutorial, For Sun Java System Application Server Platform Edition 8.2*. Sun Microsystems. 2005. Updated 7th December 2005 [cited 17th October 2009]; Available from: http://java.sun.com/j2ee/1.4/docs/tutorial/doc/J2EETutorial.pdf.
11. S.v. Otterloo, *A security analysis of Pretty Good Privacy*, Master's thesis, in *The Department of Information and Computing Sciences*, advised by M.d. Boer and G. Tels. Utrecht University: Utrecht. 2001.
12. R. Senderek. *The Protection of Your Secret Key, The Security of the Cryptographic Methods Used by PGP, The Public Key Cryptosystem RSA*. 2003. Updated October 2003 [cited 17th October 2009]; Available from: http://senderek.de/security/secret-key.protection.html.
13. *PGP Whole Disk Encryption, Proactively secure confidential data on disks and removable media, Overview*. PGP Corporation. [cited 17th October 2009]; Available from: http://www.pgp.com/products/wholediskencryption/.
14. *PGP Desktop Home*. PGP Corporation. [cited 17th October 2009]; Available from: http://eu.store.pgp.com/desktop_home.html.
15. T. Mobily. *Interview with Arturo "Buanzo" Busleiman, developer of Enigform*. 2007. [cited 17th October 2009]; Available from: http://www.freesoftwaremagazine.com/columns/interview_with_arturo_busleiman.
16. P. Zimmermann, *PGP source code and internals*. MIT Press: Cambridge, Mass. 1995. xxi, 907 p.
17. P. Zimmermann. *Letters to Phil from human rights groups*. (various dates). [cited 17th October 2009]; Available from: http://www.philzimmermann.com/EN/letters/index.html.