IK2206 – Internet Security and Privacy
GPG Lab

Getting started

•What is the fingerprint of the Course Key?
34C2 57EB 4DEA EA93 3D3E 13B0 BB24 3E2A 9DB3 07EA

•How long time did it take generate the keys?
Just a few seconds…

•Which cipher did you choose?
RSA

•How do you motivate the choice?
DSA would be more secure than RSA but can only be used to sign information but not to encrypt it. DSA is faster at signing while RSA is faster at verifying signatures. 0

•Which key-length did you choose?
2048bit

•How do you motivate the choice?
As by source 0, a 512bit RSA key can be broken with inexpensive hardware within months. It can be expected, that even 1024bit RSA keys can be broken within years (if high performance clusters are used). My 2048bit RSA key should provide enough security for the defined validity period of 3 months. A 4096 bit key would cost too much performance. (The longer the key, the more computational performance is used to encrypt/decrypt data).

•The identity you created for the key
gpg --edit-key 754E52A2

pub 2048R/754E52A2 created: 2011-11-07 expires: 2012-02-05 usage: SC
trust: ultimate validity: ultimate
sub 2048R/3AB4C316 created: 2011-11-07 expires: 2012-02-05 usage: E
[ultimate] (1). Thomas Galliker (IK2206) <galliker@kth.se>

•The fingerprint of the key
76B9 F669 9772 5DFC 8EE1 72A7 ADD4 8140 754E 52A2

Signed Data

•A table with your analysis of each part of the original message

Msg. No.	Analysis
1	This is obviously not a PGP-signed message. The message format of PGP-signed messages must conform following structure illustrated with Msg. #2.
2	This message has a “good signature”, which means that the message part fits to the given signature. Further we can find out who the signer resp. the originator of this message was. -----BEGIN PGP SIGNED MESSAGE----- Hash: SHA1 197794e5991f0aa0670b207a3ed5cd1d1b8fcaa1 -----BEGIN PGP SIGNATURE----- Version: GnuPG v2.0.9 (GNU/Linux) iEYEARECAAYFAk64GE8ACgkQuyQ+Kp2zB+p5NQCdHAPkjlgxM0N8loM6b7ti7Uqi Gv0Anj/lo+gooQf9WTS5cR6MQ67tbI5G =UPvn -----END PGP SIGNATURE-----
3	This message has a “good signature”. Refer to Msg. #2.
4	No valid signature available. Refer to Msg. #1.
5	This message has a “bad signature”. That basically means that the message and the given signature do not fit together. It can be assumed that the message was manipulated during the transmission. The signature is still intact since we can see from whom it originates. In case the signature is damaged, GnuPG would throw an exception like “the signature could not be verified”.
6	This message has a “bad signature”. Refer to Msg. #5.
7	This message has a “good signature”. Refer to Msg. #2.
8	This message has a “good signature”. Refer to Msg. #2.

•Which key do you use to sign the reply?

My private key is used to make signatures on data. The counterpart (the course system in this case), in turn, uses my public key to verify my signature.

•Output from GnuPG illustrating each type of incorrect message

Msg. No.	Output (gpg –verify)
1	gpg: verify signatures failed: Unexpected error
4	gpg: no valid OpenPGP data found. gpg: the signature could not be verified. Please remember that the signature file (.sig or .asc) should be the first file given on the command line.
5, 6	gpg: Signature made 11/07/11 18:41:35 W. Europe Standard Time using DSA key ID 9DB307EA gpg: BAD signature from "Internet Security and Privacy (IK2206) <gpg-both@netsec.xen.ssvl.kth.se>"

Encrypted data

•A table with your analysis of each part of the original message

Msg. No.	Analysis

1	This message does not comply with the message format of PGP-encrypted messages.
	`-----BEGIN PGP MESSAGE-----`
	`Version: GnuPG v2.0.9 (GNU/Linux)`
	
	`(Encrypted Message)`
	`-----END PGP MESSAGE-----`

2	The decryption failed because the message was encrypted with a public key to which I do not own the according private key. I'm simply not allowed to decrypt this message since I have no (private) key to do so.
3	This message was neither encrypted nor is its signature good. The command "`gpg --decrypt`" opens the contents of the message without using a key – this is a strong indication that no encryption was made.
4	No secret key available. See Msg. #2.
5	This message was not encrypted. In contrast to msg. #3 it has at least a good signature.
6	The exception "No valid OpenPGP data found" was thrown. That means basically that there must be something wrong with the data structure of the message. See Msg. #1.
7	This message was decrypted using key ID 3AB4C316. The content of the message is: 31619e89826d9b641c04ce4987a62f174462438b
8	The exception "No valid OpenPGP data found" was thrown. See Msg. #1.
9	This message was decrypted using key ID 3AB4C316. The content of the message is: 3ad2fbffa38db25e443d6544d75026b22904d5ed
10	This message was not encrypted. In contrast to msg. #3 it has at least a good signature.
11	No secret key available. See Msg. #2.

•Which key do you use to secure the reply?

To send encrypted data to a counterpart, the sender has to use the public key of the destined receiver.

•Output from GnuPG illustrating each type of incorrectly secured message

Msg. No.	Output (gpg –verify)
1	gpg: decrypt_message failed: Unexpected error
2	gpg: encrypted with 2048-bit ELG key, ID E617B75A, created 2011-10-26 "Internet Security and Privacy (IK2206) <gpg-both@netsec.xen.ssvl.kth.se>" gpg: decryption failed: No secret key
3	gpg: Signature made 11/07/11 18:41:35 W. Europe Standard Time using DSA key ID 9DB307E gpg: BAD signature from "Internet Security and Privacy (IK2206) <gpg-both@netsec.xen.s kth.se>"
4, 11	gpg: encrypted with ELG key, ID D38BBE06 gpg: decryption failed: No secret key
6, 8	gpg: no valid OpenPGP data found. gpg: decrypt_message failed: Unknown system error

Signed and Encrypted Data

•A table with your analysis of each part of the original message

Msg. No.	Enc.	Sig.	Analysis
1	-	-	This message does not comply with the message format of PGP-encrypted/-signed messages.
2	Yes	?	This message is encrypted, but I don't have a matching private key to decrypt it.
3	Yes	Yes	This message is encrypted and signed, but I can't check the signature since I don't have the appropriate public key to do so.
4	No	Yes	This message is only singed but not encrypted. The signature was good.
5	Yes	Yes	Everything's fine with this message: Decryption with key ID 3AB4C316 and good signature from key ID 9DB307EA.
6	No	Yes	This message was not encrypted but signed. The signature was bad.
7	Yes	Yes	Everything's fine with this message: Decryption with key ID 3AB4C316 and good signature from key ID 9DB307EA.

8	Yes	Yes	Everything's fine with this message: Decryption with key ID 3AB4C316 and good signature from key ID 9DB307EA. This message was encrypted with two different keys.
			`gpg: encrypted with 2048-bit ELG key, ID E617B75A, created 2011-10-26`
			`"Internet Security and Privacy (IK2206) <gpg-both@netsec.xen.ssvl.kth.se>"`

9	Yes	No	This message was encrypted but not singed.
10	Yes	Yes	Everything seems to be fine with this message: Decryption with key ID 3AB4C316 and good signature from key ID 9DB307EA. But there is a key involved from which we have no owner information: `gpg: encrypted with ELG key, ID D38BBE06`
11	-	-	This message does not comply with the message format of PGP-encrypted/-signed messages.
12	Yes	?	This message is encrypted, but I don't have a matching private key to decrypt it.
13	-	-	This message does not comply with the message format of PGP-encrypted/-signed messages.
14	Yes	Yes	Everything's fine with this message: Decryption with key ID 3AB4C316 and good signature from key ID 9DB307EA.
15	No	Yes	This message was not encrypted but signed. The signature was bad.
16	Yes	?	This message is encrypted, but there is no matching private key to decrypt it.

•Which key do you use to secure the reply?

My private key is used to sign the reply. The signed message is encrypted with the public key of the receiver (in this case with the public key of the course system).

•Output from GnuPG illustrating each type of incorrect message.

Msg. No.	Output (gpg –verify)
1	gpg: decrypt_message failed: Unexpected error
2, 12, 16	gpg: encrypted with 2048-bit ELG key, ID E617B75A, created 2011-10-26 "Internet Security and Privacy (IK2206) <gpg-both@netsec.xen.ssvl.kth.se>" gpg: decryption failed: No secret key
3	gpg: Signature made 11/07/11 18:41:36 W. Europe Standard Time using DSA key ID 6972F18 gpg: Can't check signature: No public key
6, 15	gpg: Signature made 11/07/11 18:41:36 W. Europe Standard Time using DSA key ID 9DB307EA gpg: BAD signature from "Internet Security and Privacy (IK2206) <gpg-both@netsec.xen.ssvl. kth.se>"
11, 13	gpg: no valid OpenPGP data found. gpg: decrypt_message failed: Unknown system error

Feedback

•References

[1] Which is better RSA or DSA public key?
http://www.linuxquestions.org/questions/linux-security-4/which-is-better-rsa-or-dsa-public-key-12593/
[2] 512bit RSA Key cracked,
http://www.mersenneforum.org/showthread.php?t=9787
[3] GPG Manual,
http://www.gnupg.org/gph/en/manual.html
[4] GPG Cheat List,
http://irtfweb.ifa.hawaii.edu/~lockhart/gpg/gpg-cs.html
[5] Christoph Moser,
He was involved in the trouble shooting process with the ambiguous ELG key problem. We further helped each other signing our PGP keys.

•Suggested improvements to the lab system

Please number the generated messages consecutively. Some people might not want to install the “awk” tool to split up the messages. In either cases it is easier to compare the message format of signed/encrypted messages.

•Suggested improvements to the lab instructions

There are some orthographical mistakes, e.g. “Import Pehr's public key, verify the fingerprint and give is an appropriate trust-level”. Just in case you care about that ☺

•Time estimation

12h