PGP for Smarties
Jan Schaumann <jschauma@etsy.com>

B60D A9F7 0D89 544A 7995
7D25 5A5B 4375 275F 0BB5

http://etsy.me/TF8k2c

Wednesday, September 5, 12
http://etsy.me/N1UIjg
Common threats to security:

IGNORANCE
Sometimes it's best not to know
PGP stands for...

http://etsy.me/SYTYfA
The Pacific Golden Plover (Pluvialis fulva) is a medium-sized plover.

http://etsy.me/SYTfYfA
Pretty Good Privacy

http://etsy.me/SYVdeP
Pretty Bad Privacy

http://etsy.me/hHFUdi
Definitions

“PGP” == “Pretty Good Privacy”
Definitions

“PGP” == “Pretty Good Privacy”

“OpenPGP” is a standard to provide encryption, decryption, signing, and key management functions. (RFC4880)
Definitions

“PGP” == “Pretty Good Privacy”

“OpenPGP” is a standard to provide encryption, decryption, signing, and key management functions. (RFC4880)

“GnuPG” == “GNU Privacy Guard” aka “gpg”
OpenPGP

• uses a combination of strong public-key and symmetric cryptography
• provides security services for electronic communications and data storage
  – authentication (via digital signatures)
  – confidentiality (via encryption)
  – integrity (via digital signatures)
  – key management
    – expiration
Buzzword Bingo
Buzzword Bingo

http://etsy.me/iFfqUa
Buzzword Bingo

http://etsy.me/iFfqUa

http://etsy.me/SZ1G9q
Buzzword Bingo

http://etsy.me/iFfqUa
http://etsy.me/SZ1G9q
http://etsy.me/N2OIIG
Buzzword Bingo
Buzzword Bingo

http://etsy.me/iFfqUa

http://etsy.me/SZ1G9q

http://etsy.me/TAHXKG

http://etsy.me/N20IIG

http://etsy.me/TAIEUh
Buzzword Bingo

http://etsy.me/iFfqUa

http://etsy.me/SZ1G9q

http://etsy.me/MHNUDQ

http://etsy.me/TAHXKG

http://etsy.me/N20IIG

http://etsy.me/TAIEUh
What's this, then?

B60D A9F7 0D89 544A 7995
7D25 5A5B 4375 275F 0BB5
What's this, then?

B60D A9F7 0D89 544A 7995
7D25 5A5B 4375 275F 0BB5

http://etsy.me/iFfqUa
In general:

• people who work together need to occasionally share secrets
In general:

• people who work together need to occasionally share secrets
• people who work together need to occasionally share secrets across physical distances
In general:

- people who work together need to occasionally share secrets
- people who work together need to occasionally share secrets across physical distances
- people who work together need to occasionally share secrets across physical distances and timezones
In general:

• people who work together need to occasionally share secrets
• people who work together need to occasionally share secrets across physical distances
• people who work together need to occasionally share secrets across physical distances and timezones
• people who work together don't always work together
In general:

• people who work together need to occasionally share secrets
• people who work together need to occasionally share secrets across physical distances
• people who work together need to occasionally share secrets across physical distances and timezones
• people who work together don't always work together

• people need to store secrets:
  • store it on a computer system owned by your company => multiple users besides you have full access
  • store it on a computer system owned by yourself => company-related information leaked
In general:

- people need to communicate securely

http://etsy.me/TAORQb
In general:

- people need to communicate securely

- people need to store date securely
Common threats to security:
Cryptography may provide:

- secrecy or confidentiality
- accuracy or integrity
- authenticity
Why we want secrecy:
Why we want integrity:

Date: Sat, 23 Jun 2012 11:59:40 –0400
From: Chad Dickerson <chad@etsy.com>
To: Jan Schaumann <jschauma@etsy.com>
Subject: Important
X–Mailer: iPad Mail (9B206)

Jan,

Can you disable Allspaw’s VPN access? We’ll have to let him go. Also, party at my place, byob.

Chad

Sent from my iPad
Why we want integrity:

Date: Sat, 23 Jun 2012 11:59:40 -0400
From: Chad Dickerson <chad@etsy.com>
To: Jan Schaumann <jschauma@etsy.com>
Subject: Important
X-Mailer: iPad Mail (9B206)

Jan,

Can you get Allspaw’s jacket size? We’re planning a surprise gift. Also, party at my place, byob.

Chad

Sent from my iPad
Why we want authenticity:

Date: Sat, 23 Jun 2012 11:59:40 -0400
From: Chad Dickerson <chad@etsy.com>
To: Jan Schaumann <jschauma@etsy.com>
Subject: Important
X-Mailer: iPad Mail (9B206)

Jan,

Can you disable Allspaw’s VPN access? We’ll have to let him go. Also, party at my place, byob.

Chad

Sent from my iPad
Symmetric- or private-key cryptography

http://etsy.me/TASe9N
Symmetric- or private-key

$ cat secret
Oehpr Fpuarvre rkcrpgf gur Fcnavfu Vadhvfvgvba.
$
Symmetric- or private-key

$ cat secret
Oehpr Fpuarvre rkcrpgf gur Fcnavfu Vadtvfvgvba.
$ rot13 <secret
Bruce Schneier expects the Spanish Inquisition.
$
Symmetric- or private-key

$ cat secret
Oehpr Fpuarvre rkcrpgf gur Fcnavfu Vadhvfvgvba.
$ rot13 <secret
Bruce Schneier expects the Spanish Inquisition.
$
Asymmetric- or public-key
Public-key cryptography in a nutshell

http://etsy.me/TAHXKG

http://etsy.me/SZ63kK

http://etsy.me/TARe5w

http://etsy.me/TAIEUh
Public-key cryptography in a nutshell

Hello Alice!

Encrypt

6EB69570
08E03CE4

Alice's public key

Hello Alice!

Decrypt

Alice's private key
Public-key cryptography in a nutshell

Alice

I will pay $500

Sign

DFCD3454
BBEA788A

Alice's private key

Bob

I will pay $500

Verify

Alice's public key
PGP can:

- provide secrecy or confidentiality (encryption)
- provide accuracy or integrity (checksum)
- provide authenticity (signature + WoT)
PGP can NOT:

• magically *imply* "security"

• know by *itself* whom to trust (or not)

• figure out *how* or *when* to share secrets

• protect you from *all* threats
Common threats to security:

- Brute-force solution: $O(n!)$
- Dynamic programming algorithms: $O(n^2 2^n)$
- Selling on eBay: $O(1)$

https://xkcd.com/399/
Common threats to security:

$ man gpg | rman -t ascii | egrep -- "^[ ]*--[^ ]+$" | \ 
  sort -u | wc -l 
  167

$
WORST. Interface. EVER.
Keypair generation

$ gpg --gen-key
[...]
Real name: Jan Schaumann
Email address: jschauma@etsy.com
[...]
You need a Passphrase to protect your secret key.
[...]
pub  2048R/275F0BB5 2012-04-24
    Key fingerprint = B60D A9F7 0D89 544A 7995  7D25 5A5B 4375 275F 0BB5
uid                  Jan Schaumann <jschauma@etsy.com>
[...]
$
Keypair generation

$ gpg --gen-key
[...]
Real name: Jan Schaumann
Email address: jschauma@etsy.com
[...]
You need a Passphrase to protect your secret key.
[...]
pub 2048R/275F0BB5 2012-04-24
   Key fingerprint = B60D A9F7 0D89 544A 7995 7D25 5A5B 4375 275F 0BB5
uid Jan Schaumann <jschauma@etsy.com>
[...]
$

$ ls ~/.gnupg/*ring.gpg
/Users/jschauma/.gnupg/pubring.gpg /Users/jschauma/.gnupg/secring.gpg
Common threats to security:

https://xkcd.com/538/
Revocation Certificate

$ gpg --output 275F0BB5-revocation-cert --gen-revoke 275F0BB5

sec 2048R/275F0BB5 2012-04-24 Jan Schaumann <jschauma@etsy.com>
[...]

You need a passphrase to unlock the secret key for user: "Jan Schaumann <jschauma@etsy.com>"
2048-bit RSA key, ID 275F0BB5, created 2012-04-24

ASCII armored output forced.
Revocation certificate created.

Please move it to a medium which you can hide away; if Mallory gets access to this certificate he can use it to make your key unusable. It is smart to print this certificate and store it away, just in case your media become unreadable. But have some caution: The print system of your machine might store the data and make it available to others!
Let's have a look...

$ gpg --fingerprint jschauma@etsy.com
pub 2048R/275F0BB5 2012-04-24
    Key fingerprint = B60D A9F7 0D89 544A 7995 7D25 5A5B 4375 275F 0BB5
uid Jan Schaumann <jschauma@etsy.com>
sub 2048R/FA19BA98 2012-04-24
$
Let's have a look...

$ gpg --fingerprint jschauma@etsy.com
pub 2048R/275F0BB5 2012-04-24
    Key fingerprint = B60D A9F7 0D89 544A 7995 7D25 5A5B 4375 275F 0BB5
uid Jan Schaumann <jschauma@etsy.com>
sub 2048R/FA19BA98 2012-04-24
$

$ gpg --export -a 275F0BB5
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v2.0.18 (Darwin)

mQENBE+W6hcBCADcP2qrc4tjVjJxvyCNPJZSxDmDLqWzo9KDEer77WeAocYuX
 [...] 
bWxBdIK299dw4wRJi1Z20cg/VIztflDF54ts55EDsQ==
=QJIN
-----END PGP PUBLIC KEY BLOCK-----
Wot a lot I got!
Wot a lot I got!

http://etsy.me/iFfqUa
Wot a lot I got!

http://etsy.me/iFfqUa

http://etsy.me/TARe5w
Wot a lot I got!

http://etsy.me/TARe5w

http://etsy.me/iFfqUa

http://etsy.me/TASWnp
Sharing secrets with Alice

$ gpg --encrypt -r alice@etsy.com secret
gpg: alice@etsy.com: skipped: public key not found

gpg: secret: encryption failed: public key not found
$
Public-key cryptography in a nutshell

Hello Alice! → Encrypt → Alice's public key → 6EB69570 08E03CE4

Alice's private key → Decrypt → Hello Alice!
Sharing secrets with Alice

$ gpg --encrypt -r alice@etsy.com secret
gpg: alice@etsy.com: skipped: public key not found
gpg: secret: encryption failed: public key not found
$

$ gpg --list-keys alice
gpg: error reading key: public key not found
$

Wednesday, September 5, 12
Sharing secrets with Alice

$ gpg --encrypt -r alice@etsy.com secret
  gpg: alice@etsy.com: skipped: public key not found
  gpg: secret: encryption failed: public key not found
$

$ gpg --list-keys alice
  gpg: error reading key: public key not found
$

$ gpg --search-keys alice@etsy.com
  gpg: searching for "alice@etsy.com" from hkp server keys.gnupg.net
  gpg: key "alice@etsy.com" not found on keyserver
$
Sharing secrets with Alice

$ gpg --search-keys alice

gpg: searching for "alice" from hkp server keys.gnupg.net
(1) Alice Cooper <alice@etsy.com>

2048 bit RSA key AB123456, created: 2009-11-25

Keys 1-1 of 1 for "alice". Enter number(s), N)ext, or Q)uit > 1

$ gpg: requesting key AB123456 from hkp server keys.gnupg.net

gpg: key AB123456: public key "Alice Cooper" <alice@etsy.com>"

imported

$ gpg: Total number processed: 1

$ gpg: imported: 1

$
Sharing secrets with Alice

$ gpg --encrypt -r alice@etsy.com secret
gpg: AB123456: There is no assurance this key belongs to the named user

pub 2048g/AB123456 1969-08-01 Vincent Damon Furnier <alice@etsy.com>
Primary key fingerprint: 666C E666 CC66 6EB6 66DB B0B6 6678 6667 AB12 3456

It is NOT certain that the key belongs to the person named in the user ID. If you *really* know what you are doing, you may answer the next question with yes.

Use this key anyway? (y/N)
Common threats to security:
Keypair generation

$ gpg --gen-key
[...]
Real name: Chad Dickerson
Email address: chad@etsy.com
Comment: CEO
You selected this USER-ID:
 "Chad Dickerson (CEO) <chad@etsy.com>"
[...]
You need a Passphrase to protect your secret key.
[...]
pub  2048R/E157FAB8 2006-09-01
    Key fingerprint = E2A7 437A 7AB8 6EA1 7E1D  F6DC BF09 CDC9 E157 FAB8
uid                  Chad Dickerson (CEO) <chad@etsy.com>
[...]
$ gpg --send-keys E157FAB8

gpg: sending key E157FAB8 to hkp server keys.gnupg.net
$
Key Verification

- easily done in person
- easiest done if both parties actually know each other
- reasonable authentication (for some organizations, anyway - mix and match):
  - Staff Directory info
  - IRC handle
  - shared domain username
  - email
Key Verification

http://etsy.me/SZ9AQc
Web of Trust
Andy Dick

(In the Army now)

Donald Sutherland

John Belushi

Pauly Shore

(In the Army now)

Kevin Bacon
Donald Sutherland

John Belushi

Andy Dick

Kevin Bacon
(Footloose)

Claudia Schiffer

Pauly Shore

Sarah Jessica Parker
(Footloose)
Problems with the Web of Trust
Better:
Web of Trust

- you have to trust every signing entity in your trustpath
- the shorter the trustpath, the better
- the more nodes in your WoT, the better
- the more edges in your WoT, the better
- the fewer leaves, the better
- the more signatures a key has, the better
Key Verification

• becomes “Key Signing”

• makes no assertion of quality of character, coding skills, weight-lifting abilities, taste in movies, etc

• only asserts “I have verified that the key with the fingerprint X belongs to person Y”

• nothing else
Key Signing

- retrieve signee’s key
- identify signee
- signee presents or confirms his/her key’s fingerprint
- signer sends encrypted content to email on key
- signee decrypts, responds
- signer signs and uploads signee’s key
Long-Distance Key Signing

- same as before modulo:
- identify signee
  - by trusted proxy (ie via WoT)
  - call phone-# (desk + cell) listed in Staff Directory
  - multi-channel challenge response (Skype+IRC +Email)
- control of uid on shared host
Please sign responsibly!

https://www.xkcd.com/364/
Wishlist

• key generation part of new-hire orientation
  • manager signs new-hire key on first day
  • team signs new-hire key on first team meeting
• regular keysigning events
• sensitive/important data is actually signed
• encrypted backups (+ self-restore)
• signed packages
• ...

Wednesday, September 5, 12
Be paranoid!
Links

• http://www.mycrypto.net/encryption/encryption_public.html
• http://en.wikipedia.org/wiki/Public-key_cryptography
• http://en.wikipedia.org/wiki/Pretty_Good_Privacy
• http://www.lysator.liu.se/~jc/wotsap/search.html

• http://oracleofbacon.org/