Cryptography and Privacy

Contents

Note: This was originally written in the beginning of 2008, and not updated since. I now do not believe this text to be particularly useful. You should probably directly look at the References (section 5).

1 Introduction

This page is yet another attempt at explaining what cryptography is, and why it is useful. A lot of pages like this already exist (see References (section 5)), but it seems to me adding more noise can help.

2 What is cryptography ?

From the Wikipedia article[1]:

> Cryptography is the practice and study of hiding information. Modern cryptography intersects the disciplines of mathematics, computer science, and engineering.

[1] `http://en.wikipedia.org/wiki/Cryptography`

Hiding information (i.e encryption) is one well-kown goal of cryptography, but *authentication* via digital signatures[2] is another which is at least as important: what is the use of sending encrypted information if you are not sure you are sending it to the right person ?

You use cryptography when you login into your e-banking site, or when you give out your credit card number to a shopping website. This prevents e.g your credit card number from being read while it is being sent.

Of course, SSH[3] also uses cryptography to avoid password snooping and other attacks. A lot of software, free or non-free have built-in crypto capabilities.

3 Why is it useful ?

Cryptography is useful to communicate securely over an insecure channel such as the Internet. In short: if A and B are communicating using secure cryptography protocols, they are sure they are communicating with the right person, and nobody can understand what they are saying.

Some people are skeptical on the practical use of such an accomplishment . Below are some of the most common reactions.

3.1 Encryption is only for the military

Of course not: several civilian applications have already been given above. The army is not the only one to need privacy: businesses have secrets, and so have people. When those secrets need to be transmitted over an insecure channel like the internet, encryption is needed.

3.2 Encryption is used by criminals

Of course it is, so what ? Criminals also use cars and credit cards to commit crimes, and we use those too ! Just because criminals use `x` doesn't mean `x` should be banned. Here is an interesting quote:

> Crime? If you are not a politician, research scientist, investor, CEO, lawyer, celebrity, libertarian in a repressive society, investor, or person having too much fun, and you do not send e-mail about your private sex life, financial/political/legal/scientific plans, or gossip then maybe you don't need PGP, but at least realize that privacy has nothing to do with crime and is in fact what keeps the world from falling apart. Besides, PGP is FUN. You never had a secret decoder ring? Boo!
>
> —Xenon `<an48138 at anon.penet.fi>` (Copyright 1993, Xenon)

3.3 But I have nothing to hide !

That's the most common argument. The first answer to that is: even if you have nothing to hide, you still need to use crypto *for authentication*. It is trivial, for example, for someone to send an email as you[4]. Digital signatures can solve that problem.

[2] `http://en.wikipedia.org/wiki/Digital_signature`
[3] `http://www.openssh.org/`
[4] `http://en.wikipedia.org/wiki/E-mail_spoofing`

The second answer is that even if you haven't done anything illegal, you have something to hide: would you allow somebody to sit just behind you and look at you computer screen all day ? Privacy is a basic right, and that's what encryption protects.

Once it is granted that you sometimes send something you do not want people to know, it makes sense to use encryption for everything: if you only encrypt what you want to hide, people will know you are sending sensitive content and might try hard to break it or prevent you from using encryption. On the other hand, if you encrypt everything, nobody can know when or if you are sending sensitive content.

Phil Zimmermann, the author of PGP[5], says all this much better than me in Why I wrote PGP[6]

3.4 Nobody reads / cares about the data anyway

Maybe so, but then would you be willing to just write it on your webpage, or send it on a postcard ?

What's more, we are not only talking about humans: fully automated systems intercepting communications and looking for keywords already exist: and even if nothing is found, they will be archived for further review.

In short, you never know who might be listening: using crypto is a small price to pay to make sure your communications are really private

4 The Web of Trust

Once you have accepted that you should use cryptography, everything isn't solved magically: encryption is relatively easy to achieve, but to achieve authentication, one needs trust. What follows is a simplified picture of what is needed, and different ways of achieving it. If you want to go into the technical details, you can start with Wikipedia's article on key authentication[7].

Basically, if you are A and you want to make sure that B is really who he claims he is, then you need to trust someone who trusts someone who trusts someone... Who knows B and can certify he really is who he claims to be !

There are several ways to achieve this: the system that is very popular on the web today is centralized: you pay money to some big trusted companies so that they can tell others that you are who you claim to be. The flaw in this system is obvious: you have to trust the big companies !

Another popular system is the web of trust, implemented by GPG[8]. Basically, you manually verify the identity of some people (for example, you meet them in real life), which you can then trust. If your network of trust is large enough, you may be able to find someone you trust who knows someone he trust who knows someone... Who trusts B.

Of course, this is oversimplified: trust is not completely transitive: if I trust B and B trusts C, I may not completely trust C. The longer the chain, the lower the trust. That's why GPG for example imposes a maximal chain length.

Since this web of trust system seemed to be a better idea than the centralized one actually working on the web, I decided to try to actively use GPG for my communications.

[5] http://en.wikipedia.org/wiki/Pretty_Good_Privacy

[6] http://www.philzimmermann.com/EN/essays/WhyIWrotePGP.html

[7] http://en.wikipedia.org/wiki/Key_authentication

[8] http://www.gnupg.org/

4.1 How I use GPG

4.1.1 Release signing

As you might have remarked, I sign all software releases on `svasey.org` with my GPG key[9]. Be aware if you find an unsigned tarball on my site: I did not package it ! (Or maybe I just forgot to upload the signature...). Please report it to me[10].

Signing a release tarball is useful to prevent them from being modified in transit: an attacker could replace it with malware, and the poor user would install it, as he would believe to be installing some innocent `svasey.org` software :-) . Problems could also arise if my web server is compromised: again, the attacker could replace the tarballs with malware.

4.1.2 Email signing

I sign all my outgoing emails. If you receive unsigned email, it did not come from me !

4.1.3 Email encryption

Unfortunately, not everybody I send mail to has a GPG key. However, I systematically encrypt all my outgoing mails to people in my web of trust. If someone else has a GPG key and asks me to send information encrypted, I will do it: it cannot lessen security !

4.1.4 TLS

If you want, you can use TLS[11] to communicate with all my websites. My certificate is signed using GPG. See the svasey.org TLS documentation[12] for more.

5 References

- The comp.security.pgp FAQ[13] is a good starting point to learn about PGP
- André Bacard's "Non-Technical PGP FAQ"[14] answers the "I have nothing to hide" and other arguments against crypto.
- Why I wrote PGP[15] is an outstanding essay by the author of PGP

[9] `http://certs.svasey.org/gpg-svasey-pubkey.asc`
[10] `http://svasey.org/about_en.html#contact-information`
[11] `http://en.wikipedia.org/wiki/Transport_Layer_Security`
[12] `http://svasey.org/tls-user_en.html`
[13] `http://www.cam.ac.uk.pgp.net/pgpnet/pgp-faq/`
[14] `http://www.andrebacard.com/pgp.html`
[15] `http://www.philzimmermann.com/EN/essays/WhyIWrotePGP.html`