Piracy, Privacy and Thought Control

Jaromil's Journal of Musings

December 23, 2009

0.1 Piracy, Privacy and Thought Control

This lecture focuses on the progressive intrusion of anti-piracy campaigns into the privacy of citizens worldwide, the threat to civil rights represented by IPRED2 and an appeal to enforce cryptographic encryption in commonly used operating systems. It was briefly held the first time on 7 September 2007 at the Ars Electronica Symposium GOODBYE PRIVACY[1]

Why privacy?

Let's first refresh our memory about the importance of privacy, so often neglected in contemporary societies based on fear:

> The distinction between what is public and what is private is becoming more and more blurred with the increasing intrusiveness of the media and advances in electronic technology. While this distinction is always the outcome of continuous cultural negotiation, it continues to be critical, for where nothing is private, democracy becomes impossible.
>
> `http://www.newschool.edu/centers/socres/privacy/Home.html`

This was stated 1 year before the 9/11 escatological brainwash.

Why piracy?

An important account is given by professor Doron Ben-Altar in his book *Trade Secrets: Intellectual Piracy and the Origins of American Industrial Power*:

> During the first decades of America's existence as a nation, private citizens, voluntary associations, and government officials encouraged the smuggling of European inventions and artisans to the New World. These actions openly violated the intellectual property regimes of European nations. [...] What fueled 19th century American boom was a dual system of principled commitment to an intellectual property regime combined with absence of commitment to enforce these laws. This ambiguous order generated innovation by promising patent monopolies. At the same time, by declining to crack down on technology pirates, it allowed for rapid dissemination of innovation that made American products better and cheaper.

Current "intellectual property" monopoly

Armin Medosh writes in his *Piratology* essay:

> Piracy does not simply exist because there are bloody-minded people who don't care for the rules and laws of the civilised world. It tends to emerge whenever there is a hegemonic power that asserts itself by establishing a trade monopoly. A monopoly, by its very nature, cuts out competition by other traders and destroys existing means of trade. People deprived of their traditional way of making a living resort to criminal activity. The hegemonic power, itself not averse to using violence to force others into submission, considers itself to be the law and defines others' activity as piracy.

[1] http://thenextlayer.org/GoodbyePrivacy

In the market of digital devices since a few decades now, business corporations are betraying free market laws when confronted with the dynamic nature of digital developments. **A few major holdings build restricted mobile objects sold worldwide**: software development and distribution to the masses is accessible only for their business partners, while users are granted the only right to choose among pre-designed mobile phones and gadgets. **Such mobile communication devices constitute nowadays the widest network around the globe, mostly used by citizens for private communications**.

Still, the laws of free-trade dictate that when you exchange money for the purchase of any item, that item belongs to you without strings attached.

But these mobile devices are not in complete control of their legitimate owners: it is not clear what the software running on them is doing and, with the rise of "trusted computing" technologies, **the possibility to run homebrew applications is denied**.

The mobile communication market is not open and doesn't even allows real competition, while being related to cultural, political and social developments worldwide. Such a monopoly enforces a form of **colonialism for information technology: there is no possibility for local artisans to interact independently with the architectures**, intervene on communication infrastructures, adapt them to their own needs and create small scale bazaars in which such modifications can be sold or shared with others.

Pirate peasants

A vivid picture is traced by this Chinese movie about piracy, directed by He Jianjun and produced by the Rotterdam Film Festival. Here is a video excerpt available for download:

`http://www.bricolabs.net/downloads/bricolabs/pirate_copy_excerpt.avi`

Out of the fiction, back to this world, **Tony Onouha** died in august 2007 trying to escape undercover cops chasing him for selling copied DVDs in an internet cafe in Athens.

> Update: a first signal of the emerging sensibility on this topic is given by the campaign I Wouldn't Steal[2] launched in 2008 by the European Green Party.

Intellectual Property Rights Enforcement Directive 2

Contemporary societies are getting more and more strict in enforcing the aforementioned intellectual property regimes, as it is clearly outlined in the IPRED2, the second "Intellectual Property Rights" Enforcement Directive proposed on July 12, 2005 by the Commission of the European Communities.

Such enforcement moves towards the "privatisation of justice" delivering to copyright holdings a direct role in investigations for copyright violations: informations about citizens can be collected and used by private corporations, threated in marketing surveys and other uses not even explicitly authorized.

> Following the IPRED2, informations about citizens can be collected and used by private corporations in marketing surveys even without explicit authorization of the subjects, in contrast with the article 8 of the EU convention on human rights (*excerpt translated from the Italian analysis by Giuseppe Corasaniti)*

While the governments drop their role in justice enforcement, facing the fact that information infrastructures are ruled by global corporations, "community oriented" technologies rapidly develop on the trend of the "Web 2.0" collecting huge amounts of private data about citizens worldwide.

Urgency

Helen Nissenbaum suggests the importance of Privacy as Contextual Integrity[3], an important concept to understand the present urgency.

Imagine:

- jailed bloggers in Cairo

[2] http://www.iwouldntsteal.net

[3] http://crypto.stanford.edu/portia/papers/RevnissenbaumDTP31.pdf

- investigative journalist in Palermo
- self determined women in patriarcal environments
- native communities in Oaxaca
- citizens demonstrating at the G8

> Building autonomous networks in extreme conditions is exposing nodes to a risk that is directly proportional to the size of the network.

The internet offers plenty of free services, on the wave of the Web2.0 fuzz and the online community boom, information exchange grows proportionally to the possibility to monitor, while intercepted private data is treated as a marketable good. Almost all civil societies private informations are hosted on servers owned by global corporations and commercial monopolies.

> The risk grows higher as more digital communication systems pervade societies with centralised architectures. On 2 February 2008 the first death sentence for Internet censorship[4] was filed against a journalism student in Afghanistan by a Sharia court for downloading and sharing a report criticizing the treatment of women in some Islamic countries.

Proposed solutions

It is important to keep in mind that noone else than *you* can ensure the privacy of your personal data. Server hosted services and web integrated technologies gather all data into huge information pools that are made available to established economical and cultural regimes.

Information technology architects can help:

- build peer to peer communication architectures
- leave private individuals store their own data
- build autonomous, intuitive and embedded security systems
- in extreme cases, scale security from personal to collaborative

An attempt: dyne:II - a GNU/Linux liveCD

This easy to employ software operating system is designed with some distinctive features:

- Nomadic architecture that can run on found computers
- Mobile personal data storage system on USB key
- Fairly strong encryption: AES/Rijndael hashed SHA/256
- Easy and intuitive, no extra operations required
- All your home directory stays in an encrypted file
- Operations are done *live* on the file during usage

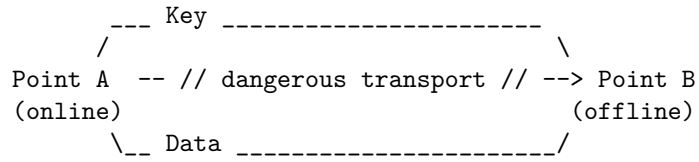
... more on `http://dynebolic.org`

[4] http://yro.slashdot.org/article.pl?sid=08/02/02/1915253

A simple but effective encryption scheme

- Data <—your private data (in a physical file)
- Key <—the key to your data (in another physical file)
- Password <—the password unlocking the key (to be remembered)

Data + (Key + Password)



Only when Key and Data meet again the informations can be accessed, if one of them is missing data is stored scrambled with AES/SHA256.

Password can be communicated (also over unsafe channels) once Key and Data meet again.

Another effective method: TrueCrypt

The TrueCrypt[5] project offers free open-source disk encryption software for Windows Vista/XP/2000 and Linux, its main features are resumed:

- Creates a virtual encrypted disk within a file and mounts it as a real disk.
- Encrypts an entire hard disk partition or a storage device such as USB flash drive.
- Encryption is automatic, real-time (on-the-fly) and transparent[6].
- Provides two levels of plausible deniability[7], in case an adversary forces you to reveal the password:
  - Hidden volume[8] (steganography - more information may be found here).
  - No TrueCrypt volume can be identified (volumes cannot be distinguished from random data).
- Encryption algorithms[9]: AES-256, Serpent, and Twofish. Mode of operation: LRW[10].

  Further information regarding features of the software may be found in the TrueCrypt documentation[11].

Salaam/Shalom/Shanthi/Dorood/Peace

Thanks to: Freaknet.org[12], Servus.at[13] and Quintessenz[14]

A thousand flowers will blossom!

---

[5] http://truecrypt.org
[6] http://www.truecrypt.org/docs/
[7] http://www.truecrypt.org/docs/?s=plausible-deniability
[8] http://www.truecrypt.org/hiddenvolume.php
[9] http://www.truecrypt.org/docs/?s=encryption-algorithms
[10] http://www.truecrypt.org/docs/?s=modes-of-operation
[11] http://www.truecrypt.org/docs/
[12] http://freaknet.org
[13] http://servus.at
[14] http://quintessenz.at