



## Passwords and PKI – how secure are they?

The current wisdom tends to be that passwords are bad (they can be shared, cracked, captured, get written down) but PKI is good (difficult to crack, makes things secret, difficult to forge).

And there's a lot of truth in the analysis. Short passwords are not a good idea. The shorter it is the more likely it can be guessed or cracked through a dictionary type attack. PKI is a bit like using a humungous length password (32 characters) by comparison.

But the biggest weakness of all is being able to give them away.

Infosecurity 2003 showed in a quick morning's series of interviews that people were quite happy to disclose their password on the platform of London's Waterloo Railway Station. For a plastic pen! So never argue that using a password is secure (unless you believe the fig leaf technique<sup>1</sup> works).

But those supporting PKI presume that the user will not, or cannot give away the PKI credentials (the private and public keys) used to support the system. Is this right? Well I have watched people hand their ATM cards to others, tell them the pin and ask them to get some cash. So that is not a problem? And that is with people who are law abiding. The real problems start when they are not.

If I have a fake ID then I can get fake credentials, use a stolen credit card to pay, and bingo – a PKI ID I can give to any number of others simply because I don't care, and nor do they. Right now there is trade in fake ID cards – why not PKI identities. And the stock answer is that you must administer the PKI properly.

Well, administering PKI is not actually all that easy. In June 2011 the Dutch PKI Company DigiNotar B.V. was hacked and later issued PKI certificates that were false. And these were not for Joe Blow or similar, but for Domains like Google, Skype, Mozilla, Microsoft and so on. The hackers that obtained these could 'appear' to be those organizations, create other keys and so on. And all that without breaking the cryptography.

And that is only one aspect of the procedural problems. Best to avoid them.

LockLizard does use PKI technology to identify users, but does not issue credentials directly to users. They are hidden in encrypted wallets that cannot be transferred to others. So the two largest weaknesses of passwords and PKI are avoided. There are no passwords to give away, and credentials cannot be copied and given away. Trying to create fake customer records is rather difficult because you have to break several system components, not just the offline one.

So passwords/install codes are a bad idea, and PKI, used with some care, is much better.

---

<sup>1</sup> First documented use in the Garden of Eden was a cover up.



## About LockLizard

LockLizard is a DRM (digital rights management) company that specializes in document security and copy protection for PDF, flash, ebooks, elearning, software, and web based content. We protect information with US Government strength encryption and rights management controls to ensure complete protection against copyright piracy. Use our DRM software to control document use - stop copying, prevent printing, disable print screen, expire content, instantly revoke access to information, and track document usage (views and prints). <http://www.locklizard.com>