http://www.coincoin.fr.eu.org/?Web-of-trust-is-a-security-failure

'Web of trust' is a security failure

- 6- Webographie -

Date de mise en ligne : mercredi 14 septembre 2011

'Web of trust' is a security failure

Here is a simple yet unpleasant thing (one that I have circled around and implied before, but never stated outright) :

Any time you propose a security system that uses a 'web of trust' model to validate anything, you've failed ; the system is not secure in practice. You can demonstrate all of the math that you want, but in the end it comes down to **the users must pick the right people to trust in order for the system to be secure**. And they will not. This is not a theoretical 'they won't', it is an experimentally and historically proven 'they will not', because they never have before now.

(Some number of them will try their best but not know enough. Some number of them will pick randomly. Some number of them will make mistakes. And if the system is attacked, some number of them will be fooled.)

When you propose a web of trust system, what you have really done is abrogated the work of making the system secure and instead dumped it on the users. This is a great way to feel morally superior (after all, the system works perfectly if used right so it's clearly the user's fault for screwing it up), but it is very much not a useful way to design an actual security system. You have not solved the real problem and you are ducking the issue.

(Attestation is a handy idea, but it does not need to be handled in the system in order to be useful ; in real life, people already use all sorts of out of band mechanisms to handle it.)

Another way of putting this is that a web of trust system is not actually a secure system out of the box ; it is not secure by itself, and indeed it's often not operable by itself. Instead, it's just most of the components of a secure system and assembling the actual secure system is left as an exercise for the users. Claiming that the pre-assembled component is 'secure' is vacuous, because it is not yet a complete and operable system.

This is a specific instance of the general issue that asking users questions never increases security (in part because (most) users don't care about security). And yes, 'who do you trust ?' is clearly a question.

Web of trust also has a number of practical low level problems that I've written about in WebOfTrustFlaws (especially when used as a replacement for SSL CAs).

Sidebar : web of trust as an implementation detail

The one time that a 'web of trust' system is acceptable is if the users don't have to answer any questions in order to use it securely, ie they are not required to pick their own set of trust roots. Instead, the system is designed to work with a preconfigured, pre-vetted list and then the designer takes responsibility for keeping that list good.

(The system will need a way to update the list, for obvious reasons.)

Cet article est repris du site http://utcc.utoronto.ca/~cks/space/...