Unravelling the Web of Trust

PGP's Web of Trust was a grand idea of the early 1990s. Sadly, it didn't work. Understanding why it didn't work is essential for moving forward. Let me illustrate some issues by means of anecdotes.

First, what is the Web of Trust? At its most basic, an individual would sign over the key of another, creating a link or line to that person. Then, this link as a signature over other's key would be shared with other people, typically via a keyserver. Thirdly, the aggregate of all those links would create a web showing how the people interconnected. It was presumed in some vague sense that more lines to a person (key) would mean more trust.

One Example - PGP

To me at least, the first sign of trouble was when a person wanting their key signed thrust a passport at me. I rebelled and said put that away - but it laid a seed of doubt for the next sign of trouble. At one of the frequent Fosdem meets, I saw 2 lines of people, facing in parallel, show their passports to each other, and their keyid. Once each showing was done, the lines shuffled so that new couples could do the same.

What was going on here was two entirely contrasting, competing, and indeed excluding viewpoints. One side believed that trust related to the other person naming themselves as Jane Smith or as it was; whereas the other side believed that trust derived from the other person proving their name via state-issued documentation. One side believed trust included allowing the other person to pick their name, the other side believed trust derived from banning the person from picking their name.

They couldn't both be right - but they could both be in the same web of trust, PGP style.

Second - PKI

To understand why this conundrum existed, let's turn to the world of browsing X509 PKI. In that more sterilised key signing world, a certification authority (CA) would issue a certificate stating that a name in a certificate was correct, more or less. PKI sided with one of the views from PGP as above, and against the other, but went further: not only did they side with one view, they documented that view in great depth in a thing called a certificate practice statement (CPS) which little document ballooned over time to a certificate-industrial-complex of dozens of documents, audits, costs, cartels and dodgy consumer practices.

The point being that PKI documented its view of what 'trust' was, which I think is a fair statement because it called itself *the trust business*. Whereas PGP's WoT never did so, allowing the emergence of contradictions at the very level of trust.

PGP's WoT never worked (in part?) because it didn't document the trust part of the web.

But, although it took this crucial step forward to document, PKI didn't really work either as what it documented was not really trust. Purchasers of certificates were forced to do so, else face software that didn't work. Or worse, have software lie to users about how the site is 'untrusted' with the wrong certificate but was perfectly 'trusted' with no certificate at all. There wasn't a lot of trust at site side, but there was a lot of hate when certs expired. Users were continually confused, and eventually browsers hid the certificates from them - so users certainly couldn't trust what they couldn't see. In the sense of trust, PKI failed because although it documented itself, it missed the target.

3rd - CAcert

It would take many more pages to explain why PKI never found trust (2008a). But one CA showed how to do trust, and that was CAcert (2008b). Trust abounded because this was an open community CA, and people just wanted to participate - they wanted to join, to get their keys signed, and eventually to become assurers and sign others' keys.

But trust didn't take concrete form until an audit was imposed over it by one of the browsers (I was the auditor), and that audit forced through a number of changes to lift the game: training and testing for assurers, documentation for all the processes, arbitration to correct errors, mass testing over the organisation, etc. Although CAcert struggled to make a mark in the world, a sense of trust over the assurers arose. We could trust the assurers to do the right thing! And, we could even trust the assurers to do other things, other than just their direct job.

But this was a very different situation - we as Assurers trusted other Assurers, and it became a badge of honour to get to that level. It wasn't so much that the organisation was trusted, and indeed its 'trust' level in the browsers went down as the trust internally went up. It was more that we trusted each other in a community, because of what we had done. Obscurely, to figure out if someone could be trusted, we just asked.

And note that this trust was not translated into certificates or signed PGP keys. For some reason that seemed odd, could we have even done that? It was out of this that the realisation grew that a certificate could not carry 'trust' per se - it could carry a badge like the word 'Assurer' but that was meaningless without a whole lot of context. The cert didn't carry the context, because it was human and interactive! If we got the context by asking, we didn't need the certificate, and if we had the certificate, we'd still ask for the context.

Hence, CAcert also failed to deliver a *Web of Trust*, in the technical terms of PKI envisaged earlier, because trust turned out to be a human to human quality with deep context; it didn't trivially or easily go into a certificate or into a web.

The Ask!

Can trust be digitised, put into a certificate, or a web? What is trust anyway? Is this just a conversation where we all have different ideas, or has nobody actually sat down and developed an agreeable theory of trust? If we had a definition, what could we do with it? Touch it? Measure it? Share it? Break it?

To proceed: (a) what are your anecdotes that reveal *to you* something about trust? (b) can we isolate some principles from the sum of anecdotes? And (c) can we define trust?

References

2008a, Ian Grigg, "PKI Considered Harmful," https://iang.org/ssl/pki_considered_harmful.html

2008b, Ian Grigg, "An Open Audit of an Open Certification Authority," 22nd Large Installation Systems Administration Conference (LISA 2008) 13th November 2008, https://iang.org/papers/open_audit_lisa.html