How to renew Trust in the Internet

Michael Scott

Chief Cryptographer
MIRACL Labs
mike.scott@miracl.com

Abstract. Trust in the Internet is at an all time low. Its time for action.

1 In the beginning..

We all make multiple trust assumptions every day. And in truth most of them are justified and we are rarely disappointed. Indeed it would be hard to imagine a more difficult environment than one in which most of our trust assumptions proved false.

Maybe in the Garden of Eden we all originally trusted one another. If so we were quickly disabused. Betrayal was just around the corner.

But when trust does break down it tends to be an isolated thing, and our other trust assumptions remain valid. So I may discover that my wife is having an affair, but friends and family will remain true, we patch up and adjust our trust parameters, and life goes on. We might cry "I will never trust anyone ever again", but we don't mean it, and we will, because life without trust is unimaginable.

In the past trust was greatly enhanced by its face-to-face nature. I trusted the banks a lot more when I had a friendly local bank manager to talk to. Since banking became faceless, trust has suffered. And from the other side it is easier to betray some-one you have never met. To maintain trust remotely is a big ask. So just when we thought we had the trust thing nailed down...

2 ... along came the Internet...

An optimal resolution to the problem of trust in the Internet was never going to be easy. By its very nature internet-based relationships are more challenging. But since we now reveal so much about ourselves on-line our privacy (and our financial well-being) are at serious risk. We do have the amazing potential to build useful relationships all over the planet, but we need a way to instil trust into those relationships if the Internet is to flourish.

It would appear that the Internet was designed by people with a "Garden of Eden" world view. The possibility of betrayal of trust seems to have come to them as a complete surprise. Email was invented and implemented before Spam was even considered as a possibility. It appears that inventors, often being idealists, do not factor in the darker side of human nature.

However a driver in the early days was certainly an idealistic belief in egalitarian values. I am sure the early pioneers envisaged an Internet of equals, and where power would not aggregate to a small number of powerful entities. In a similar vein I would think that they would have liked the problems around trust, once identified, to be resolved in a fashion compatible with those values.

From the earliest days one of the building blocks of trust and security on the Internet was cryptography. Unfortunately with the technology then available, the only solution was the highly centralised concept of PKI the Public Key Infrastructure. The PKI system supports SSL, which in turn underpins e-commerce. By design this involves a central root of trust which typically manifests as a single RSA private key. If this is revealed the whole thing unravels. This entity - the Certificate Authority or CA – that controls the root of trust, holds a disproportionate amount of power, which does not fit comfortably with the original ethos of the Internet.

Because the trust issue was not dealt with properly from the start, the Internet faces an uncertain future. Currently trust in the Internet is at an all time low. An Internet of Things will be a disaster unless we fix this. Part of the problem was the lack of vision to see that these shortcomings were not inevitable.

Some of the potential applications of the Internet have already been stymied by unresolved trust issues. E-Voting has stalled. E-Commerce is under threat. Migration to the cloud is stuttering. And E-Currencies seemed to be going nowhere...

3 ... then, out of the blue, along came the block-chain! ...

Banking is a great test-bed for the consideration of trust issues. The costs of (and rewards for) betrayal are high, and hence the need to evolve strategies to allow banking to flourish, as without banks and a trusted currency, commerce cannot flourish. The traditional solution is a highly centralised hierarchical system, based on a per nation basis on a central bank which issues currency, and then the so-called pillar banks that look after day-to-day banking. So if we trust the central bank, all will be well. The wording on American bank notes “In God we Trust” surely sums up the apparent inevitability of the devolution of Trust to a single powerful entity. But where there is money and the centralisation of power, there will be corruption and betrayal. Its not the Internet way.

In fact a partial alternative approach to solving trust issues in banking was always there, just never fully exploited. In Ireland we have what we call Credit Unions, as an alternative to the big centralised banks. They make a point of being based on the co-operative model. Trust is distributed amongst the customers of the credit union, who are also its owners.

What we are suggesting here is the extension of the co-operative trust model to the internet. Let us make the statement that “we all own the internet” a reality. In a co-operative environment things are organised so that trust flourishes because it is seen to work and betrayal is quickly detected and unlikely to result in any pay-off. That’s the plan.

The block-chain provides an alternative distributed approach to managing a currency without the need for a central bank. Trust is distributed. “In the block-chain we Trust” may not have the same ring to it, but it works just fine. And the block-chain cannot be subverted unless the majority of those involved betray trust and conspire together. So just how common are conspiracies?

Scott’s law: No conspiracy can survive in a setting where anyone can join the conspiracy.

4 The future of Trust

So the block-chain represents a distributed trust solution for the E-Coin problem. But it doesn’t end there. Other often simpler distributed trust solutions exist for other scenarios as well. The common thread is that trust should be distributed, although how it is done might vary in detail on a case-by-case basis.

A general approach to a solution suggests itself. Consider a setting where trust is distributed amongst multiple entities, and where any party can self-select as one of those entities, and where for a breach of trust to occur, all of the entities would need to conspire. Then apply Scott’s law.

Starting from this ideal, let’s work towards the practical. And to make it concrete let us consider the authentication scenario. Let’s say I need to be issued with a credential that would allow me to access a cloud-based service. The issuance of the credential should only occur if I can prove in some way that I am indeed entitled to it. The credential comes from adding together components delivered to me by three separate entities, (a) the service provider, (b) the cloud owner, and (c) an external provider. My concern would be that my credential could in theory also be issued to some-one else. However unless all three entities conspire together to do this, or all three can be fooled into issuing my credential to the wrong person, then this cannot happen. If the chance of any single entity failing to do what they have been entrusted to do is 1 in 100, then the chance of an overall failure of trust is 1 in 1,000,000. You get the idea.

So imagine a system whereby that CA-based PKI root of trust is replaced by a distribution of trust, which exhibits no single point of failure, and which is managed by a group of independent entities that do not necessarily trust one another, but at least one of which behaves honestly. At the same time we can take the opportunity to fix some of the other problems of classic PKI (no effective means of revocation, complex deployment for the individual user), and move to simpler identity-based methods, the mathematics of which naturally support this idea of distribution of trust.

To make all this work a new type of Internet entity will be required – a Trust Broker, or a Trust Authority. They will be required to issue cryptographic part-secrets, and to protect their own part-secrets. They will be completely law abiding within their own individual jurisdictions. They will be expected to be open and transparent, and to have a reputation for honesty. But if they are villains it doesn’t really matter, they can do no damage by themselves, and they will eventually be found out. As in all well designed co-operative systems, there is really no point in behaving badly.

Finally let us demonstrate that this is practical. Taking again authentication as an example consider a scenario in which a credential share is of the form $s_i.H(ID)$, where s_i a large secret number randomly and independently generated by the Trust Authority TA_i, ID is the recipients identity proven to the satisfaction of that TA_i, and $H(.)$ is a hash function which hashes identity to a point on an elliptic curve. The overall credential is $s_1.H(ID)+s_2.H(ID)+s_3.H(ID)+...+s_n.H(ID)$ if n TAs are involved. This is simple addition of points on an elliptic curve, and so the overall credential is $s.H(ID)$ where $s = s_0 + s_1 + s_2 + ... + s_n$. If just one of those shares is absent, its the same as having nothing. If TA_i is hacked, then only s_i is lost - the overall system remains secure. If some-one fools a TA into issuing a secret for an undeserved identity, then that part-secret on its own is useless. No entity ever knows the master secret s. With new ideas from cryptography secret shares in this simple addable form are entirely possible (which is not the case for old-style crypto).

5 A Proposal

How do entities register their willingness to act as Trust Authorities, and what is in it for them? Well they can do it for free, or for a fee. Probably the effort they put into carrying out their duties, and hence the amount of trust that can be assigned to their decisions, will be proportional to how much they are paid.

So imagine a network of TAs that are available to support the distributed trust scenario outlined above. A practical question would be how to these TAs get established, where do I find one, and how do I establish its trustworthiness. Here we outline a solution based on two ideas; the Block-Chain and the Web of Trust.

The Web of Trust is actually a very old idea, originally associated with the venerable cryptographic tool known as PGP (Pretty Good Privacy). This was arguably the original idealistic attempt to exploit public key cryptography for the benefit of the internet community. However in contrast with the Certificate Authority based PKI which eventually prevailed, it was based on a kind of distributed trust model, very much in tune with what we are proposing here. The big problem with Public Key Cryptography was always that of binding the public key to its owner. With CA-based PKI the owners "identity" is bundled with the public key into a Certificate which is digitally signed by a Certificate Authority. On the other hand with a Web of Trust, the public key is digitally signed by potentially a multitude of friends and colleagues, the basic idea being that the more people indicate their endorsement of my right to ownership of my public key, the more trust can be placed in that assertion.

A couple of other practical matters need to be resolved. First we need to establish a TA's URL and IP address so that it can be found on the internet, and secondly each TA needs to have a trusted public key to allow users securely access it.

Now a very hot topic of debate in the Block-Chain community is its potential application to problem domains outside of supporting a crypto-currency. One of the simplest ideas is to use a block-chain as a simple Proof-of-Possession of certain data on a certain date. Simply pop the time-stamped data (or more correctly a hash of the data) into a block-chain. Once accepted it becomes part of the ledger and cannot be changed.

Currently the issuance of domain names is centralised and under control of ICANN (Internet Corporation for Assigned Names and Numbers), a private sector organisation. That is a lot of centralised power! ICANN is responsible for managing and coordinating the Domain Name System (DNS) to ensure that every address is unique and that all users of the Internet can find all valid addresses. However using a block-chain it is possible to distribute this functionality and take it out of centralised control. This is exactly what a block-chain-based crypto-currency called Namecoin does, a development that has been acknowledged by ICANN.

So our idea is to bundle a Namecoin-friendly TA Domain Name and IP address along with its public key into a block, which is stored in the block-chain. Any-one who wants to use its services can find it there. But why trust it? This is where the Web of Trust comes in. Once established other TAs will sign its public key, and presumably have the complement returned, causing a new more trusted block to be created. When probed the block-chain will reveal all of the useful details of a TA, along with a complete history of its establishment and the development of its level of trust (which increases as it gathers more signatures on its public key from other TAs with which it collaborates, and from grateful customers). Revocation is easy – a compromised TA signs a revocation block which terminates that particular thread of history.

But of course a block-chain at the same time supports a currency, so it is entirely appropriate that charges can be levied for each transaction in order to reward the TA for its services and to discourage time wasters.