

Government role in Trust

Government has a pivotal role in establishing the level of trust that society needs in many areas. We trust banks and hospitals, without having to rely on anecdotal endorsement from others, because we know there is some government involvement in supervising them. The Internet needs the trust enhancement that only government can give. This is essential for Government 2.0 and for many other potential uses of the Internet.

It is worth quickly noting that government action can reduce trust, as we saw with China's push, now abandoned, to put opaque government software in every PC. Government will always be tempted to use any involvement in computing and networking to achieve other government objectives.

Risk is endemic in life. Eating is not safe, but is safer than the alternative. So we are designed to trust what we are forced to trust. Certainly this applies to computing and networking. We trust our computer even though we know that many computers like our own have been compromised and recruited into botnets. We trust our ISP even though we know that some ISPs have been caught utilizing and even changing data passing through them.

In the past governments have been talked into academic and ill-conceived security measures, such as supporting digital signature use based on a substantial misunderstanding of their appropriate application and of the law. Note that I strongly support the appropriate use of digital signatures, as, for example, in IETF standards. Internal government procedures show undue faith in the Internet Security industry solutions such as virus checkers and packet filtering. What is needed is to think clearly about what government can do that can't be done without it. The key thing is to provide the core trusted point, and to be very clear about the endorsements that are made from theirs. I will illustrate with a couple of examples.

1. Secure Client Environment

The needs of nearly all Australians using the Internet can be met via a very secure environment where:

- Computers are booted from read only media (such as CDs) that have been provided via a secure mechanism. After booting they would connect via a secure protocol (using digital signatures) to a central service that would effect any security fixes needed at that point in time.
- All user programs would be signed and sandboxed. The signer would be a government key built in to the read-only boot media. The signature would specify the appropriate level of sandboxing. Unsigned programs can be run in a tight sandbox that renders them harmless but is likely to make it difficult for them to be useful. Sandboxing doesn't have to be complex: a unix (or windows) user mode process is a form of sandbox.

Providing and certifying software doesn't have to be at all similar to the Chinese planned provision of opaque software. The signatures can be completely transparent even though they can not be reproduced. And it is possible, and appropriate, for the source software and toolchains to be made available so that the read only disks and the signed software can be completely reproduced exactly as distributed.

It is quite easy to do this for a sophisticated free operating system and environment, such as Linux. It is also possible for the government to work with Microsoft and Apple to produce similar setups for Windows and OSX. The possibility of losing the Australian market will focus their attention. Phones and PDAs also need to be covered, and while that is harder, it is an essential step to allow Internet connected mobile phones to be used safely for commerce.

Not everyone will want to work in the carefully sandboxed world. I think it would be appropriate for such unsafe use to be registered, if not licensed.

2. Secure identification

The Internet is naturally anonymous. What the social networking phenomena (such as facebook) shows is that many possibilities open up when we have identified individuals. People are willing, too willing, to give up privacy to obtain those benefits. This will be particularly true to enable business applications. There is no reason for Australians to trust external companies like verisign. It is appropriate that people and companies wishing to do business with Australia register their public keys with an Australian government key registry. However many aspects of identity don't need public key cryptography, but still need a trusted core. And in the context of (1) above the core public keys would be supplied as part of the read only booting process.

There is much more that could be said about both these points, but I urge consideration of the general point about the recurring need for government to establish trust in various contexts to allow society to function efficiently.

Robert Kenneth Smart
Robert.Smart@seagullwinds.com
0400 142 964
61 Jannali Cres, Jannali NSW 2226

Formerly CSIRO Networking research. [Skill Group leader of Distributed Systems in the Division of Information Technology, focussing on security. Later acting Project Leader in the merged CSIRO Mathematical and Information Systems. Technical author in the report to the ATO on responding to the Internet in 1997, available at [The Internet report - Australian Taxation Office](http://www.hpsc.csiro.au/users/sma045/the-internet-report.pdf) (<http://www.hpsc.csiro.au/users/sma045/the-internet-report.pdf>) which is still somewhat relevant to government 2.0.

Currently I am setting up a software development and consulting business registered as Seagull Winds. I am available for consulting.