[illegible] for NAA
[illegible]

Luttrell, Tas (REPS)

Submission No. 51

From: Roger Clarke [Roger.Clarke@xamax.com.au]
Sent: Saturday, 10 May 2003 12:24 PM
To: Committee, JCPAA (REPS)
Cc: Luttrell, Tas (REPS)
Subject: Re: Inquiry on the Management and Integrity of Electronic Information in the Commonwealth

Dear Joint Committee Secretariat

I hereby make the following submission to the above Inquiry:
http://www.anu.edu.au/people/Roger.Clarke/SOS/JPAA0305.html

I will be overseas from 26 May until 18 June.

Yours sincerely ... Roger Clarke

--
Roger Clarke http://www.anu.edu.au/people/Roger.Clarke/

Xamax Consultancy Pty Ltd, 78 Sidaway St, Chapman ACT 2611 AUSTRALIA
Tel: +61 2 6288 1472, and 6288 6916
mailto:Roger.Clarke@xamax.com.au http://www.xamax.com.au/

Visiting Professor in the eCommerce Program, University of Hong Kong Visiting Professor in the Baker Cyberspace Law & Policy Centre, U.N.S.W Visiting Fellow in Computer Science, Australian National University

SUBMISSION
Joint Parliamentary Committee on Public Accounts and Audit
Inquiry into the Management and Integrity of Electronic Information in the Commonwealth

Roger Clarke

Principal, Xamax Consultancy Pty Ltd, Canberra

Visiting Professor, Baker & McKenzie Cyberspace Law & Policy Centre, University of N.S.W.

Visiting Fellow, Department of Computer Science, Australian National University

Version of 10 May 2003

This document is at http://www.anu.edu.au/people/Roger.Clarke/SOS/JPAA0305.html

---

Introduction

I was invited to provide some comments to the Committee in the context of its Inquiry into aspects of electronic information, in particular in relation to two topics: PKI and Gatekeeper.

I am a consultant practising in the strategic and policy aspects of eBusiness, information infrastructure, and dataveillance and privacy. My company has operated continuously since 1982. I spent 1984-1995 as a senior information systems academic at the A.N.U. I have degrees in Commerce (Information Systems) from U.N.S.W. and a doctorate from the A.N.U., and have been a Fellow of the Australian Computer Society since 1986. I am at present a Visiting Professor at U.N.S.W. in the Cyberspace Law & Policy Centre and at the University of Hong Kong in eCommerce. I am Board Chair of a company owned by the nine Australian bodies politic, and a Board member of Electronic Frontiers Australia Inc. and of the Australian Privacy Foundation Inc.

I have conducted research, performed consultancy assignments, and published long series of papers in the areas of security and privacy, and in particular on digital signatures and PKI. The consultancies have been conducted for many agencies of governments in Australia, and in Canada and Hong Kong. They include past and present assignments for the National Office of the Information Economy (NOIE). I was also for a time a member of the Committee that nominally oversighted Gatekeeper, which was at that stage styled the Government Public Key Authority (GPKA).

Information Security Generally

It is common for the term 'information security' to be used to refer not only to the protection of data against inappropriate access, but more generally also information management and the protection of information integrity. I use it here in that general sense. Background information on Information Security is in Clarke (2001a), and bibliographies are in Clarke (2001b and 2003a).

The importance of information security has been recognised by the profession for decades. Australian information systems professionals have reasonable grounding in the relevant concepts and techniques. A number of specialist information security consultancies and services providers deliver advice and support. The country's research capabilities in security are strong.

Unfortunately, the importance of information security has not been grasped by executives in business and government. Successive scares in relation to Internet security, and discussions about the susceptibility of national infrastructure to disasters, criminal acts and terrorist strikes have not been sufficient to gain their attention. This is partly because the strategic significance of information is still not adequately appreciated, and especially because security risks are merely background noise to a busy executive concerned about 'the bottom line' or the urgent implementation of the government's current policy.

For some years I have been hopeful that programs would be devised to raise awareness among executives, and to educate senior managers. My hopes have not been fulfilled, and I have consequently focussed my energies elsewhere. It is noteworthy that I generated a great deal more interest among a recent delegation of businesspeople from the People's Republic of China, and have proposed to them that I run a week-long course there, through the Beijing Institute of Technology.

It would be valuable if the Committee were to spur the commissioning of a concrete awareness and educational program targeted at executives and relevant managers in both government and business, as a complement to the national infrastructure initiatives currently under weigh. Possible channels include the National Office for the Information Economy, the Auditor-General, the Defence Signals Directorate, the relevant Branch of the Attorney-General's Department, and the Information Management Steering Committee (IMSC).

The Committee might also find it instructive to seek information from a selection of agencies about the nature of the information security threat assessment, vulnerability assessment and risk assessment that they undertake, when such assessments were most recently performed, and what concrete measures have resulted from those assessments.

Also of interest would be agencies' responses to questions about their business continuity plan (sometimes referred to as 'disaster recovery plan'). This is commonly perceived by executives as just a technical matter, and consequently machine-readable data and software are backed up, but no arrangements are in place for alternative offices, or fallback procedures to be used by staff in order to sustain a limited, interim service. I fear that, even after Canberra's western fringe was ravaged by bushfire in January, many executives may still not appreciate their responsibility to assure continuity of services, and not just recoverability of lost data.

The Focus of the Inquiry

The primary motivation for the use of digital signatures and public key infrastructure (PKI), including Gatekeeper, is **not** the management and integrity of information. Their primary use is to authenticate the identities of parties to electronic transactions. One element of this is the protection of data against access by inappropriate parties.

Given the Inquiry's Terms of Reference, I think it would be inappropriate for the Committee to place undue focus on PKI and Gatekeeper. I believe that the bulk of the Committee's efforts would be most valuably invested into questions of:

- the use of threat, vulnerability and risk assessment techniques;
- the level of knowledge about and application of relevant standards;
- the use of mainstream information security tools;
- awareness, education and training in relation to those techniques and tools; and especially
- means of increasing executive commitment to them.

In relation to "the adequacy of the current legislative and guidance framework", I draw attention to the need for ongoing development of, and revision to, standards documents, the principal instances of which are listed at Clarke (2003a). Equally important, however, is recognition of the enormous variability of circumstances, and hence the need for each organisation to intelligently apply relevant standards, rather than them being imposed by some central authority and blindly implemented by agencies.

Digital Signatures, PKI and Gatekeeper

However, provided that digital signatures, PKI and Gatekeeper do not deflect attention too far away from what I believe are the primary issues, these aspects do have some relevance to the Inquiry. This section provides some definitions and references, followed by a brief review of the problems in the area.

A digital signature is a block of text added to a message, which provides evidence that the device that sent the message had access to a particular 'private key'. In order for the recipient of a signed message to test that evidence, it is necessary for them to have access to the corresponding 'public key'. Such 'key-pairs' are an invention of the 1970s. They have a much shorter history than conventional, 'symmetric' cryptography (which features a single key rather than a pair of related keys), and the techniques are only maturing very slowly. A tutorial is provided in Clarke (1996).

Unfortunately, naive technologists and marketing interests have projected the idea that digital signatures are far more than that. In particular, they have pretended that key-pairs can somehow be 'bound to' real-world identities such as people and corporations. Governments around the world have accepted these unjustified claims, at great expense to the public purse.

The term **public key infrastructure (PKI)** is much-used, but seldom fully understood. I define is as "the comprehensive set of measures needed to enable public key technologies to support the authentication of assertions" (Clarke 2003b). Appendix 2 to that paper provides a list of the elements that are needed to make up a PKI. Even when the elements are expressed as short bullet-points, the list fills two pages.

The conventional approach to PKI that has emerged since the mid-1990s is based on a particular certificate-format standard called 'X.509v3'. It is described in section 3 of Clarke (2001c). **The conventional approach to PKI is utterly flawed**. The deficiencies are documented in Davis (1996), Ellison & Schneier (2000a), Ellison & Schneier (2000b), section 4 of Clarke (2001c), Clarke (2001d) and Winn (2001).

Some of the inadequacies are inherent in the technology, and some are a result of deficient implementation. Because of the complexity involved, an effective PKI is extraordinarily difficult to devise, and would be extraordinarily expensive to build and implement. Worse still, it would be extraordinarily inconvenient and privacy-invasive. The privacy risks were documented long ago in Greenleaf & Clarke (1997), Clarke (1998) and Clarke (2000). To reduce the costs and intrusiveness, some of the necessary elements of a PKI are inevitably omitted, undermining the design.

Gatekeeper is an example of a conventional PKI, and is accordingly utterly flawed. It inherits the following important deficiencies:

- the companies that offer the necessary 'certification authority' (CA) services do not 'stand by their product', in that they provide extremely limited warranties and indemnities. The many problems that would result from the use of the scheme would rebound on agencies, and to a very considerable extent on Australian citizens. Moreover, most citizens are not in a position to even understand the problems, let alone resolve them;

- the scheme presumes that every citizen would be able to take very good care of their private signature key. This is simply not possible with the grossly insecure (primarily Microsoft) operating systems that the public uses. See section 5.3(b) of Clarke (2001d);
- the arrangements for managing the revocation of lost, stolen and otherwise compromised private keys are completely inadequate. As a result, prosecutions in which evidence depends on the Gatekeeper scheme would fail;
- the scheme would require Australian citizens to be subjected to enormously intrusive procedures, and even then would fail to prevent people with serious intent from circumventing it.

The question has to be asked as to why Gatekeeper has been persisted with for so long, when it is so tragically inadequate. I participated in or was otherwise familiar with a number of projects conducted by the agency responsible for the project, which was originally the Office for Government Information Technology (OGIT), subsequently renamed the Office for Government Online (OGO). The agency was responsible for many well-conceived and well-run initiatives. But **Gatekeeper is a standout as the worst-performed project that OGIT/OGO was ever involved with.**

I and several colleagues drew the problems to the attention of the then OGIT at the very outset of the project in 1997. We continued to draw the problems to the attention of the responsible executives during the period in which the agency created and then dismantled the Government Public Key Authority (GPKA). I have retained copious documentation of these matters, and should any witness attempt to defend the conduct of the project, I would be pleased to shake the dust off it, and provide documents, specify dates, and name names.

It is therefore completely rational for agencies to resist the proposition that they should implement Gatekeeper. It would be highly expensive, it is highly and unjustifiably privacy-invasive and would be resisted by many people and organisations, and, fundamentally, it could never achieve its objectives anyway.

Quite simply, the succession of OGIT/OGO executives who were responsible for the initiative between 1997 and 2000 were not competent to understand the nature of the technology (which was, and still is, arcane and difficult). Much worse, however, they were not capable of assimilating the information that they were receiving, and preferred to accept the ambitious and self-serving promises of technology providers and a few government security specialists. All of those executives have since left the Commonwealth Public Service.

The responsibility for Gatekeeper subsequently passed to the National Office for the Information Economy (NOIE). The executives of NOIE have been left with the task of doing what they can with the remnants of the initiative. A current project is developing a new, more comprehensive and more sensitive framework.

Conclusions

Alternatives to failed conventional PKI like Gatekeeper do exist. I have researched and proposed approaches to the use of public key technology that would both be effective and avoid excessive intrusions into privacy. The fundamental need is for each organisation to decide what kinds of assertions actually need to be authenticated, and to apply available technologies to achieve that purpose. It is vital to individual freedoms that anonymity and pseudonymity be supported, and that identities be contextually limited rather than singular. My proposals are presented in Clarke (2001d and 2003b). I made an invited presentation on these matters to the [U.S.] National Academy of Science in Washington DC in October 2001, and have been invited to do so by the OECD, in Paris, in December this year.

Constructive conclusions which I submit to the Committee for consideration are as follows:

1. the Committee should recommend that relevant agencies implement concrete measures to encourage executive appreciation of, and commitment to, the importance of information and information security, including information management and information integrity;
2. more specifically, the Committee should recommend that this be achieved through the commissioning of an awareness and education programme for senior executives;
3. the Committee should recognise that the rejection of Gatekeeper by agencies is not merely reasonable, but is actually strongly advisable, because the scheme is unjustifiably expensive, unjustifiably inconvenient and intrusive, and in any case ineffective;
4. the Committee should express support for NOIE's current project to broaden the scope of authentication, to recognise the enormous risks of negative impacts of authentication schemes on citizens, and to ensure wide consultation with affected parties, especially the general public.

References

Clarke R. (1996) 'Message Transmission Security (or 'Cryptography in Plain Text')' Privacy Law & Policy Reporter 3, 2 (May 1996), pp. 24-27, at http://www.anu.edu.au/people/Roger.Clarke/II/CryptoSecy.html

Clarke R. (1998) 'Public Key Infrastructure: Position Statement', May 1998, at http://www.anu.edu.au/people/Roger.Clarke/DV/PKIPosn.html

Clarke R. (2000) 'Privacy Requirements of Public Key Infrastructure' Proc. IIR Conf., Canberra, March 2000, at http://www.anu.edu.au/people/Roger.Clarke/DV/PKI2000.html

Clarke R. (2001a) 'Introduction to Information Security', February 2001, at http://www.anu.edu.au/people/Roger.Clarke/EC/IntroSecy.html

Clarke R. (2001b) 'Information Security Bibliography', February 2001, at http://www.anu.edu.au/people/Roger.Clarke/EC/IntroSecyBibl.html

Clarke R. (2001c) 'The Fundamental Inadequacies of Conventional Public Key Infrastructure' Proc. Conf. ECIS'2001, Bled, Slovenia, 27-29 June 2001, at http://www.anu.edu.au/people/Roger.Clarke/II/ECIS2001.html

Clarke R. (2001d) 'The Re-Invention of Public Key Infrastructure' December 2001, at http://www.anu.edu.au/people/Roger.Clarke/EC/PKIReinv.html

Clarke R. (2003a) 'Information Security Standards, April 2003, at http://www.anu.edu.au/people/Roger.Clarke/EC/IntroSecyStds.html

Clarke R. (2003b) 'Authentication Re-visited: How Public Key Infrastructure Could Yet Prosper' Forthcoming, Proc. 16th Int'l eCommerce Conf., Bled, Slovenia, 9-11 June 2003, at http://www.anu.edu.au/people/Roger.Clarke/EC/Bled03.html

Davis D. (1996) `Compliance Defects in Public-Key Cryptography` Proc. 6 th Usenix Security Symp., San Jose CA, 1996, pp.171-178, at http://world.std.com/~dtd/compliance/compliance.pdf

Ellison C. & Schneier B. (2000a) 'Risks of PKI: Electronic Commerce' Inside Risks 116, Commun. ACM 43, 2 (February 2000), at http://www.counterpane.com/insiderisks5.html Ellison C. & Schneier B. (2000b) 'Ten Risks of PKI: What You're Not Being Told About Public Key

Infrastructure' Computer Security Journal, v 16, n 1, 2000, pp. 1-7, at http://www.counterpane.com/pki-risks.html

Greenleaf G.W. & Clarke R. (1997) 'Privacy Implications of Digital Signatures' Proc. Conf. on Digital Signatures, Sydney, at http://www.anu.edu.au/people/Roger.Clarke/DV/DigSig.html

Winn J.K. (2001) ‚The Emperor's New Clothes: The Shocking Truth About Digital Signatures and Internet Commerce`, Idaho Law Review, 2001

Navigation

Go to Roger's Home Page.

Go to the contents-page for this segment.

Send an email to Roger

Created: 2 May 2003

Last Amended: 10 May 2003

These community service pages are a joint offering of the Australian National University (which provides the infrastructure), and Roger Clarke (who provides the content).

XAMAX Consultancy Pty Ltd

The Australian National University
Visiting Fellow, Faculty of
Engineering and Information Technology,
Information Sciences Building Room 211

Xamax Consultancy Pty Ltd, ACN: 002 360 456
78 Sidaway St
Chapman ACT 2611 AUSTRALIA
Tel: +61 2 6288 1472, 6288 6916