SUBMISSION NO. 4

Submission To Australian Federal Parliament
Joint Select Committee on Cyber Safety

Prepared By
Louis Leahy
Director
Armorlog International Ltd
Suite 3, 6-16 Riverview Street
PO Box 80 North Richmond
New South Wales
Australia 2754
Armorlog@Armorlog.com.au
1 June 2010

1. **This submission deals primarily with the Committee's focus resolution topic bullet point number 5 "breaches of privacy" in so much as we address the fundamental failure on computer networks the outmoded two factor authentication that is widely used and is the cause of most problems with fraud. Consequentially it also has reference to point 4 "identity theft" particularly as some attempts to fix the issue result in facilitating identity theft. It also presents a mechanism to "improve the online environment" the topic of the Committee's bullet point number 1 and discusses this in the context of point 7 "opportunities for co-operation nationally and internationally".**

2. **There are numerous forms of attack on modern computer systems, networks & access devices that generally involve some degree of human error resulting in frauds being perpetrated. These are focused around securing the traditional user name and password for access to systems and resources.**

3. **Perhaps the issues have arisen because the requirement to authenticate users over wide area networks (WAN) was not apparent in early data processing requirements which gave rise to development of the traditional username and password logon method to manage resources.**

4. **Currently the Structure of the internet sites in using this methodology leaves users open to attack by fraudsters. It does this primarily because of the following weaknesses that exist in the way nearly all commercial websites are currently constructed.**

    a. **The address at which users login is generally made available to everyone, in most circumstances this is not required and only done as a matter of convenience and to contain costs.**

b. **Most networks still only rely on outdated 2 factor authentication information about which resides on the client side computer and leaves users open to attack from keyboard logging, malware, phishing attacks, man in the middle attacks and password guessing programs.**

c. **Most networks do not deploy lockout mechanisms to prevent password guessing.**

d. **Most networks present all credentials for login on the one screen and often one or more of the credentials is not masked.**

e. **Current solutions that attempt to secure the identity of the person logging on reside on the client computer and as a result fail to give the necessary added level of security to the user if the user's computer is compromised.**

f. **Most networks currently use character systems that are widely known and where a custom input is used it is generally on public display. Often where custom sets are used it has the inadvertent result of lessening security by reducing the possible password combinations.**

g. **Most networks use a single username across the network that is referred in communications & documents and on screen which exposes the users account to fraud. This username is can be accessible to network users within the organisation exposing the user to internal fraud and may often be published on communications with the user exposing the user to external fraud.**

h. **It is relatively easy for a skilled fraudster to illicit the clients credentials on a 2 factor authentication system commonly know as phishing it can take many forms including fooling users by telephone, instant messaging, text messaging, email and via surreptitious website attacks that install malware even within the browser while the user is actively on the internet. These types of attacks are starting to proliferate and while software vendors are very adept at developing solutions unfortunately users are not as adept at installing them and keeping up to date.**

i. **Some networks have unfortunately incorporated procedures in the management of their systems, sometimes in order to try and control fraud, that inadvertently actually result in greater amounts of private information being revealed about users that actually facilitates identity crime as it provides opportunities for fraudsters to accumulate further knowledge about a target that assist in change user details to take over their accounts & thus identity.**

j. **Most networks facilitate users duplicating passwords used elsewhere. When this occurs users are at greater risk in regard to identity theft.**

k. **Many networks do not prevent users using easily guessed passwords.**

l. **Many networks allow computer user names and passwords to be stored in the computers internet browser.**

5. **These weaknesses have facilitated fraud which is occurring at greater rates and is undermining confidence in computer networks in particular the internet. When users authentication credentials are discovered this results in the users privacy being compromised sometimes very seriously. We have developed an new authentication technology that addresses these issues. We refer to this technology as Variable Proprietary Character Set Multi Layered Login™ or the acronym VPCSML™. A paper outlining this technology with screen shots of the software accompanies this submission. Details to access an audio visual presentation are also contained at the end of this paper.**

6. **One of our Company's main objectives as part of the rollout of our technology is to offer a free website verification service that will act as an opt in mechanism for sites that are prepared to abide by a simple set of rules the basis of which are is an undertaking by licensees that they must agree not to allow the use of the technology for antisocial purposes such as money laundering, pornography, prostitution, weapons dealing, bait advertising and unlicensed, defective or illegal product distribution or dumping. Licensees will be required to display an unobtrusive Armorlog logo, licence number & web reference that will enable users to check the site is legitimate as a further level of validation for consumers unfamiliar with the licensee or if the user suspects the site may be a fraudulent or spoofed site.**

7. **This will be an opt in arrangement making it easier for internet users to indentify sites that are acting within the constraints of the above social agreement. Armorlog will progressively provide a site rating on the lookup that is nominated by the web provider but subject to complaints monitoring as a method of self regulation to indentify misclassification. We believe this is a better solution in comparison with attempts to block selected content at ISP level as it will assist parents in setting firewall settings with an additional set of criteria to select suitable sites that are allowed through the family router or computer firewall. We hope that in time operating system vendors will have an opt in option to filter based on the Armorlog Licensing listing & classification. An important factor in this is that it will be self funding via the normal software licensing fees for anyone choosing to use the new authentication technology. The negative in comparison to ISP filtering is that this is untested and will only be successful if the technology with its inbuilt social agreement is widely accepted.**

8. **With this in mind we have also endeavoured to structure the distribution and licensing model to provide a recurring income stream to IT professionals to assist them in providing technical support and content and assistance on networks and relieve some of the economic pressures on them, that could prevent them from undertaking necessary work for the benefit of the development of the internet that they may otherwise choose to do if it were not for having to worry about inconsistent income generation from project orientated nature of their business. We hope in doing this that it will facilitate an adoption of the technology more quickly and more widely to address the aforementioned challenges.**

9. **We have endeavoured to have our product reviewed by the Government in particular we made submissions to the Australian Taxation Office, the Department of Defence and the Department of Finance and the Prime Ministers Office for it to be considered however no assessment has been undertaken by any section of Government. This is in spite of the fact that there is currently a proposal to rollout digital certificate technology from a foreign multinational by the Australian Taxation Office to other Government Departments including the Simplified Business Reporting arrangements which will involve many small enterprises that will have great difficulty in dealing with the complexity of implementing the cumbersome certificate requirements.**

10. **Unsurprisingly we are of the view that digital certificates are inferior to our technology and are not an effective solution as they reside on the client computer and consequently if control of that computer is seized by a fraudster either remotely or locally the logon will still appear legitimate as the information resides on the client computer which is a fundamental flaw. We are also greatly concerned by the proposal that the Auskey will form one set of credentials to access multiple Government services this significantly weakens security and exposes the users to magnified difficulties if their account is compromised.**

11. **In fact the Australian Taxation Office's (ATO) newly marketed Auskey (a name which it appears may infringe on another international company's trade mark) touts that it is even easier to transfer the digital certificate by USB from one device to another which will further weaken it effectiveness. Indeed we would argue that such security sensitive applications should in fact be tied to preferably MAC address or if roaming is to be allowed a static IP address. Further to demonstrate the difficulties with implementing digital certificates we point the recent introduction of the Auskey to tax agents and the ongoing interruptions it caused to tax agent operations to such an extent that the ATO felt compelled to extend lodgement programs for Agents to cope with the problems it created. We believe the use of these certificates could significantly hinder the take up of simplified business reporting. Personally I find this state of affairs particularly disappointing as I wrote to the Commissioner to introduce our technology and received a letter back advising that the ATO is not responsible for such decisions however as an accountant and registered tax agent I received a lot of ATO communications and I have received numerous pieces of information from the Commissioner and Assistant Commissioners about Auskey which begs the question if that was true why is the ATO writing to us about its new security technology.**

12. **We have to admit unfortunately that they are not alone in disregarding what we have developed. We have written to the largest 50 banks globally the Australian Bankers Association, the American Bankers Association, the NSA, the top tier accounting firms, all the major computer hardware and software vendors, many of the internet service providers and every internet registry without any positive responses. It appears there is a distinct lack of will on the part of major players to recognise the problem. The indifference appears widespread we also wrote about our invention to over 300,000 journalist and with the exception of a handful of independent internet based publishers we were essentially ignored. We even tried the ABC inventors to no avail.**

13. **I also personally requested that my paper be published in my professional accounting association's magazine National Accountant however to my dismay the editor and editorial committee stated that my creation is not sufficiently related to accounting. I was intrigued by this rejection particularly in light of the recent professional standards changes that make in incumbent in accountant's audit processes to detect and comment on control systems with reference to fraud risk. The fact is what we have designed is definitely within the realm of accounting it is a business system control but has an application also to the wider community in particular the internet community but also to computer networks in general. This was particularly disappointing given I have supported the National Institute of Accountants for over 26 years. We also submitted a paper to the World Computer Conference in Brisbane and were knocked back because I had a verb in the wrong place, a false accusation of mismatch in topic title and that the paper was claimed to be not scientific which is not surprising given that we are not scientists. We were also criticised for not revealing full details of our intellectual property, for not including pictures, not numbering paragraphs and that our paper is based on a commercial patent. There was no actual assessment or any substantive argument as to the acceptance of the paper based on the merit of my invention it was simply form over substance.**

14. **We also approached the CSIRO as we understood they were arranging a technology incubator with funding from large revenues they are receiving from their wireless patent. The offer I received from the officer involved was that the CSIRO couldn't help but he was able to assist personally. No doubt he understands the significant potential for our technology. Needless to say I poetically declined this offer which I viewed as highly inappropriate and a clear conflict of interest as my approach was clearly to the CSIRO and he was in its employ I had not approached him on a personal basis.**

15. **We approached a Government sponsored venture capitalist the only one that had funding at the time and they refused to sign a Non Disclosure Agreement and intriguingly the entity I was referred to by them was a different legal entity to the one listed as the approved venture capitalist. Needless to say I chose to discontinue that particular line of enquiry.**

16. **We have also lodged an application with Commercialisation Australia however it appears that the process for this does not suit the development of a commercial venture such as ours. The process of applying particularly the budget model is overly complex and full of traps that appear to be designed to restrict the number of successful applicants and the amount of funds to be expended. I suspect in relative terms to the amount of funds that we may actually qualify if at all it has probably not been worthwhile and simply a distraction many of the applicants I met at a function for this had the same opinion. We are coming to the view that this whole process is very disingenuous. We would be interested to see what the management costs are for each dollar of funding extended.**

17. **Essentially we have come up against significant amounts of intellectual, academic and anti-commercial prejudice and some skulduggery. We are of the view having experienced such high levels of recalcitrance that it is imperative that Government acts to ensure that networks develop in a secure and socially acceptable manner.**

18. **Fortunately we are blessed with a strong Australian can do attitude and are not easily deterred from our endeavours. I have been invited to present the paper I have written at Worldcomp 2010 in Las Vegas, this is independently peer reviewed and one of the largest gatherings of computer scientists globally. We have also been assisted very professionally by Austrade and the NSW Department of Industry & Trade to arrange to be able to exhibit our newly developed software at CommunicAsia 2010 in Singapore.**

19. **There have been some large class actions resulting from a systemic failure by institutions to protect consumers privacy in North America (Countrywide & Heartland). Given the apathy we have experienced by institutions toward addressing these fundamental flaws we suspect there will be many more. However as more and more people become aware of the flaws in current networks it will become more difficult to deny liability where reasonable steps to protect users are not being taken.**

20. **It is important to note that what we propose is not a re-write of systems the fear of which we suspect may be the reason why a new solution such as ours is ignored. We have specifically designed the solution to be an adjunct to existing systems to facilitate its implementation.**

21. **We identified a great need to address these security issues some 10 years ago and have been working on our solution to it. We sincerely believe it is worthy of proper consideration. It is apparent the Parliament in constituting this Committee has also identified the importance of these issues and we commend the Honourable Members for taking action.**

For Armorlog International Ltd