15-09-2019

To the Review Committee
Australian Federal Government
Australian 2020 Cyber Security Strategy Review

By Email to cybersecuritystrategy@homeaffairs.gov.au
& submitted online at https://www.homeaffairs.gov.au/reports-and-publications/submissions-and-discussion-papers/cyber-security-strategy-2020/submission-form

We understand the Government is preoccupied with many important matters including the oppressive drought that has befallen us. Never the less we would seek to impress upon the Government that authentication reform is critical as it will improve trust on the internet which will secure communications and encourage people to engage online and reduce carbon emissions from unnecessary travel & congestion that are contributing to the climate change issues we all now face.

We have designed multilevel authentication for the 21st Century that prevents password guessing, password dictionary attacks, password phishing attacks & password keylogging attacks. It works to secure user interactions across the internet.

These are the main forms of attacks in 70% to 80% of instances that result in financial losses according to Verizon research over many years.

Our solution is the ONLY solution that achieves this necessary protection against these attacks.

Full details about our technology are available on our site at https://armorlog.com

It is a great Australian invention no less transformative than the CSIRO wireless patent that now brings in hundreds of millions of dollars in licensing fees but was originally laughed at by market controlling incumbent American multinational companies who then later sought to exploit it without paying fair royalties for its development.

Following is the link in the documentation for authentication proposed by Data61 who has been commissioned by the Government to implement security standards for data sharing including initally open banking, energy and telecommunications.

https://consumerdatastandardsaustralia.github.io/standards/#authentication-flows

Consumer Data Standards
Introduction. These standards have been developed as part of the Australian Government's introduction of the Consumer Data Right legislation to give Australians greater control over their data.. The Consumer Data Right is intended to be applied

sector by sector across the whole economy, beginning in the banking, energy and telecommunications sectors.
consumerdatastandardsaustralia.github.io

You will note that there is no provision other than to use the existing standard onetime passwords and a prohibition on calling the users account password.

Unfortunately neither measure will stop credentials phishing attacks taking control of access accounts please refer to our video that explains the problem and the solution.

https://armorlog.com

If our technology VPCSML was used they would not have to have the prohibition to call for passwords and would essentially protect the api.

A technical explanation of our multilevel authentication is available on our website at https://armorlog.com .

We have endeavoured to engage with Data61 many times over many years and we have unfortunately been continually ignored.

At one point the CSIRO prior to Data61 existence did allocate an officer to look at our technology but that officer tried to have us deal with his own company outside of the CSIRO which we had to decline as it appeared to us to be in breach of public sector governance standards.

This matter is critical and the Government should take steps to ensure multilevel authentication is implemented.

The risks with api's was highlighted in the UK open banking review and which concluded that there is a need for improved authentication.

Nothing in what Data61 is proposing is new it is simply a rehash of existing practices and it will not stop api breaches.

The recent Landmark White api breach is an example of how existing api security is effectively non existent and the representations being made by existing technology providers and so called standard setters are fraudulent.

The critical matter with api's is that once an attacker has breached the virtually non existent security under current models they then have access to all the data provided by the api.

This is a great concern because the Government now has many initiatives in play to open up access to data in many spheres. No doubt it is not lost on the Government (or should not be) that if it does not resolve this authentication issue it will put these plans in jeopardy.

Opening up data will bring many significant benefits from research and competitive efficiencies perspectives however if the Government fails to properly address authentication security before it undertakes these programs it will be recklessly exposing the Australian public to significantly increased risks of identity theft, invasions of privacy, data theft and financial fraud.

We have also written to the Government many times about the authentication weaknesses of Auskey & MyGov and unfortunately these weaknesses are in the process of being replicated in the new MyGovID also.

Here is documentation that confirms that the ATO intend to rely on device based authentication https://softwaredevelopers.ato.gov.au/myGovID

Please review our video at https://armorlog.com for an explanation as to why device based authentication fails.

Authentication needs to be independent of devices because devices, fail, get broken, get lost, don't get software upgrades, are stolen, become obsolete, are easily imitated, are subject to sim card swaps, vulnerable to keylogging malware and so on. It is these device weaknesses that attackers exploit to gain access to network assets.

The Review would also be aware that these services are provided by our competitor the ATO who, as we have written to the Government about many times, have continued to attack us most recently as last week and we have sent copies of our responses to this continued harassment to many sections of the Government over more than 8 years with no intervention to have this persecution cease.

Over the more than 10 years we have been writing to the Government, the Government has failed to undertake any review of our technology, this is completely irresponsible and reckless.

We maintain that the ATO deliberately mislead a Federal Court judge about the significance of these matters and the role they play in providing public authentication services in Australia.

It is disappointing that Government has continued to ignore us and worse through its agencies is actively continuing to attack us.

We maintain that the Commissioner of Taxation and other select Officers of the Department of the ATO have deliberately and wilfully mislead key Government Ministers and the Parliament repeatedly now over many years to our severe detriment.

We will now be forced to curtail our patent strategy because of the ATO actions and because they failed to pay compensation for damage they have caused and the resources and time they waste in their continued attacks on us and the funding they have denied us that we are rightfully entitled to.

This is disappointing as it will significantly diminish the benefits for Australia as an Industry can be built around my invention that can be as big as RSA built around digital certificates which effectively, we supplant.

If we are to prevail now however the Government has to act quickly because of its' failure to act in the last 10 years.

We have to act to secure patents in India and to maintain the patent portfolio in other major jurisdictions to protect the IP for the benefit of Australia.

Renewals for patents are due by the end of this coming week and we are not in a position financially to meet these obligations as a result of the ATO incessant attacks on us and interfering with our capital raising and forcing the closure of our long standing business of 23 years we do not have the resources to continue to try to protect the IP for the benefit of Australia.

In decades to come if the Government fails to support our endeavour people will look back on this as yet another squandered opportunity similar to the Hargraves aircraft wing invention IP for which the benefits were lost to Australia.

Putting aside the critical National interest aspects of this matter, it would be a mistake to think that such opportunities are falling out of the sky when in fact this is simply not the truth these opportunities are extremely rare and should be jealously protected for the benefit of future generations of Australians. Australia simply cannot continue to rely on importing technology it creates back into Australia from other Countries who have had the good sense to exploit if, if it does our technology transfer costs will become insurmountable.

We are completely in your hands if all the years of work we have put into this is going to be exploited for Australias benefit we have done absolutely everything we possibly can and our family has made great sacrifices for the good of everyone over many years but we simply can't continue to do it alone we need institutional assistance if it is going to become the new standard and we need it quickly.

In the 10 years that the Government has ignored us its agencies have spent hundreds of millions of dollars on Cyber Security and yet the number of breaches continues to climb at an alarming rate and the costs to society are mounting. In all this time the Government has never undertaken an assessment of our technology and has instead sought to make our lives a living hell.

We deserve the benefit of the doubt in these matters given the persecution we have been subjected to and have endured because we know we have the correct solution to protect society from the scourge that is credentials breaches that are continued to allow to persist because technicians are mistakenly treating the symptoms of the problem and not the cause.

We would beg that the Government is not so arrogant as to continue to ignore us or dismiss us yet again such behaviour is so last century. After the persecution and indifference, we have suffered

over many years we deserve to be heard and request that the Government acts quickly to protect Australian interests in these matters and lead industry to implement this new initiative to protect the community from credentials theft.

Thanks
Louis Leahy
CEO
Armorlog Group

www.armorlog.com

"Building Internet Integrity"