Will Technology Make Information Security Impossible? And Must Technology be Invented Just Because We Can?

Thoughts Occasioned by Brunner's "The Productions of Time" and Asimov's "The Dead Past"

Paul Wernick and Bruce Christianson

University of Hertfordshire College Lane, Hatfield, Hertfordshire AL10 9AB, England
tel. +44 1707 286323 p.d.wernick@herts.ac.uk

[Major spoiler alert: this paper reveals major plot turns of these stories. If you want to read them for the first time and maintain the element of surprise which Brunner and Asimov achieve, please do not read any further.]

1 Introduction

In his science fiction novel The Productions of Time [2] John Brunner postulates a technology that can record the thoughts and emotions generated by the human brain during sleep, and replay them on demand later for an audience. Isaac Asimov's The Dead Past [1] describes a device that can look into the past and display what actually happened. Brunner's book and Asimov's story raise interesting questions about the confidentiality and integrity of information; how would each be affected by the invention of these devices, and what countermeasures can be envisaged? There is also a deeper question which we do not consider here – what would be the effect on individuals and society of being unable to protect our private thoughts?

A common theme that emerges from these two works of speculative fiction is: can the implications of technical innovations for society be predicted? More generally, can (or should) the invention of devices with extreme implications for privacy and information security be controlled?

2 Plots of the Works

2.1 The Productions of Time

Our hero, Murray Douglas, is given an opportunity to revive his flagging acting career by joining a company for a new production. The brilliant but erratic and controlling director assembles a group of actors in an isolated country house, each of them has had a career-threatening problem. His stated intention is to produce a new play by developing ideas improvised by the cast. At the house, the director provides each actor with the source of their problem – in Douglas' case, caches of alcoholic sprits. It is all very strange ...

In his bedroom Douglas finds a strange aerial attached to his mattress, linked to a tape recorder under his bed. Similar systems are in the bedrooms of the other company members. Eventually it turns out that this device is intended to record brain impulses as the sleeper dreams, dreams turned into emotional nightmares by the availability of the source of the sleeper's weakness. The "servants" are actually a group of criminals who have travelled from the future to record these emotions and dreams. The recordings will be taken back to the future where, as most people lead bland lives, they command high prices amongst thrill-seekers who can vicariously experience the raw uncontrolled thoughts. In that future world this mind-reading technology is controlled by the government, and private possession is illegal, but the profit to be made from illicit recordings is sufficient to make the game worthwhile.

Finally, of course, Douglas defeats the criminals and escapes safely – with, inevitably, The Girl.

2.2 The Dead Past

Asimov postulates a device that can look into the past and project the vision on to a screen. The chronoscope' device is operational but its use is under strict government control. A historian cannot understand why the government goes to considerable lengths to prevent him using it. Furious at his research being blocked, he investigates, and works out that a cheap chronoscope can be built by any amateur with sufficient knowledge using easily-available parts. He promptly publishes details of how to make one.

Asimov then has a character point out that anything which happened even a second ago is in the past, and that it can now be seen by anyone with a chronoscope. The inventor, instead of creating a window into the past for historians – indeed, the device can only see 120 years into the past so this is of limited utility – has created the ultimate snooping device, which allows anyone to see what anyone else did a moment ago.

3 Implications of These Inventions – What are the Threats?

What have these two science fiction works – a 1960s novel and a 1950s story – to do with the theme of SPW 2015? We suggest that together they would pose a great threat to the secrecy and integrity of information. Although secrecy and integrity are conventionally regarded as different security services, current mechanisms for providing one generally rely on the availability of the other at a "lower" level of abstraction, and it is this dovetailing which is threatened.

3.1 Threats to Secrecy

Brunner postulates a device that needs to be close to the victim but, even without a more powerful device that could read minds at a distance, the implications for

secrecy as currently implemented are disturbing. If Brunner's thought-reading device were capable of reading a person's thoughts in detail, then it would be impossible for a human to keep any secret, since it could be read directly from the secret-holder's mind. Even if it could only read more general information, this might provide clues to passwords and answers to security questions. Can a system rely on something you know to identify you when an enemy can just read it directly from your brain? Your security question: your dog's name, your mother's maiden name, your school; all can just be read from your brain and repeated as required.

Asimov's invention would bypass the need to read minds, as any security-related actions which took place in the past can be observed. As you type in your password, you can be watched and your keystrokes observed. However well you try to hide your actions it is inevitable that over time your typed passwords will be seen. If you are issued with a security device to plug in to authenticate yourself, the issue process will be visible to enemies, information which can potentially be used in the future to subvert that process. If you try to hide the device, your action will be seen, so no location will be secure by virtue of secrecy. Worse, the design and production of the device will be visible, making duplication much easier. If biometrics are employed, the process of identifying the person with the biometric value will be observable. How valuable is a biometric when an enemy might see the way your details were captured in the first place and subsequently use this information to replace your details with their own (see the discussion on integrity below)? No secure back channel will be free from observation, so any such channel will be vulnerable if it relies on any covert activities.

Any system that relies on the use of specific devices whose presence guarantees that a person is authorised to access secure material is also threatened. Even if an attempt is made to control access to and/or possession of these devices, a sufficiently determined attacker could peek into the minds of their designers, and observe the manufacturing processes. This might enable that attacker to produce illicit copies which would be indistinguishable from newly-made legitimate examples.

In any case, what is the point of trying to maintain information secrecy when the result of somebody reading or hearing the information can be read out of their brain? The only secrets that can be kept are those that nobody ever needs to know. The only reassurance in these circumstances is that the bad guys will be as badly off as the good guys. Forget the master criminal with his[1] secret master plan. The police will have it even as he's thinking of it, and even before he's told his evil henchmen or committed it to paper – assuming that the police are taking advantage of the technology to watch everyone.

[1] Traditionally all (or almost all) master criminals are male, Elementary's Jamie Moriarty being a notable exception.

3.2 Threats to Integrity

The two inventions make vulnerable any authentication-, confidentiality- or integrity-maintaining system that relies on maintaining a secret.

Current mechanisms for guaranteeing the integrity of information at a distance primarily rely on secrecy. Digital signatures based on public/private key pairs demand that the key part in the hands of the signer be kept secret. But this reliance in practice often relies in turn on another secret – what is the passphrase I use to access my key material, where do I keep the device which contains my secret key? This approach is just as vulnerable as the secrets discussed above.

Biometric-based authentication approaches will also be vulnerable to attack, as the integrity of the information used to confirm identity might be comprised in a similar way. However, there are alternative approaches to integrity preservation which do not rely upon keeping secrets – for example non-repudiable publication of a hash value[2].

4 Potential Solutions – and One Problem Solved?

We have identified two possible means of addressing the threats outlined above. One of these relies on making security mechanisms impossible for an enemy to reproduce by denying them access to useful parts of a previous datastream, whereas the other depends on not revealing a shared secret to a vulnerable party i.e. a human being.

Christianson and Shafarenko's Vintage Bit Cryptography approach [3] is based on the idea of flooding an attacker's information-capturing resource with large amounts of data – far more than can be stored, in which the actual information to be transferred will be hidden at previously-agreed secret locations, with the rest being discarded and not stored by the recipient. The security arises from the attacker not being able to determine in advance which bits of the data stream actually encode information and which do not; the attacker therefore needs to store the entire datastream until this can be determined, whereas the communicators can happily discard irrelevant bits and are thus not faced with the same axiomatically-insuperable data storage problem.

This approach may help resolve the problem arising from Asimov's history reader, as the attacker cannot store all the bits whilst waiting to identify which parts of the datastream are important and which are padding. If we assume that the covert data channel from the past to the future has large, but not infinite, capacity, it will not be possible for an attacker to extract the useful parts in the same way as the legitimate recipient[3]. It should however be noted that Christianson and Shafarenko still rely on secure bootstrap of an initial

[2] Jikzi (LNCS 1796, 22–47); DODA (LNCS 2845, 74–95); or a slight re-purposing of the Eternity Service: `www.cl.cam.ac.uk/ rja14/eternity/eternity.html`

[3] Whereas even a low-bandwidth covert channel from the attacker's future into their past breaks most security protocols.

weak secret between the communicating parties, which is potentially vulnerable to both types of attack[4].

Despite the concerns raised above it may be possible to resolve the problem of secure communication (although not that of reading information from participants' minds) by the use of tamper-evident boxes. However these boxes must not contain any secrets installed in such a way that this installation may be observed, or depend for security on any action or attribute of a human, or a secret known by a human, as these are all open to reading by one device or the other. (We assume that neither Brunner's nor Asimov's devices can look inside a device and read stored contents not visible to humans without leaving some trace.) We therefore need boxes which leave the factory in a known state and are later brought into agreement to communicate with each other using secrets shared on a one-time basis and impossible to read without affecting the devices, by using some physical mechanism analogous to Kish pairing of devices or quantum entanglement. The secret is thus unreachable and unreadable by the vulnerable element of the security infrastructure, i.e. people.

After one-time mutual initialisation a pair, or larger group, of these boxes could authenticate within the group by some challenge/response mechanism, and then communicate securely, all on the basis of their shared secret. Even if attackers could see the boxes and their operation, or perhaps even obtain them in factory-fresh condition, without the one-time physically shared key they would not be able to communicate with a specific set of boxes, as they are not in possession of the shared secret held in the boxes. The only remaining issue would be that of maintaining the physical security (secrecy and integrity) of boxes, as a member of a group in an attacker's hands would be sufficient to make all authentications and communications insecure.

Paradoxically, we consider that one security-related problem will be solved by Asimov's device. His invention would allow us to literally see with whom we are communicating in almost-real time, which may help resolve the issue of authentication[5].

Regardless of whether the technology described by Brunner and Asimov becomes science or remains fiction (but see below!), we believe that it is a profitable exercise to re-evaluate our security infrastructure, including physical as well as cryptographic security, from the point of view of the threat model which they would enable.

---

[4] Unless this was done before the inventions can be deployed, whence the term "Vintage".

[5] Indeed, it could help solve the data integrity problem, providing we make strong assumptions about the integrity of the data supplied by the chronoscope. Such assumptions are unnecessary for secret sniffing, because in current protocols a correct guess for a secret can usually be verified independently of how the guess was obtained.

5 Wider Implications

Brunner's criminals use unlawfully-obtained technology to further their mind-ripping crimes. Asimov's history reader is suppressed for the best of reasons. In both cases, future society apparently suffers from the same issues we currently face; that devices which are safe in the hands of the good guys are very useful for criminals who will therefore expend considerable effort to obtain them and the knowledge needed to use them. A current instance is the spate of thefts of high-value cars using stolen technology which enable thieves to clone the immobiliser-disabling devices needed to operate the car. Once technology is readily available it becomes not just a source for good – Brunner's mind-reading technology could be employed by mental health practitioners to help treat people – but an enabling technology for the bad guys.

If at some future time a technology appears that can read the minds of people without their permission and then replay the recordings to others for surveillance or entertainment purposes, how would society change if this equipment was in the hands of a government which claimed to be working for the good of society as a whole or of private corporations, or of criminals, who do not have this defence? And if this device is invented, can we provide sufficient countermeasures to maintain our privacy against these scanners? And, if privacy protection technologies to defend ourselves against this snooping are invented, who will control access to them? Will mere possession of such a defence without suitable authorisation be seen as an indication of criminal intent?

Asimov's story poses a different problem. His is a technology which may actually be of little value to the bad guys in the long term, since anyone – including the police – can keep an eye on them as they plan and execute their illegal operations, but which will change society as anyone can see anyone else's activities. Blackmail will be impossible as everyone will know that they are being observed all the time – Bentham's Panoptikon made real. The threat of blackmail will be removed, but at the price of a complete loss of privacy as everything will be known anyway – there are no unshared secrets left to reveal.

Both Brunner and Asimov assume that the technology is nominally under government control, as are, for instance, today's information interception technologies, but in both cases the government's attempts to control the technology are failing. What if these get into the hands of the wrong people (or, depending on your opinion of governments, other wrong people), as from past experience seems inevitable? Are some inventions too dangerous to invent? Should the development of some technologies be banned entirely because of their implications for society and/or for individual freedom and privacy? If not, who should control access to this technology? And what actions should they be allowed to undertake in order to maintain this control?

Research has been recently published [4] that allows human thoughts to control external processes beyond game-playing using an EEG headset. Other research described in the same report allows a mouse's brain to be influenced by a surgical implant controlled by a human's brainwaves, control which can change the animal's emotional state. This is turn triggers observed chemical changes

in the mouse's physiology. We are already demonstrating an ability to control external events by reading human thought processes using technology. This is equivalent to Brunner's much cruder manipulation of his hero by the provision of alcohol. We are now one step closer to being able to manipulate people and record the resulting patterns. That the results of the experiment have been observed by the researchers is another step towards Brunner's dystopian vision.

As we look back 60 or more years to the stories we started with, we can see that the issues they raised are even more relevant – and even more all-embracing – than they were then. Can we maintain any privacy at all as new technology emerges, or will we have to pull down the net curtains, replace all our walls with glass windows, and let everyone see everything we do? When Steven Rambam said, "privacy is dead, get over it," was he being more prescient than even he realised?

References

1. Asimov I (1956) The Dead Past. In Earth is Room Enough, Panther Books Ltd, London, 1971 reprint, 9-52.
2. Brunner J (1967) The Productions of Time. Penguin Books Ltd, Harmondsworth, 1970 reprint.
3. Christianson B and Shafarenko A (2009) Vintage Bit Cryptography. In Security Protocols, Christianson B, Crispo B, Malcolm JA and Roe M (Eds.). Lecture Notes In Computer Science, Vol. 5087. Springer-Verlag, Berlin, Heidelberg 261-265.
4. ETH (2014) Controlling genes with your thoughts. Online at https://www.ethz.ch/en/news-and-events/eth-news/news/2014/11/controlling-genes-with-thoughts.html (accessed 14 Nov 2014) (formal publication in Nature Communications online at http://www.nature.com/ncomms/2014/141111/ncomms6392/full/ncomms6392.html)