Will Technology Make Information Security Impossible? And Must Technology be Invented Just Because We Can? (Transcript of Discussion)

Paul Wernick

University of Hertfordshire

I took the title for the theme of this workshop absolutely literally because I've been using fiction as a starting point. I've taken a couple of items of technology created in the minds of science fiction writers and walked them forward and just seen what the implications would be for information security. So, just to give you an idea of what I'm going to be talking about I'll outline the stories. This is going to be a complete spoiler for both of these stories, so apologies to anybody who will actually want to read them later on. I'll talk about the technologies, what threats they pose to information security separately, and possibly when used together, and some possible countermeasures that we've thought up, though hopefully you will come up with others.

Both of these by the way are quite old stories. John Brunner's is from 1967, Asimov's from the 1950s. So firstly, John Brunner's Productions of Time, our hero, who is an actor, joins a company being set up in a house somewhere to improvise a new production. Turns out that all the members of the cast have some weakness or other, our hero drinks a lot, somebody else has a drug problem, someone has an interest in young boys, etc. And our hero finds that each member of the company is actively given access to whatever it is is their weakness. Even more puzzling there's some sort of wire grid on the beds where they sleep at night, and what he finds out eventually is that some people have come back from the future, and they're using technology to capture the thoughts of each actor as they they relive their experiences, to take them back to the future and market them to people who enjoy these sorts of vicarious pursuits. A bit by accident, a bit by bravery, he foils the plot, gets away, and of course he gets out with the girl.

So we've got a technology that must be capable of capturing mental patterns. There's more to it than this, and Brunner's idea is that it captures emotions. The technology he envisages has to be able to identify which particular mental patterns go with particular activities, or particular relived experiences, and to be able to record them in such a way that you can play them back when our villains go back to the future, so that the people who are buying these sort of black market things can enjoy them.

Frank Stajano: It is also a requirement that the technology must be able to allow the guys to go back in time?

Reply: This is true.

So let's have a look at the other story, Asimov's Dead Past, which is a novella. Here our hero is an historian and Asimov postulates a device, I presume some sort of television screen device, using which you can look back and see what's happened in the past. And our historian thinks, this is absolutely brilliant, I'll be able to go back and look at all the unexplored areas of history, and all the controversial elements, go back and see what *actually* happened. It will open the world of history to reality rather than the conjecture of historians based on poor documentation. Not only that, but this thing's comparatively cheap to make. You can buy the bits easily, and you can put them together, and you can then have your 'view of the past' device, wonderful. So why hasn't anybody done this, why hasn't anybody published the details of it? So our hero decides to do something about this.

All of a sudden the government are stamping all over him and saying, "how dare you do this, you're not allowed to do this," but the government won't say why. Eventually the historian manages to publish the design, and the government then points out two important flaws in his reasoning, one of which is, Asimov's take on the technology, that it only goes back a certain short time, well a hundred years, short for an historian, into the past, and therefore you can't actually see what happened a long time ago. Secondly, that of course everything that happened a moment ago is in the past, so you can see anything anywhere. Somebody could replay the last sentence I've just spoken. So everything in the past is available. Privacy has disappeared, there is a device snooping on everybody, permanently. And that was the reason why the government said they didn't want this thing published. And the denouement of the story, there you are, privacy is gone.

So what sort of technology have we got here? Well, something that can observe the past, can see what's going on, on Earth at least, it doesn't take it beyond that. It could be projected in sufficient detail for viewers to recognise what's going on. Asimov's idea is, as you go a hundred years into the past it fades, but what happened five minutes ago is nice and clear. And for this purpose we're going to assume that this is good enough to be able to see, for instance, what keys somebody hit on a keyboard, so you can literally look over anybody's shoulder and see what they've typed in, and see what they get back on their display.

So what are the implications of these for information security? Let's think about confidentiality. Well firstly, is it possible for a human to keep any secret, if you can just look in their mind and read it out. Let's put to one side the idea that you needn't bother with any other technology than just read it out of the secret-holder's mind.

Let's think about what happens perhaps when secrets are in transit. You use devices to implement security features, you've got black boxes, you've got some software, crypto, things running on machines. Brunner's device allows you to read the mind of the designer and say, how do you design this? What features have you put into it? There's this black box, but you just look in the designer's mind and there it is, now you know how it works. You can also read out passwords

from somebody's mind, and indeed their answers to their security questions; what was your dog's name? just read it out of somebody's mind; what's your mother's maiden name? read it out of their mind. It is possible to read all of that information that we commonly use to maintain some level of confidentiality straight out of people's minds.

Asimov's history viewer, you can see any actions that relate to confidentiality. If somebody is typing in their password, you just look over their shoulder and you see what they've typed, nice and easy. And if you didn't get it first time, you just replay it until you've got all of it. What about the security device? Well you can see how it was issued. Somebody gets a particular device, they work for a company perhaps, or work for an intelligence agency, how do they get their device, let's look at the detail, and the issuing process, so we can replicate it. How is it used: are there any special tricks? If you hide it because you don't want to carry it on you, where is it hidden? Nice and easy to see. How did they make it? Well, let's have a look in the factory and see what happened, or look on the designer's board. And any secrets that are entered into it to make it secure by a person, well let's have a look and see what they did. Let's say something is individualised by somebody connecting it to a computer and typing something, we'll see what it says.

The one saving grace here is that the good guys can also see what the bad guys are doing. If you've got the criminal mastermind sitting in his – it is usually *his* – lair, usually dark, somewhere underground, laughing hideously, and sending his minions out to do bad things, well the police can watch what he's doing, and it makes detection a bit easier.

What about the implications for integrity? Well, a lot of integrity protection is based on the confidentiality of something anyway, so really the same issues apply. You've got a wallet, you've got all these wonderful security features, but you roll it back far enough and eventually it's something somebody has, or something somebody knows, or something measurable about them.

Ross Anderson: I'm not sure I buy this. In a world with total pervasive surveillance, like David Brin's proposal where everybody can see everybody else as a design feature, there's no need for particular controls and integrity, because if you want to know what I agreed with Mr. Bloggs at 3 pm last Wednesday at a car dealer in Leicester you just turn on this chronoscope and you look back, sorted, finished. There is no more need for digital signatures, there's no need for message authentication codes, all that just can get tossed.

Reply: As long as you're dealing wih stuff that can be actually put up on a screen and read.

Mark Lomas: Even then you have to look through the entire history because the information that they had five minutes ago may be corrupted ten minutes ago. And therefore you'd have to go through the entire system backwards.

Ross Anderson: Well, a contract is just a crystallization of what people agree to, the agreement was at a particular period of time and they would start doing stuff about it. Where people dispute contracts, you typically resolve that by looking at the correspondence that went before, and the delivery notes that

went afterwards. Once you have got that all completely visible in plain sight, and once you've got an ongoing relationship between people, if somebody says, "no I never said that", then at that point you go back and you verify, just as you would if ...

Mark Lomas: What you're saying is you can verify an individual piece of information, but if you want to verify the totality of something you have to go back to its independent ...

Ross Anderson: Well that's the case, even if everything is legitimately signed, you end up with terabytes of stuff that you've got to wade back through, and ...

Bruce Christianson: But one of the things that you can do with digital signature is agree a chain, or a local tree of what's included and what isn't included.

Ross Anderson: And then of course the dispute is not whether the contract is signed, but whether the executive that signed it had the proper authority of the company to do so.

Bruce Christianson: And so forth. So the counter-point of an integrity property is being able to prove that a particular document *wasn't* annexed to the contract, it wasn't around at the time the contract was signed.

Keith Irwin: So, the integrity stamp in this case is going to be the exact time and location where you can go back and see this signed. You can still do a chain, you just say, oh I'll go back and look at this one, and you can see when I'm signing this, it shows the integrity stamp, which says, well when this part came it was here, and you can work your way back, it's a little longer to validate but it's still doable.

Max Spencer: But it's like just going back and looking at the time when the agreement was made. It's slow, you just have to actually go and observe, check that the thing really was actually the same, and surely that's a good argument for using some kind of digital mechanism.

Reply: Which is great until you're actually digitally signing a bag of bits of some sort ...

Bruce Christianson: Yes, precisely.

Reply: ... which represents something else. If it's something you could actually see in front of you, we sit down, and we sign the contract, great, wonderful, you can look over a person's shoulder and see what it is. But if it's a large data store being transferred it's a bit more difficult to work out what was there.

Ross Anderson: I think there's a broader point here. *If* we understand that integrity becomes a different kind of problem, because the cryptographic keys that we currently use for signatures and MACs are no longer relevant, so we just look at the original source materials. *Then* there's a similar criticism of the argument in respect of confidentiality, which is that if you can observe the plaintext being generated by people opening their mouths and talking, then whether you've got access to the keys you used to encrypt the data becomes entirely moot ...

Reply: Yes.

Ross Anderson: ... and this reflects the policy discussions that we're having nowadays with the run up to, the next snoopers' charter. Twenty years ago it was all about whether the government would have access to keys; now who cares? It's all about the government having access to the plaintext that's kept on the servers of Google, Facebook, and so on. And whether that was encrypted on its way to the datacentre in Oregon using SSL is almost an irrelevance.

Reply: Yes. As long as you can demonstrate that the plaintext you're looking at, and the stuff that was sent, and the stuff that was received, are the same thing.

Ross Anderson: But in that case the TLS is the policeman's friend rather than his enemy. It means that when he does seize information from Google through M-Lab he can then wave it in front of the magistrate and the defence lawyers have a harder time quibbling it.

Reply: Well, let me press on. Another issue for integrity is that of biometric-based information, which again, has to be captured and entered in some way, and suffers from exactly the same issues as any other information. But again, it's something that isn't actually directly readable by people and therefore able to be confirmed that it is in fact the right information.

We have thought of a couple of potential solutions for this, one of which actually was prefigured a couple of minutes ago, which is vintage bit cryptography[1], it was Bruce and Alex Shafarenko was it not? The idea is that you just send masses and masses of bits, and only a few of them will actually contain the information, the rest of it is just padding. And the poor attacker is left trying to capture all this stuff, and there's just too much, too many bits being passed down the line for him to capture it all and analyse it, or to keep enough information that's sufficiently far in the past to be useful.

Bruce Christianson: The argument is that the bandwidth from the past to the future, although large, is not actually infinite.

Reply: As the good guy you don't have to worry about all the extra bits, you don't have to worry about keeping them. The bad guy has to keep them all on the off-chance that some of it will in fact be relevant. So that would get round some of the issues there. However much you look into the past all you're seeing is this incredibly long bit stream that you can't capture anyway.

Another possibility is to have devices that don't actually reveal anything to a person, or reveal anything in public. One of these technologies relies on looking inside somebody's head, if the information that's maintaining the security isn't in anybody's head, that's not going to work. The other technology relies on what can be seen outside physical devices, externally visible phenomena. If the connection doesn't produce any phenomena like this then that can't be seen either.

Ross Anderson: Well at present if you sign an international treaty, or if the President of the USA signs an Act of Congress, then this is video recorded, right, and it's put on the TV. And given that the cost of videoing stuff and saving it are dropping precipitously, the prospect exists that you could record

[1] LNCS 5087 pp 261–275.

all contracts forever in this way. If you buy insurance from a telephone call centre, they tape record the conversation and keep it for seven years. Maybe this is just how everything will operate in the future.

Reply: A system of connected devices that don't produce any external phenomena, as I'm suggesting, would at least allow secure communication.

Bruce Christianson: What Ross is saying is you don't actually need to keep secrets. Is that right, Ross?

Ross Anderson: Well, if I'm running an insurance company and I have an archive of the recordings of every transaction of any of my call centre operators has ever made with a customer or a prospective customer, I can do some very lightweight things to guarantee the integrity of that. I could put a hash of it in the New York Times every morning, and I can keep my backup tape with my lawyer, whatever, that's a minor engineering detail. The fact that I've got all the plaintext is what I rely on. If there's a dispute I pull the recording and I play it.

Bruce Christianson: There is still a question about how you verify that it really was me at the other end of the phone call.

Reply: Or somebody else who looked over my shoulder when I typed in my password.

Ross Anderson: But there's no password, I have the recording of your voice.

Bruce Christianson: Yes, but the question is whether it really is me.

Frank Stajano: It's increasingly possible, plausible let's say, to have synthetic generation of videos of things that never happened.

Ross Anderson: Do I care.

Frank Stajano: Yes, if you're relying on that as evidence.

Ross Anderson: But my evidence I secure by computing a SHA-512 of all yesterday's communications and publishing to the newspaper.

Frank Stajano: Yes but, if it's in an adversarial context, you could still have done this with synthetic videos and published the thing in the New York Times. There's no guarantee to someone who doesn't believe you that these were things where you *actually* interacted with a client, as opposed to a reconstruction.

Ross Anderson: Now we're getting to somewhere useful, because how a transaction between me and a call centre disadvantages me is that they've got a copy of the contract but I don't. So the policy intervention here might be to say that you make a copy of the contract available to the customer as a condition of its future enforceability, and you can then talk about the technology and the infrastructure necessary to do that. And then I keep a copy of the contract if I want to rely on it, and you keep a copy of the contract if you want to rely on it, and if we argue about who's lying later then a judge looks at us and looks at the evidence, and looks at the available forensics, and makes his mind up in the context.

Bruce Christianson: But that evidence includes the video recording of you giving me the copy of the first video recording.

Frank Stajano: I think it's a good idea. I would prefer the version where I, the customer, make my own recording of the call with the call centre; because I envisage, since we are talking science fiction, that the call centre could *in real*

time create a different one, and send me that different one. And then not only would I have to have the stupid call with the call centre, which probably involves 30 minutes of muzak, but also I'd have to re-watch it *again* to make sure that they sent me the same thing that actually happened! If I record it myself, at least I don't have to do that.

Ross Anderson: So what happens at the moment if you buy insurance is they send you a certificate of insurance with a schedule, and you may then find that they've got some of the details wrong, so you phone them up and you do it again. Now it's only if you've got a dispute later, if you crash your car and there's an argument over who said what when you registered the claim, that the recordings as a practical matter has to be replayed. Do we want to think of some infrastructure to make this easier?

Reply: Yes.

Ross Anderson: Do we want to have a central government repository where people could lodge copies of their recordings, or copies of hashes of their recordings. What's the appropriate technology here?

Alastair Beresford: Both parties could record what they thought the conversation was, and swap, and maybe with enough sensible audio processing you might automatically be able to check they're similar enough to say that you don't have to listen to them again, so that might be an alternative.

Bruce Christianson: But the slight difficulty is the case where my end of the recording was in fact made by a simulacrum of me, and the reason I don't have a copy of the recording is because I wasn't involved in the transaction, and that's why I can't produce my copy, but the court's not going to believe that.

Alastair Beresford: But I guess the insurance company would have two copies, neither of which would involve you at this stage if it was some other criminal that produced it.

Ross Anderson: What actually happens is that two people have a different view of what was said, because each person has a different mental makeup, different things are salient to them, important or unimportant, so if they write up minutes of the conversation afterwards you may get two completely different descriptions of the same process, which is why you have written contracts in the first place.

Alastair Beresford: Or what people say is ambiguous like the phrase "don't stop", which can be interpreted as "carry on" or "*don't!* Stop!"

Ross Anderson: Exactly so.

Reply: Actually now I think maybe Asimov's device sorts this out, because all the caller has to do is to know when I phone up the insurance company ...

Bruce Christianson: He just needs to know the coordinates.

Reply: ... and then just watch the transaction going through, play it back, play back history.

Bruce Christianson: But I like Ross' idea of saying, let's think about what the infrastructure would be to have a distribution mechanism that essentially assigns coordinates to all these things.

Ross Anderson: Well, we're actually building this infrastructure because we're all carrying around lots of devices with cameras and microphones, and they're all backing up in Google's datacentre in Oregon. So just wait twenty years and Google maps will become clickable, and replayable, and then we can show you what happened here 17 hours ago. The Chronoscope is being built, and it lives in Oregon, and it's free so long as you pay for ads.

Joan Feigenbaum: So I heard a talk by Bruce Schneier in which he considered not the continuous Chronoscope but just the little pieces of it, which Ross just alluded to, that already exist. He was most intrigued by the potential effect on families and, in particular, the potential effect on marriages. You have all these conversations in marriages that consist mostly of "no you said this, no you said that, no you said this." What if couples could actually resolve all those disputes? Suppose they could answer the question "What did you actually say three days ago when we were discussing this thing that you're supposed to be doing right now?"

Bruce Christianson: I predict the divorce rate would go up.

Joan Feigenbaum: Right. Schneier said "My relationship with my wife would not improve if we could always *prove* that what we think the other person said is *actually* what the other person said."

Reply: I think we'd just move the argument a bit rather than resolving it.

Jeunese Payne: There was an interesting mini series on Channel 4 where they showed these sorts of scenarios. One of the scenarios was what if you could record absolutely everything, through your eyes, and then you could play it back. And there was a marriage scenario in this, where some guy's wife had been cheating on him, and he made her play it back, and they even played back previous sexual encounters while they had sex, instead of actually having sex with each other, and all sorts of creepy stuff. The mini-series is called Black Mirror, and most of the episodes to me are very creepy, but they all play with this idea of what happens if technology goes a little bit step further, and that's one of the possibilities that they do. Also whenever someone goes to the airport they have to play back their last 24 hours or whatever, for the security guy to see.

Reply: I think we're getting back almost towards the vintage bit cryptography, because if I've got to play my last 24 hours back in real time then we'll stand at the airport for 24 hours.

Jeunese Payne: No, not real time, the speed's sped up, and he and you would have to view it.

Frank Stajano: Well if you know in advance it's 24 hours, just do the nasty thing 25 hours before!

Jeunese Payne: Well I don't know if it was 24 hours, but basically you have to play it back. The whole point was that nothing was really private anymore, peoples previous recordings were taking over their life, and their current situation, so this guy had gone on holiday and he was complaining about the hotel, and he was playing it back on the TV through his eyes saying, can you see the

mess on the floor, can you see this. Instead of actually just living in the present, everybody's living in the past.

Joan Feigenbaum: So nothing is private, and nothing is ambiguous.

Reply: But society relies on ambiguity.

Joan Feigenbaum: Exactly.

Frank Stajano: Most of your life recording will be of you watching the TV of the previous recording.

Reply: Yes, watching your TV, and you're watching a previous recording, not quite infinitely, but just 61 years of it.

Keith Irwin: I had a question about the second solution. Are we assuming that the Chronoscope can only see people going back in time?

Reply: Well I assumed it could see anything.

Keith Irwin: The question is are we talking about only light, or do we have a wider electromagnetic spectrum? Do we have tempest attacks into the past? I just wanted to ask what the assumption was.

Reply: The poor man was writing in the 1950s, give him a break.

Keith Irwin: I'm asking how *you're* defining it.

Reply: Video and I'm assuming audio as well, and that's about as far as it gets. So no, nothing further into the electromagnetic spectrum.

So therefore you have two devices that talk amongst themselves without actually producing any external phenomena, and don't have any human input into their setting up.

Keith Irwin: Right, so they mustnt have like the transistor buzz depending on their calculations and that sort of thing.

Reply: Well, yes exactly, and no light displays that say what they're going to do, just as a way of transmitting stuff at least outside the Chronoscope.

So there are some other implications here. The first thing is ...

Dylan Clark: I just wanted to revisit the idea that video would remove ambiguity. I don't think it necessarily would, because I think it depends on the viewpoint of the observers. I can, I had some training in the professional use of violence, now my friend showed me videos of what they term police brutality, and to them it is police brutality, to me, from things I know, it's clear that the police are trying to disable the person without hurting them. And yet, from each of our viewpoints, it's the same video, but it's totally ambiguous.

Reply: Well, back to treaties again, as Ross pointed out, their wording is often ambiguous to get both sides to sign them.

Anyway, another issue that I touched on with Asimov's device. Both authors have said these devices have to be illegal, or controlled by the government for the public good. Brunner's criminals have stolen technology, and they know when they go back to the future they're going to get picked up by the police unless they are fairly swift of foot. The government knows that Asimov's device exists but deliberately suppresses it because of the effect on society.

Another thought, which is that both authors postulate a future society that suffers from the same problems that we have. There is some privacy but both are subject to technology-based attacks. That technology being distributed, despite

the fact the government wants to control it, does leak out sooner or later. And the technology that can do good, such as the police watching the criminals preparing to commit their crime – this is the map of where their armoured car goes, oh good, the police can see where they're going to hit it – but can also have bad effects.

The question of how it would actually change society, we've already had this discussion. If these devices existed what effect would there be on society, going beyond any of the technological aspects of it? And would we be able to devise countermeasures to protect our privacy? There have been some suggestions that we keep our own copy of the record, or maybe that we have an edited copy of the record – are we actually allowed to cut stuff out of our past, not be 100%? And who controls access to their devices – will it actually be illegal to have a device that stops somebody else from looking at your past? In a way for me the technological aspects are less interesting than the societal ones, and I think if these devices existed, life would be interesting. Thank you very much indeed.

Ross Anderson: There was an interesting article in The Guardian a couple of days ago called The Future of Loneliness and Internet Isolation[2]. It talks about these issues, and it has to a link to a YouTube video, which brings out the way in which pervasive surveillance changes people's behaviour.

Reply: Yes, if you know you're being watched ...

Ross Anderson: Absolutely. You change what you do.

[2] www.theguardian.com/society/2015/apr/01/future-of-loneliness-internet-isolation