Introduction: Information Security in Fiction and in Fact (Transcript of Discussion)

Bruce Christianson

University of Hertfordshire

Hello everyone, and welcome to the 23rd Security Protocols Workshop. Our annual theme is not intended to constrain the contents of the discussions, but more as a suggestion for an unconventional point of view from which to look at them: this year our theme is Information Security in Fiction and in Fact.

Fiction can become fact. Sometimes this happens spontaneously, because the idea is already in the air, fiction picks up on it first, and fact just takes a few years to follow. Sometimes it takes more than a few years, I've still got a jet pack on back order since 1963. Sometimes, however, the link is causative. The reason that clamshell mobile phones look the way they do is because the engineers who designed them watched Star Trek when they were little.

But the movement can be in the opposite direction: fact can become fiction just as easily. The fact of the unbreakable Enigma machine became fiction without the Germans realising that it had. Secure public-key cryptography might, if you believe some people[1], have already gone the same way. Or, if you prefer to believe Ross Anderson and his collaborators[2], all of our algorithms for quantum computers may be about to be re-catalogued as works of speculative fiction, set in an alternate reality where magic is real. And what if it turns out[3] that P = NP, and there aren't actually any exponentially hard cryptographic puzzles at all? The whole of cryptography would join the long-bow as something that we can enjoy reading about in tightly plotted works of historical fiction.

I have alluded to the fact that fiction comes in a number of different genres, and sometimes we're perhaps a little careless at failing to distinguish these. The historical fiction genre is where we try to be as careful about the facts of history as we can, subject to the small number of changes we have to make to get the plot to work. Gothic novels, in contrast, are not subject to such constraint.

The same goes with the future. On the one hand we have what used to be called hard SF, where we try and respect the currently received laws of physics, apart from one or two innovations needed in order to make the plot work, and at an opposite extreme we have space opera, where it's OK to just push an entire alien civilisation in through the wall whenever we feel like it. Maybe a lot of

[1] apps.washingtonpost.com/g/page/world/a-description-of-the-penetrating-hard-targets-project/691/

[2] Ross Anderson and Robert Brady, 2013, Why Quantum Computing is Hard - and Quantum Cryptography is Not Provably Secure, arxiv.org/abs/1301.7351

[3] www.claymath.org/millennium-problems/p-vs-np-problem
www.travellingsalesmanmovie.com/

the developments that we dismiss (rather disparagingly) as security theatre are actually intended as security opera, and trying to look for a sensible plot in the background is to completely misunderstand the nature of the entertainment on offer.

So. What can we learn from the way information security is presented in fiction? In particular, can we learn something interesting about what people *believe* to be true? And what could we achieve, if we put our minds to it, in terms of making things that are currently fiction become fact in the future? In the other direction, what could those who write fiction learn from us? Particularly those who compose *convenient* fictions, people like politicians, and the civil servants who advise them. And what sort of genre do we want our own work to occupy? Do we really see everything we currently do as falling into the little niche market of fiction called Early 21st Century Noir, or should we be trying to break out of that genre and into the mainstream?

This is, as always, a workshop and not a conference. We've got a mixture of people that we have had before, and people that we haven't. We try to put a few people who've been at least once before up at the front of the programme, to help those here for the first time to get an idea of what to expect, but if you come and give the talk that you planned to give when you planned to come, then something has gone terribly wrong. Please expect to be interrupted, even if you're in the middle of interrupting somebody else.

This is intended to be a low friction arena, and if you break somebody's protocol during their talk, it is polite to try and help them fix it afterwards. You'll get a chance to revise your position paper, in the light of these interactions with the other participants, before you have to resubmit it.

We also publish transcripts of these discussions, but they too are works of fiction, because they are heavily edited, and we won't let you say anything stupid on the record. So this is a safe environment in which to take risks.

Frank Stajano: Yes. On the subject of the fact that this is a safe environment in which to try things out, the proceedings are then going to be heavily edited for taking out any stupidities and so on. What you say is going to be recorded multiple times.

Reply: Yes, we have a kind of Minority Report thing going.

Frank Stajano: The recordings are going to be made available to you and, for practical access control reasons, to everybody else who is also an author, but they are not going to leave that group. The primary person to revise your thing, to edit out the stupidity[4] is going to be *you*!

[4] Except when it is essential to the plot.