Introduction: Virtually Perfect Security (Transcript of Discussion)

Bruce Christianson

University of Hertfordshire

Hello everyone, and welcome to the 18th Security Protocols Workshop. Our theme this year is "Virtually Perfect Security", which is an attempt to tie together three slightly different interlocking strands. The first is the fact that although we talk about security as if it were some sort of metaphysical property (so that a system is either secure or isn't), we all know that really whether a system is secure or not depends on the context which you put it, and you can move a system to a different context and change whether it's secure or not. In practice, we also usually prove security relative to a particular abstraction, and the danger is that we have a system that "really" is secure, and then we discover that the attacker is using a different abstraction. Our attempt to find abstractions which the attacker can't fool with this trick with has pushed us into talking about security using abstractions that are further and further away from anything that a user might think of as comprehensible or convenient.

This brings me to the second strand. We're very used to pieces of hardware or software not providing us with the abstraction we want. The basic service provided by a micro-processor is pretty useless to an application programmer, the service provided by a low level network interface is not very useful to anybody doing systems programming, and the solution that we use is the usually the same: we build up a series of virtual machines. So long as you keep one eye on the price/performance ratio, you're generally OK. I've said on many occasions in the past that you can think of computer science as a branch of pure mathematics in which the homomorphisms cost money. As soon as we try to use this approach in security protocols we discover that they don't layer well at all, but we keep trying to do it largely because it's the only trick we have. So we build an authentication protocol, and we try to build other security services on top of that, and then somebody else comes along and puts some middle-ware in, and we have to go back and do it all again. It seems there's something about the nature of the abstractions that we're using for security that we really don't understand (or that we're just not allowing for) when we try to layer.

The third strand is that there still seems to be some hope of knowing whether we've got it right or not when all the endpoints have at least one foot in the real world. But increasingly we have situations where one of the parties in the protocol exists entirely in cyberspace. Second Life is an obvious example of this kind of situation, but a potentially more worrying one is applications like e-Science, where you're doing an experiment, the experiment is entirely in cyberspace, and the reason you're doing it is because you don't know what the correct outcome ought to be. Thinking about the potential security implications of projects like this is really quite unsettling.

There has been some work in the past looking at the extent to which an attacker (or a legitimate participant) can find out which virtual machine they're running on. Attackers, for instance, would quite like to know whether or not they have been sand-boxed. David Deutsch has made a very good argument in one of his books[1] that says that the universe is in fact a simulation running on an anonymous computer, and he has an experimental programme that he believes will prove this; there's a counter-argument in some of the early works of Hilary Putnam[2] but personally I regard the last word on the subject as the second of the "Ghost in the Shell" movies[3]. The question is, does having a presence in the real world give the attacker an advantage, or is it actually a handicap?

The intention as always is that this should be a workshop and not a conference, so expect to be interrupted. Conversely if you are interrupted, feel free to depart from whatever it is you planned to stay when you stood up, and if the interruption gives the urge to go off on a tangent, please do so. In the interests of spontaneity and unexpectedness, we've already changed the programme, so please make sure you pick up the new running order.

[1] David Deutsch, "The Fabric of Reality", Penguin, 1997.
[2] Hilary Putnam, "Brains in a a Vat", pp 1–21 in "Reason, truth and history", Cambridge University Press, Cambridge, 1981.
[3] See `http://en.wikipedia.org/wiki/Ghost_in_the_Shell_2:_Innocence`