The topic that I suggested when we were asked for abstracts and talk titles back in January was “Protocol governance: the elite, or the mob?” And sustainability is very fashionable these days so let’s ask ourselves whether protocols are sustainable. We’ve had one or two comments from previous speakers that all protocols tend towards failure because of environmental changes. I agree with that entirely. We’ve been discussing for over a year now in various fora why the CA infrastructure is so broken; there was a wonderful panel at financial crypto last year with a chap from Mozilla having to defend himself against a room full of annoyed people. Why is it that security APIs are almost unfixable? Some of us have looked at that a lot at Cambridge.

Well I think we understand that in these cases the interface has become unmanageable because of economic and political failures. There’s asymmetric information, there’s other externalities, there’s conflicts of interest, and there are governance failures at scale. Now up until now we’ve talked about security economics, but when you start talking about large scale-governance failures, that gets you into the realm of politics. So I wonder if there are any ideas we can pinch from leafing through a few books on political theory.

A bit more background: a couple of things that we’ve done in the last five years. The failure of PIN entry device tamper resistance: it turned out that devices that were certified to be secure weren’t, and a couple of bad guys got access to a warehouse in Dubai where PIN entry devices paused to catch breath on route from the factory in China to the distribution chain in Europe – and put wicked electronics in them. They got caught, they got arrested, and they should have been tried last October. But they got off because the banks would not bring evidence against them. The certification regime is still as broken as ever, nobody has the incentive to fix it; just pretend that things are secure when they’re not.

Then there’s the No-PIN vulnerability, which we talked about a couple of years ago; one bank tried to fix it and then abandoned the fix. Two weeks ago I was at a Payment Systems Economics Conference in America and the chap from the European Payments Council was speaking. So afterwards I asked him, “Well what about all these EMV vulnerabilities, when are you going to do something to fix them?” He’d been talking about how the EPC would help governance and the payments base. No, he didn’t want to know. He didn’t even want to discuss the topic; he said, “that’s the banks’ problem, not our problem”.

So this tends to convince us that economics and politics are often too hard. Another of the inputs to this thinking was a wonderful talk that I heard Eric Rescorla gave at Indocrypt 2011, last December. He said, why are all the fixes to
TLS, in his words, “stone knives and bearskins”? You’ve still got all these attacks like Bleichenbacher’s attack, and Klima’s attack, which should have been fixed by moving to another ciphersuite with OAEP. Instead they fixed it by messing around with error messages. MD5 collisions – dealt with by sequence number randomisation rather than moving to SHA256; BEAST, well don’t even ask! And even things that were anticipated well in advance, like AES, for which plug-and-play design provision was made, they’re still not there on almost half of the servers on the Internet. What’s happening is that you’ve got two sided effects which are so serious and the scale is so large that you end up having to do one-sided hacks. There just aren’t the appropriate control points where you can win, and challenge, and contest what’s been done at the moment.

OK, so where do we get into politics? Suppose you have a benevolent monarch who could mandate upgrades. This is presumably how you would do TLS if you had a world government. A world government would just say, TLS 1.0 is evil, and as of the 1st July anybody caught using it will be dragged off in handcuffs. Now the problem that we have is that many of the failures of protocols, APIs, and security architectures, result from lobbying. A good example here is the expansion of the CA universe from three firms to 600 firms, which led to all the problems that we had with Komodo, and Diginotar, and others. And the problem we have here is that if you had a world government then the world government’s court would be absolutely chock full of lobbyists, and the place would be even bigger than DC and there would be even more lawyers, there would be even more corporate officers, and there would be even more shining parties and grand lunches. And the lobbyists would tout the mark 2, right? Because lobbyists operate best where there’s a concentration of power. So the insight is that this is the crypto equivalent of “power corrupts”, and “absolute power corrupts absolutely”. So if the W3C really could dictate protocols then you would see it starting to rot in the same way that the national capital of any powerful country starts to become infested with the lobbyists.

So what sort of governance evolution might we expect in the protocols world? What sort of stuff gets done in politics to stop governments rotting, to see to it that countries persist, not just over a generation or so, but over centuries? Are there any ideas that we can pinch?

Well when you read through your primer on political theory you see that human governance systems have tended to evolve through a number of different models. There are dozens and dozens of these, and there are different political theoreticians who have put forward different taxonomies, but wherever you look you can find some rather interesting and suggestive ideas. For example, as soon as we have animal husbandry or agriculture, you see the rise of chieftdoms where hunting bands would coalesce into a larger unit and come under the control of one particular guy and his family. And this is, if you like, early ARPA-NET, run by a guy in California, or local sysadmins at your local computer laboratory. There’s a boss sysadmin who is in effect the chief of that particular chieftdom, and who resolves all problems.