Metadata of the chapter that will be visualized in SpringerLink

Book Title	Security Protocols XXV	
Series Title		
Chapter Title	Reconciling Multiple Objectives – Politics or Markets? (Transcript of Discussion)	
Copyright Year	2017	
Copyright HolderName	Springer International Publishing AG	
Corresponding Author	Family Name	**Anderson**
	Particle	
	Given Name	**Ross**
	Prefix	
	Suffix	
	Division	
	Organization	University of Cambridge
	Address	Cambridge, UK
	Email	ross.anderson@cl.cam.ac.uk

Abstract

Ross Anderson: Well if we have to reconcile multiple objectives, game theory suggests that there are two ways of doing this: you can use politics or you can use markets. You can cooperate or you can fight. If you want to get something you can't produce yourself, you either produce something and trade it, or you go out with your friends with pointy sticks or with ballot boxes and take it some other way. Game theory gives us at least the beginnings of a framework for understanding how people make these choices.

Reconciling Multiple Objectives – Politics or Markets? (Transcript of Discussion)

Ross Anderson(✉)

University of Cambridge, Cambridge, UK
ross.anderson@cl.cam.ac.uk

Ross Anderson: Well if we have to reconcile multiple objectives, game theory suggests that there are two ways of doing this: you can use politics or you can use markets. You can cooperate or you can fight. If you want to get something you can't produce yourself, you either produce something and trade it, or you go out with your friends with pointy sticks or with ballot boxes and take it some other way. Game theory gives us at least the beginnings of a framework for understanding how people make these choices.

For the past 25 years, this workshop has been about seeing protocols breaking as they evolve, and I think one thing we've learned over the period is that this is about power. It can be economic, or it can be political. In previous workshops, we've touched on this. In 2012 for example, we asked whether democracy calls for a loyal attacker, like a loyal opposition; I gave the example of Sofortüberweisung, the payment system in Germany that provides an overlay payment service to compete with Visa and Mastercard. Two years ago, Khaled and I talked about crowdsourcing social trust.

What we put our minds to this time is whether there's a more systematic way of modelling the politics of protocol change that's a bit north of basic game theory – fairly general, but gives us something that we can actually talk about. The inspiration comes from a chap called John Groenewegen who's a recently retired institutional economist at Delft, and who studies innovation in the electric power industry. He's come up with a model (which is too small to read here) and in any case is an inspiration rather than something we're going to use directly.

Last year at Dagstuhl, we brainstormed a bit about this with Richard Clayton and one or two other people, and we simplified it to a four-level innovation stack. This is taking away the industry-specific stuff from Groenewegen's model. At the top layer, you've got cultures, values, norms – civilization, call it what you will. This is the thing that persists for hundreds of years, and changes only very, very slowly.

The next layer down, you've got an ecosystem. You've got a confluence of economics, of politics, of business. This takes place over a period of decades. Examples of ecosystem change: collapse of the Warsaw Pact; Britain joining the EU in the 70s; Britain leaving the EU in a couple of years time. That's the scale of the ecosystem, of how things come together on a scale between culture and organisations.

F. Stajano et al. (Eds.): Security Protocols 2017, LNCS 10476, pp. 1–14, 2017.
https://doi.org/10.1007/978-3-319-71075-4_18

And then you've got the everyday rules: the organisations, the contracts, the networks. This is where you get change on a period of perhaps a decade, that it might take you to build up a company, to establish a new protocol, to establish a new way of writing software or whatever.

At the bottom, of course, you've got individual actors. The things that we do every day, for and to each other – habits, routines, transactions – which may be mediated by markets or by manners.

The obvious thing here is that the time constants change between layers, and that crossing up to the next layer is hard. People try and build their businesses into ecosystems. A very small number succeed: IBM, Microsoft, Standard Oil, James Watt with his steam engines. He didn't get to control the ecosystem, but certainly the steam engine changed the global trading ecosystem because it made ship transport rapid and reliable.

If we use this as a framework, can we start to classify changes in protocols? I think that the usefulness of such a model is that it does give us a handle on the kind of protocol changes we've been discussing here over many years. ATM encryption is designed for single banks by IBM and some other companies; it extends to multiple banks by Visa; the company becomes an ecosystem; in the process, it acquires the complexity and we get the API attacks. EMV is an evolution of the same ecosystem and suffers from the same birth defects: too many legacy banks; too many legacy national networks; too many features; nothing like strict central governance. You get No-PIN attacks, pre-play attacks, and so on. Features plus institutional economics breaks the assurance, and this we can think of as a hallmark of when a company becomes an ecosystem. Or we could talk alternatively about how Windows APIs became horribly complex as Microsoft developed its ecosystem, and they were used in various lock-in and other plays. This is the same sort of thing going on.

Case two. Protocol bugfixes. We've seen a dozen attacks on TLS in the past 15 years or so. Kenny Patterson has some information collected on this. Whenever you find a new timing attack, or error attack or session resumption attack, then you have to fix it at one end, because there's still a few percent of shoppers using Internet Explorer version 6, and merchants are not prepared to say goodbye to their business. People like Eric Rescorla have written about this at great length. About how you end up being able to tweak open SSL code but not architecture, because that's the way things work once you get these two-sided market effects going. If you're going to talk about protocol evolution, this brings in mind the debate you have in biology between punctuated evolution and gradual evolution. Or as they say in zoology, 'the creeps versus the jerks'. This suggests that when we come to protocol evolution, these two-sided markets effects put us solidly in the category of punctuated evolution. At the level of business dynamics, you can see these as being minor skirmishes to defend an ecosystem – which, in the process, make it more rigid and in various interesting ways less adaptable.

Case three. Protocol tussles. See our paper on Sofort in 2012. Another example: Android Pay. Another example: SSL/TLS vs. SET, STT and SEPP, if you go back to 1996. This is standard incumbent versus challenger play, which you

see written about at great length in Shapiro and Varian's classic book. What's happening here is that you've got all-out wars over ecosystem boundaries or mechanisms. Will it be IBM or will be Apple which controls the desktop – and all the things that come from that? This is something about which very large amounts have been written by people who write books on technology policy. Maybe we can just learn from these books and don't have anything to contribute ourselves.

Well, maybe not so fast, because in the protocol world, we've also got this interesting case of protocol complements. Jim Bidzos in the late 1990s realised the revenue from Public Key Partners was about to tail off because the RSA patent was due to expire in 2002. What do you do about that? Well, you set up Verisign, and you sell this wonderful idea of the certification authority, and you arrange that everyone needs to go and pay $10 every year to refresh their certificate. At the time, if you were around, you would remember that people got very, very bullish and bubbly about the prospects for Verisign and its former competitor Baltimore. Baltimore got into the FTSE 100 stock index by promising investors that within a few years, everyone would have to pay £10 every other year in order to refresh the public key certificate for their toaster. Well, the Internet of Things is about to happen, and perhaps you'll see that coming along.

Then, of course, you had this huge big fight whereby the spook agencies wanted to get their certs in too. There were big debates over whether, for example, the Turkish government's certs should be in software shipped in America and Britain, and Iran being excluded hacked Diginotar – and you've got the flight to quality and certificate pinning and all the rest of it. Now we perhaps have a good view of this fight, but it's an odd and interesting fight, because it's a fight over complements. If you've got an open ecosystem, which you might roughly call TLS, how do people make money? We fight about the secret sauce that you've got to have alongside it in order to make it all work.

How might the Internet of Things change things? Much could be said about this. Let me define an Internet of Things, and I'll use the capital T for Things. This consists of a microecosystem of a Thing, which is an object that has got a microprocessor and software and communications in it, which communicates to the cloud, which communicates to an app on your phone. So a Thing with a capital letter is a thing that you can control from your phone with the assistance of some third party who may or may not sell your information to the spammers.

So what can we predict with protocols here? The interesting thing about the Thing is that all of a sudden the dominance of the global ecosystem of TLS is shattered. There is no particular reason why your Things should talk to your phone through the Thing vendor's cloud using a standard protocol, except for the fact that there exists an API to call it – it's a few lines of code, you don't have to think, and so on and so forth. But the barrier to innovation is now very, very radically reduced. When you think about it, perhaps the only thing that says that a Thing still has to have an involvement with TLS is whatever ad network you're using in the mobile phone app.

Paulo Esteves Verissimo: I missed the point. Why would you not need standardised protocols? Things can be made by a lot of different kinds of firm. Standards are something you want.

Reply: This is the point that I'm coming to next, because the original idea that many promoters of the Internet of Things seemed to have had, is that things would talk to each other – and thus the vendor of the Thing would be deprived of the opportunity to monetize them. Why should anybody have the incentive to allow Things to do something as stupid as talk to each other is not entirely clear. My worked example is the HAN – the home area network. We were promised – gosh, at least 10 years ago, perhaps 15 years ago – that we would have home area networks where your fridge would talk to your toaster to your immersion heater to your boiler, and through your electricity meter to the network. And the network would be able to say, 'There's not an awful lot of wind at the moment, and the clouds are blocking out the sunlight to the PVs, so we would really like you to use less electricity, and I just put the price up to 30p' – whereupon your home would intelligently turn off the immersion heater, and start cycling the freezer a little bit less aggressively, provided it stayed below whatever threshold it was and so on. In other words, the idea was that you would have adaptive response for all sorts of worthwhile purposes in the home.

That failed to happen. Completely failed to happen – because when the European Union brought in the Electricity Directive in 2009 they put in a mandate for smart meters but they forgot to put in a standards mandate for home area networks. So when each member state transposed it, they adopted different standards, and so if you were Mr. Samsung, you don't want to make 27 varieties of smart fridge – especially when that would undermine your chance of monetizing any information from the fridge. So you will see to it that your Samsung fridge will talk to your Samsung server and to a Samsung app. Similarly, when Canon sells you a printer, that will talk to Mr. Canon's servers in Japan, which will talk to a Canon app, and so on and so forth.

The necessary preconditions for creating an ecosystem within the home were never even remotely close to being created. The incentives are all in favour of fragmenting these protocols rather than creating an ecosystem in which one particular protocol predominates.

Unless of course, you get a powerful player who decides otherwise. At present, of course, the player in that market is Google with Nest. Because Google, through the app store, has got some influence on what apps do, and if Google becomes a dominant player in managing home energy, then perhaps – at least this is what the guys at Google think – they can get the protocols around Nest adopted by vendors of devices, and they can get the platform economics going that way. From the point of view of protocols, this is an interesting worked example, or rather, non-working example. Yes?

Paulo Esteves Verissimo: Well we have one new mobile phone protocol, which is exactly is the combination of three existing protocols. Do you see something similar happening here? Do you just see two or three or maybe 10 protocols,

which can then be merged into one conglomerate protocol and then to something where people start thinking about the next level?

Reply: Well, this brings us back to our perspective, which is the next slide. How does our perspective help? Recall the innovation stack. At the top, there's culture, values, norms. Controlling that is the aim of all good dictators. How do you get your worldview across to everybody? Then there's the ecosystem, which is what you're trying to do if you want to create an environment for home innovation and you're someone like Google.

How do you get to control an ecosystem? By controlling something at the next layer down. Contracts, organisations networks. You've got a killer app, for example, and if that killer app is controlling the home thermostat – the Google idea, maybe that's your way in. If it was controlling the buying and selling of energy, your gas meter, your electricity meter, and perhaps payments that you got from the sense of turning your immersion heater off, then that would have been another platform on which you could have made a bid for ecosystem dominance.

Now how does tech in general make a difference? In the old days, stuff used to bubble up at the human level. Ideology would be something that evolved out of zillions of conversations between individuals; or you could have an individual leader, a military leader, or a religious leader who would get a tribe together, and the tribe could become a nation, and then it could become a huge movement and then it could become a worldwide religion. It's an innovation system, but in a non-technical sense. Now what's happening is that technology enables this, and protocols – and in fact software in general – can be seen as an enabler of this kind of social innovation.

What one's doing with creating a protocol is trying to build out an idea into a firm or to build a firm out into an ecosystem. What are the conditions under which a protocol may enable you to do that? Remember the incentives facing individual actors. Actors want to maximise impact. They want to be rich, famous, or both. If they're pure Darwinian operators, they want to have large numbers of grandchildren but we've got other metrics too nowadays. And the strong and the smart succeed and then try and limit innovation by others. How can a protocol empower actors? How can a protocol enable you to turn your business into an ecosystem or turn your ecosystem into total world dominance?

Let's step back a sec, and look at recourse. If the theme of the workshop is where people have got conflicting objectives, then what sort of actors might adopt a protocol? Well, competition in the business sense is an obvious one. Sofort started off when merchants got fed up paying 2.5% to Visa and MasterCard, and somebody got the idea, 'We'll let them do bank payments directly, pay less money to Visa and MasterCard – and let us take a commission of the savings.' Another example is crowd innovation: insulin pumps, for example. You can buy insulin pumps if you're diabetic, which will automatically pump insulin in response to readings from a glucose meter, but these are rather crude devices, and some people like to reprogram them so that they can get finer grained control. In order to do this, they have to hack the pumps. This makes the pump

vendors worry about liability, and raises all the issues about whether the protocol should allow a certain amount of latitude for innovation in the first place.

Or look at disputes. If things go wrong, people tend to go to the government, and the government can offer redress after the fact. You sell me a rubbish thing online, I go to the county court and get an order against some of your money. Or escrow before it: I decide to buy some drugs from you on Silk Road, and so I hand my money to Dread Pirate Roberts, and when I confirm that the drugs have been received and that they burn rather satisfactorily, Dread Pirate Roberts releases the money to you. This can be a governmental arrangement, a private arrangement, various kinds of arrangements – but there are ways in which you can put redress into a protocol.

The third sort of actor that you find where people adapt a protocol is for industry to specialise a protocol for their needs. You take something off the shelf and you adapt it to what is specifically required for cars, for healthcare or whatever.

From looking at a number of cases like this, one of the things that we begin to suspect is that a key factor for success in protocols is: does the protocol support innovation of some kind? Is it possible to take the vanilla protocol, and turn it to another use? We already understand this from software platforms. The reason Bill Gates has got an awful lot of money is that the Windows platform that he built, and the DOS platform before it, enabled anybody to use the existing deployed base of PCs to write new kinds of software. So you could write a new card game. You could just as easily write control software for a sawmill. In neither case did you have to crank up a factory to make all the computers from scratch. So a key thing here is that to get people to adopt protocols, you have to create the ability to adapt protocols.

The lesson that we then get from the failure of the home area network idea in Europe is that the regulators should have put a protocol there, and they should have done it first before they worried too much about the details of the mandates, about which country would have to see to it that how many of its population adopted meters for gas and/or electricity by such and such a date. If you had provided the platform in which people could have innovated, then there was some chance that you could have had app pull rather than legislative demand push.

And in fact if you look at the Daily Telegraph today, you'll see that there's an extensive article on page 23 and also on the website about how the whole smart meter episode is running out into the sand. The smart meters aren't working right; they're not interoperable; if you change suppliers the meter becomes unsmart; you then get an email telling you to go read the meter; and a smart meter is more difficult to read than a dumb meter because you've got to press half a dozen buttons in order to actually get out a reading in numbers that you can then copy on a piece of paper and carry indoors to type into an email to the power company. Yes?

Paulo Esteves Verissimo: Going back to the original thing. You talked about access conditions. Then you seem to talk about HANs as a thing from the past

or something failed. You seem to point to the regulators that should have acted. I agree with what you say, your competition has made standards work, and most of the time that's how it works.

Reply: Mm-hmm (affirmative).

Paulo Esteves Verissimo: I don't think it's too late for HANs, because actually I think the whole thing is just starting. HANs, people talked about them for ten years, but it's actually, with the smart meter thing and with the concept of a network ... So there's a network that gets to the smart meter, which is the gateway. Then, that the market make the gold. I can see that working on both sides.

Reply: Well sure, a lot of people think it's a matter of religious preference, HANs should exist, but HANs don't exist. In different countries we don't even have agreement on what the underlying radio platform should be. Should it be a low-energy Bluetooth? Should it be a variant of Zigbee? And the thing that breaks that roadblock may very well be Mr. Google rather than bureaucrats in Brussels. But the point is that the people in Brussels were trying to pull the wrong levers when they said, 'Let's have a deployment mandate.' They should have engaged the tech community in the right way to begin with to see to it that there was a way for information to flow backwards and forwards.

Paulo Esteves Verissimo: These problems happen. See the car makers. Car makers are very powerful companies. A few of them think, 'Oh, no. I'm going to do it my way,' and so on and so forth, but they haven't really. There's a substantial level of standardisation of components, not just electronics, so that they can be interchangeable, because obviously that's the way to recheck the system.

Reply: Yep.

Paulo Esteves Verissimo: That's what I will believe will happen in houses, but it's probably not mature now.

Reply: Well, I could talk some length about safety and security in cars, but that's a different talk. We have peripherals in progress about that, and I'm happy to talk about it offline. For current purposes, here's the punchline. That platforms for innovation are really the key here, because if you want to turn your product into an ecosystem, let others innovate on it. Tuomas?

Tuomas Aura: I have been wondering about this, why we don't have any HANs. There's lots of proposals for home networks and home hubs and nothing really happened. There was the Xbox, and then there are the home routers, and I was googling about, and proposals for things that are smart. It seems that the problem is that they all got closed protocols.

Reply: Yes.

Tuomas Aura: And –

Reply: That's exactly the consensus in network economics.

Tuomas Aura: Is the problem you're suggesting is that someone like a big authority in Brussels, comes up with an open platform? Or –

Reply: No.

Tuomas Aura: Or do you think there's anyone who can make this open platform?

Reply: Okay, the purpose of this talk is to explain what's going on. The entrepreneurial action that follows from it is separate. If you believe that you can do a startup that will make home networking work, then these are the sort of things that you need to think about when you're planning that startup, right? And here are some examples of how stuff succeeded. You've got Windows, Linux, and Android have done well by creating two-sided markets that bring app developers in touch with users. You've HTML, right? which extended this to web developers – and Facebook, which extended it to everybody. And all of these are about innovation of one kind or another.

Now, the existing examples which allow greater or lesser amounts of innovation – such as ATM networks, contactless, and of course TLS – can also be seen in this light. ATM networks turned out to be adaptable enough to bring tens of thousands of banks on board and to extend from ATMs to point of sale, to subway ticket machines and all sorts of other things. This is, I say, a framework in which you can start assessing how a new protocol might be useful, And if it isn't, don't waste your money on a startup to produce it. Paul?

Paul Wernick: What I'm seeing here is a situation not unlike system dynamics, which shows who influences what in terms of arrows connecting things, because there are a fair number of actors around, and they all have different degrees of influence on each other. I think that would be as helpful as thinking about specific examples, because I think it's a generic problem that goes beyond computerised technology.

Reply: Well sure, it goes beyond computerised technology, but I prefer to see these things in terms of network economics. Partha, you had your hand up.

Partha Das Chowdhury: I can see this ability to create a backbone that can talk to various (alien) devices over a VN. What concerns me is how do you fix liabilities. Consider the case of the Mirai botnet, where the CCTV cameras were manufactured in a different country so the manufacturer is not liable to laws in that country where it was being used for an attack.

Reply: In the specific case of the Xiaomei cameras, the customs man at Rotterdam should have sent that container back to China, because if you put the CE mark on a product, you're saying it adheres to all applicable standards. And we do now have a couple of ISO standards on vulnerability lifecycle management. So if you ship a CCTV camera that's got an embedded factory root password that you can't change and there's no means to upgrade the software, then such a device should a priori never be sold on the soil of the European Union. It should not be allowed in at the harbour. We've got the laws, right? Nobody's enforcing them because nobody understands this yet. But believe me, that's going to

change. Until you get a catastrophe, nobody pays attention. And perhaps people not being able to use Twitter for five hours was a sufficient catastrophe (laughter) that the customs officials will start doing their job. At least we'll certainly hope so. We hope it's not going to take any fatal accidents before they get off their behinds. Joan?

Joan Feigenbaum: I have an answer to your, 'Where might new protocols be useful?' Electrical outlets. Something to prove to, so we can innovate our way out of having to carry adapters around every time we take a flight overseas.

Reply: Yes. If everybody ends up using Mac adapters!

Joan Feigenbaum: Well, Mac adapters are not the most convenient things, so it would be wonderful if some great innovator could get me out of having to take all these adapters everywhere I go.

Sven Uebelacker: Actually, I wanted to make this argument for exactly the opposite, and say, are protocols irrelevant right now? Because we are so used to translating one protocol into the next one. And MAC adapters and even the new IP developments work this way. You just combine an antenna array with software, which makes your mobile work.

Reply: It depends how you define 'protocol', and I'm going to come on just now to show that we can think of that perhaps slightly more broadly for a virtual viewpoint.

Virgil Gligor: So I agree with you that protocols should be platforms for innovation. In terms of home area networks I think people didn't find the business case to start with –

Reply: Exactly.

Virgil Gligor: And if you look at the building automation, where there is a lot of innovation, it's all based on closed networks and it's all a handful of producers that don't interoperate with other, very fragmented and not much innovation ... public innovation. There is innovation for example within Honeywell, how to manage these large buildings, and ZMax and some others – but not in terms of open protocols. They eliminated a lot of manpower, a lot of salaries, everything else. So there was prior activity. However, we did not see that all that clearly in home area networks.

Reply: Well this is well known if you look at industrial control systems protocols. Where protocols like DNP3, for example, take about 40 years to change because there are too many powerful stakeholders. So we cannot put authentication into SCADA systems before about 2040 and there will still be plenty of the current legacy being used then. So we have to reperimeterize. And that's just an example of the accumulation of protocol tweaks causing fossilisation and the two sided-market effects as well.

On the home area networks side, bear in mind that despite Bill's huge power and wealth, Microsoft was never properly motivated to cause printers to work

properly. Right? Because Microsoft didn't make money out of printers. Printers were a pain. Printers were things that you had to have hundreds of in a shed in Redmond, so that you could test out all your patches every patch Tuesday. They're a source of pain rather than a source of pleasure. Is it any surprise, therefore, that when you go and buy a printer nowadays, the printer doesn't talk to anything except a server in Japan? That basically you have to email a document to someone in Japan that you don't know, from your mobile phone, in order to have it come out of your printer in your kitchen?

Is it any surprise that people are abandoning physical printing altogether, now that it's largely possible to do so? Printing was something that the modern world never managed to engineer properly, and we may very well find that because of the impossibility so far of finding good HAN protocols that make business sense, that all sorts of other current activities will just die – because nobody can make enough money from them.

Virgil Gligor: In terms of home area networks and home automation, entertainment systems evolved quite a bit – Xboxes and the like. Very successful. Microsoft, not being a hardware company, invested in Xbox and did fantastically well. But that was the limit in terms of penetrating the homes. The question is, what's the next boundary? What's the next piece of innovation that would allow the Microsofts of the world to penetrate the home? Or the Googles or the Apples?

Reply: Well, let me go on to the next slide. Thinking about scale, things like Windows, Linux and Android enabled innovation by people who knew how to write software. Let's say to a first approximation that's a million people. It might be five million, ten million, I mean, who's a programmer? Lots of people write occasional bits of code. It's, in order-of-magnitude terms, probably in the low millions worldwide.

HTML comes along and suddenly the number of people who benefit and who are empowered as producers goes up by an order of magnitude. Because it's a lot easier to put together a website that sort of works than it is to write a program that does something sort of useful. Okay, so we get an order of magnitude scale-up.

And then something that perhaps people haven't particularly thought about is when social networks came along – Facebook – that gives you a further two orders of magnitude in scale-up, because for most people in the world, maintaining their own website is too much bother. HTML looks too weird and the tools that you can use to write it are either too difficult, like emacs, or too fiddly if it's a proprietary graphical editor. So isn't it what people actually want – to open an account, drop in a photo, recruit a few of your friends and you're fine. Takes you five minutes.

So this is a way of bringing innovation to the masses. What we've also –

Fabio Massacci: But it's not the same type of innovation –

Reply: Yes, I know.

Fabio Massacci: Uploading a photo's not the same as writing a usable program.

Reply: Yes, but then it enables different types of innovation, so that the existence of things like Twitter, for example, empowers all sorts of people. Including some people that we might prefer not to have been empowered such a certain New York property developer. Now, if that New York property developer had to sit down with a box of punch cards, and encode his entire campaign in FORTRAN, then perhaps –

Virgil Gligor: We'd have been better off.

Reply: Or he would at least have learned to be a little bit more careful and meticulous with the way he organises information.

And what we've also found is that the old idea that ideology was something that evolved out of gazillions of conversations is perhaps being supplanted by mechanisms whereby you get statistical machine learning from crowdsourced data. Which of course brings its own issues of autonomy and, if you like, who's actually taking control.

You then get other side effects such as the fact that political debate moves increasingly from public spaces to private ones. And all the various strange things that we had this morning on the radio about MPs saying, 'X should be done and Y should be done about' – what were they talking about? They were talking about ticket touting. And the people who are obviously lobbying for laws to prevent secondary sales of tickets, were people who could've solved the problem perfectly easily with their own websites where they sell concert tickets, by adopting even ten percent of the smarts used by Ryanair.

So what we're seeing is a dislocation as the world goes from innovation done by people – talking about stuff, doing stuff in old fashioned human ways – to technologically empowered innovation, whereby you go and you collect your supporters, your customers, whatever, by means of platforms, by means of protocols. And then use them to build your empire.

So, anyway, that's the kind of framework for thinking that we've been trying to develop. What we'd like to suggest is that people start thinking about slightly more socially difficult test cases.

Now, as a computer scientist, your first reaction is to look for problems that might be easily soluble using theoretical computer science concepts or small-scale engineering. For example, there's a huge debate about how we get new protocols to react to emerging scale issues – things like Bitcoin. If Bitcoin can't process enough transactions per second, and now there's a day's worth of transactions and the thing's breaking because it takes you a day to get your transaction though, do you increase the block size? Do you do something different? Do you set up a separate blockchain?

But when we look at many of the problems people wrestle with, they're about dealing with what lawyers call incomplete contracts, where people make agreements with each other without always knowing the exact details in advance. When you contract with a builder to build your house, they may very well find

that there's a sewer or an electricity main in the wrong place, or that there's unstable soil or whatever, and you end up having to go back and renegotiate halfway through.

So if you're a private actor, you can fix this at small scale by specifying an adjudication in the contract. You can write a contract with your builder – and in fact your builder will usually do this if you buy a house in Britain – saying that if anything comes up because of any of the following things that can go wrong, there's a process for adjudication and a procedure to go and find someone to adjudicate on it.

If you're an entrepreneur, you can try to provide this scale. And one of the reasons that the Silk Road worked is that Ross Ulbricht, the Dread Pirate Roberts that set that scheme up, set up an escrow system so that people buying drugs would leave the money in escrow for a while, so that you can see whether the drugs arrived or not. That plus a reputation system enabled the thing to work while underground markets had not worked previously.

Social adjudication can also work. Examples perhaps are Grameen Bank. And these are examples where innovation has got the chance of breaking out of narrow computer science confines and perhaps coming up with something interesting and useful. Paul?

Paul Wernick: Paul: The example you gave of building a house is quite interesting because the Guardian has been pushing recent examples where people have had great pains getting builders to do what needed to be done. Like problems building houses are inevitable. So the power seems to be with the builders. The adjudicator is an organisation funded by, and returning its profits to, the builders. And the poor house buyers were obviously stuck.

Reply: Yes well if you sign a contract like that, then more fool you.

Paul Wernick: But to build a house, that's the contract you sign!

Reply: Well, build your own then. Or alternatively, run for parliament and change the rules. But you'll find that the house builders have got more money and more power.

But the main message here is basically this; we started off seeing protocol security as being something that was fundamentally logic and mathematics. The BAN logic was hot off the press when the first of these workshops was held 25 years ago...

Bruce Christianson: 24 years ago.

Reply: I stand corrected! And then we moved to engineering. We talked about things like robustness principles – can you do something a little bit more general to deal with protocols, where proofs might, for various reasons, be inadequate? From 2001 we've had economics, fixed versus variable costs of protocols. Then we've had things like psychology, social trust. Of course, that's also a bit about crowdsourcing.

And so what I've tried to suggest today is that approaches from institutional economics might give insights into the political economy of protocols. That this

isn't just a straightforward matter of the welfare theorems or of network externalities. It also matters what sort of institutions you're trying to construct, what sort of scale they are and what the relative time constants are.

And societies, if you see them as machines, are machines with a whole lot of different wheels which turn at a whole lot of different speeds, and the game that smart players are usually trying to play is to power their innovation up from the rapidly moving wheels of individual action, through corporate action, through ecosystem control, and finally, perhaps for a very few lucky individuals, world dominance.

Now, in order to do that, I'm suggest that you need to think about how you empower others to innovate. And perhaps the interesting question in the theme of the workshop today is, 'Can we support innovation in dispute resolution?'

That is a bigger and deeper problem than just trying to preset some tradeoff between, for example, privacy and law enforcement. It's a bigger and more general problem, and if we see it in terms of enabling people to negotiate, where there is the real capacity to negotiate on both sides – right? So I'm less interested in cases where states can compel, or a house building oligopoly can compel. While these are of political importance, there's relatively little play in them from the point of view of a technologically mediated platform that enables stuff to go forward. Insofar as we can contribute by engineering innovation, it's likely to be in this mucky, sticky bit in the middle where you're trying to deal with dispute resolution in the real world, where things aren't perfect. And workable second-best solutions may actually bring real progress.

Tuomas Aura: Hello, I just wanted to comment on this. I think this kind of thinking about the real economics and politics around it is really important. So I think we don't generally mention that in the research papers, but hopefully take it into account to some extent. But then, when I give to my students a design problem for security architectures or protocols, many of them propose things like, 'Let's use the security cards for registering students,' or an IOT application that changes the field in IPSEC protocol. And these are things that we cannot do when we design a system. We are stuck, we can't deal with the phone operators or change the SIM card properties or we can't change the norms or standards just for our application.

But that's not always obvious in even these basic things, it's not always obvious to new people and students who come to that area. Even going further back to the basics of what's possible to do with productive elements and innovation, it would be useful to have that preconception.

Reply: That's basically why I wrote my book – so that students coming into this field could have enough concrete cases to perhaps get some feel for what generally works and what generally doesn't. Of course, that's only a start and there's much more to go. Mark?

Mark Ryan: Can you give a bit more detail about what kind of innovation you're mentioning? This space of law enforcement versus privacy? What can the individual do?

Reply: In the space of law enforcement versus privacy, perhaps there's no play in that situation at all anymore. Certainly in Britain, the government has declared itself to be omnipotent and omnicompetent, and has declared the debate to be over. Insofar as there is a debate, it's going to be about the situation in the rest of Europe where the European Court of Justice has ruled against data retention. It's going to be in the USA where, for the time being, for better or worse, most of the data to which UK police forces want access happens to be located. And so if you want to be a privacy activist in the UK, you have to work with European and American bodies. I do, I'm off to the EDRi General Assembly at the weekend and I'm also on the advisory council of EPIC. One has to see these things in the international context.

Now, there, I suspect it's mostly about political lobbying and action. But my point here is that there are potentially many other areas where engineering innovation can bring real benefits. We have seen many cases such as the eBay and Amazon reputation systems, where reputations can do good. And there have been other cases where perhaps it does harm by locking people in to exploitative monopolies. Understanding this is important if you're to find the opportunity to do a startup that does make a positive difference.

Author Queries

Chapter 18

Query Refs.	Details Required	Author's response
AQ1	Please confirm if the corresponding author email id is correctly identified. Amend if necessary.	
AQ2	Per Springer style, both city and country names must be present in the affiliations. Accordingly, we have inserted the city and country names in affiliation. Please check and confirm if the inserted city and country names are correct. If not, please provide us with the correct city and country names.	