Towards Flexible Credential Negotiation Protocols

(Transcript of Discussion)

Pierangela Samarati

Università di Napoli “Federico II”, Italy

The problem we are looking at is how you specify, enforce, and communicate security policies in a world where people, computers and objects move, change identities, present themselves without identification or authentication and still want to interact and access services.

Brian Monahan: Couldn’t you send the policies to the client, get them to do the computation and send back the proof, which is then used, so then you can check? That’s also nicely private as well.

Mads Dam: Firstly it’s dangerous to send off the policies which regulate access to the client. Second point, how do you make sure that the information that you sent away doesn’t reveal information that you don’t want to be revealed by a query?

Virgil Gligor: You can always map it into a score.

Ross Anderson: Absolutely, a credit rating.

Richard Clayton: If you are willing to disclose your business practice.

Ross Anderson: You can borrow twenty thousand pounds from me if your credit score is greater than three thousand two hundred. What’s the algorithm? Not telling you, it’s a secret! [Laughter]

Brian Monahan: But you still give them some information.

Frank Stajano: So wouldn’t this be a good place to use some secure multi-party computation where nobody gets the result? Then neither of the parties would be able to get the kind of answer that they may have and agree. So, if it’s false then nobody knows what the other one was putting in, but if it’s true then they know about everything.

Richard Clayton: It depends how you do it. If you’re a shopper and you go into a shop, you don’t tell the person behind the counter what your income and outgoings are so you can see whether or not you can have a new sofa, a third party does that, the credit rating organisation. However, you still have to give your personal information to the credit rating people, so although it may be a third party to the shop, it’s not a third party as far as you’re concerned.
Frank Stajano: If you’re using a third party, I would suggest some protocol where they’d be able to do the computation but the party who gets the result is the one that actively runs services.

Ross Anderson: There is a strategic tension here. Usually what you’re trying to do is price discriminate, and this is not what the customer wants, unless he’s very poor. If the customer is not poor, then you do not have a collaborative environment, you have a hostile environment. That’s the fundamental problem here. The client wants to appear to be poor, and the server wants to find out if he’s lying so he can charge him more.

Larry Paulson: How to get a bargain if you’re shopping in a foreign country, assuming you know the native language. Ask in English: “how much is this shawl?” The girl who’s serving doesn’t know how low you will go, so she asks the boss in her native language the lowest price he would take for it. Then you can bargain down to that price.

Matt Blaze: I’m not sure that we’re not making a mistake here. The examples in this discussion have been security protocols that are partially implemented as relatively slow, off-line human intervention processes; such as applying for a mortgage, and so on. There’s considerable cost for the client so you can’t repeat it over and over again. The mechanisms that you’d actually be describing are, in contrast, on-line services, where the costs of reissuing a request from a client are in fact very low and you could probably do it over and over again. I understand how keeping your policy secret in the slow human-intervention type of protocol may be a feasible thing to do, but I’m less persuaded in the actual examples you’re giving that it is feasible to keep aspects of the public policy secret. This is because the client can issue so many requests with different parameters, that they may be able to quite accurately reverse engineer your policy. So one has to be very careful in the way one responds to the queries.

Reply: There are occasions when the policy is sensitive, but the problem here is that what is sensitive is the information I use to evaluate the policy. And it’s true you can have many attempts to find out my policy, but for instance, if I have a favourite customer to which I give a bonus of a hundred dollars, and I don’t want to tell the others because they might get upset, this is policy information. The fact that I’m giving the bonus is certainly sensitive information. By making many requests you find out my policy on each one of the customers, so you won’t be able to pretend to hold that property if you don’t.

Matt Blaze: But again one of these heavyweight protocols, where there is actual money involved in doing the transaction, results in a high cost to the client. I think that in most of the examples, where we’re doing completely automated processing in an on-line service, the ability of the client to do tweaking of the parameters, and essentially differential analysis of the policy, is quite good.

Ross Anderson: You could try and detect the differential attacks. If you’re running a website, you might see somebody drop out of buying a book a thousand