The main idea behind this talk is an idea of Giampaolo Bella from the University of Catania. The general picture nowadays is that each transfer has just one precise short-lived goal, such as for an eBay purchase, and each transfer may attempt malice aiming for personal benefit to them of money, or any kind of purchases. In the context of brief encounters, each transfer can just quickly leave one context and join another. If each may choose transfers, they can really collude towards the same malicious goal, and if they want to share the greater knowledge. But it’s more realistic, that each malicious transfer will act for his own sake, and just use the resources at his disposal, and try to attack on his own.

The question is, what is the right threat model to analyse this kind of scenario? Is a Dolev-Yao threat model which attempts collusion on chain of proof of knowledge really appropriate? And so we are wondering if these transfers can really have a static state regarding which transfer is honest, which transfer is dishonest, and if we don’t, whether we need a more innovative model where every transfer can switch from a dishonest behaviour to an honest behaviour, or vice-versa.

It might be a bit embarrassing to work on the NSPK protocol again and again, but what we need is a known protocol and a known attack that everyone understands perfectly, and we shall show a known attack that is expressed in the Dolev-Yao model, and we are wondering, what could done in a new threat model?

Our new threat model is where every transfer can attack each other. In the general attacker threat model, each transfer may act as a Dolev-Yao attacker. But an important point is that there is no collusion or no sharing of knowledge otherwise this malicious Dolev-Yao attacker will just be seen as one global Dolev-Yao attacker, and it will not be able to model scenarios where attackers are attacking each other. So this threat model might be more appropriate to an analysis of privacy in the context of brief encounters, collusion may not be practical, because there is no time to join forces, and so maybe a general attacker is more appropriate. This model is a simplification of the threat model which was introduced by Giampaolo in 2003 so this is the threat model, we have static partitioning of principals between bad transfers, weak transfers and good transfers. The bad were the attackers, the good were doing transfers following the protocols just as they are written there, and the weak are bits in-between, which means they didn’t launch attacks, didn’t participate in attacks actively but maybe passively. And maybe this threat model where each transfer may

attack each other is realistic because now it’s becoming easier for everyone to just attempt to launch an attack, for example, from the web. So we completed each of the NSPK protocols with the computation set. So in this protocol the man-in-the-middle attack proves that the nonce there is shared, and is a transfer, and so this gives the possibility to pretty much make each transfer have the ability to attack each other, or at least to try. And of course the NSPK is a very basic protocol, so we assume there was a known attack on the protocol, and we are interested in helping the original attacker to that scenario.

We also want to automate the way we validate a protocol in the new threat model. We adapted SATMC, which is a type of model checker, to capture the GA threat model and used that tool to run this experiment.

So now a quick look at the modelling. We reduce the problem of finding an attack on the protocol to a model checking problem. The property we want to check, for example, can be one of the previous attacks. And so the status of the transitions needs to be modified to support the new threat model of the attacker. We could just track the knowledge of one Dolev-Yao there, where now we want to trust the knowledge of every transfer.

Bruce Christianson: What does not trustworthy mean in that context?

Reply: Actually for the General Attacker model we suppose that anyone is not trustworthy, so this means that anyone may act as a Dolev-Yao attacker, but in the model there we give more precise definitions. So for example, we have a provision that an agent is known as trustworthy, which for our model, we just describe any transfers and non trustworthy transfers about to fake or intercept messages, as any transfers about to infer some new knowledge by either encrypting, decrypting or composing without the proper nonce.

And so in conclusion, this new threat model seems appropriate to find interesting properties in protocols, such as situations where transfers attack each other or may retaliate against each other. So we were able to express a new threat model, and to return the results that we expected from our analysis. And are doing more protocols, such as Google’s SAML protocol. So in these situations, we have clients, in this protocol we have a client who wants access to some service from a service provider; for doing that he transmits to authenticate with a supervisor, so the client receives a notification from an identity provider, and then can provide it to a service provider to access the service. So the conclusion is that the Google version of this protocol was good, and there is an authentication but it was too general to generate, for example, this authentication here can be replayed. So, for example, a service provider could just replay, if a malicious service provider managed to convince a client to authenticate and to access his service, he was able to replay authentication of the clients, and to, for example, accept the notification of this provider in the name of the client. And so we are wondering what this general attacker can bring to this scenario, for example, since we suppose that anyone is malicious, we could imagine that it could be the service provider itself which makes this transition from the clients, and their service provider, and so accessing information from the client.