Pseudonymity in the Light of Evidence-Based Trust (Transcript of Discussion)

Daniel Cvrček

University of Cambridge and Technical University Brno

George Danezis: Surely as soon as you link two pseudonyms once, then you can't take that information away from an adversary. But what you said may be theoretically possible if you could prove that you also have another pseudonym that has good reputation without revealing it, which is really I think the property you're looking for.

Vaclav Matyas: Well practically this is what we would like to see, and the only way we've discovered so far is some kind of ZKP, so that you can prove that there are links between the pseudonyms that we operate with. We don't see anything better so far, but we would eventually like to find a different approach.

Pasi Eronen: I guess you could also do something like that with some more trusted computing platform. That could be a third party that links these pseudonyms but doesn't reveal the information to anyone else.

Reply: There may be certain small domains of trust in the system but the domains are not the whole system. There are no globally trusted parties.

Vaclav Matyas: Surely some of the military wouldn't mind to introduce certain level of uncertainty in the system so that you can eventually plausibly deny maybe all your pseudonyms?

Reply: What we are proposing is the possibility to create a number of different pseudonyms not revealing the real identity of user. In typical environments there is a very small difference between the price of creating one, and let's say, two or three other pseudonyms, because you can automate the process too easily.

B. Christianson et al. (Eds.): Security Protocols 2004, LNCS 3957, p. 275, 2006.