Innovations for Grid Security from Trusted Computing
(Transcript of Discussion)

Wenbo Mao

Hewlett-Packard Laboratories, China

Bruno Crispo: But why do you need to chain the certificates, I don't understand. Usually I look for, for example, storage, and then I go find somewhere that can provide the storage I need, but why do I need a chain?

Reply: Do you mean, you do it yourself?

Bruno Crispo: No, somebody else does it for me, but in a sense when I issue a request, it's to the grid, so everybody is authorised to respond.

Reply: OK, that view says, there is a server, which can do for any. In that standard architecture, you need some superbeing staying there to serve some other people, so we come back to the point, how big the superbeing is. So many people ask for him to serve, so you need to go back to the original idea that if you buy big servers, somebody has to buy them. Here in this model mostly you have your own, OK, you are bounded, and then you can carry on. In your approach, the user need not worry, but somebody needs to worry; here nobody needs to worry.

Marios Andreou: Sorry, I'm not quite clear, do you mean the policies of the local user are applied by default to the accessing user or not?

Reply: The accessing user is mapped to the local user policy, yes. After mapping you can propagate, you need to, so, these guys don't know their accessing user at all, since it's chained, they only know this guy.

Marios Andreou: So they're applying local policy to the accessing user?

Reply: Yes. There are different ways to say the same thing.

Bruno Crispo: Probably to audit the processes it's easier to use an all-software solution. I think there is a version of Solaris that allows the role of "internal auditor" to be set so as to audit also the activity of the administrator.

Reply: Is it hardware based?

Bruno Crispo: No, it is a feature of the operating system. The operating system also builds a log that is read-only even for the system administrator.

B. Christianson et al. (Eds.): Security Protocols 2006, LNCS 5087, pp. 150–152, 2009.

Reply: OK, that's nice to know.

Mike Bond: Are you building this on top of the 1.1b of the TPM specs, or on the 1.2 TPM?

Reply: For this, year one, phase one, 1.1, in future considering science collaboration in years four and five, we need to think about so-called attestation things.

Mike Bond: How many different people's identities are you considering putting in one TPM, you were saying that people can share a TPM, I mean, what sort of numbers are you talking about?

Reply: Virtually unlimited.

Mike Bond: But the TPMs that exist at the moment (OK, the API can be implemented in anything, but) the TPMs that exist and are deployed at the moment don't have a high level of tamper-resistance. If each of them only contains one person's credentials, then it costs a lot to hack a lot of people, but if you put all their credentials in one TPM, then you have a security risk.

Srijith Nair: Can't you virtualise the TPM?

Mike Bond: No, I'm talking about the physical device, because it costs a certain amount to open up a physical device, and then having so many virtualise that device.

Reply: For the client machine, this is not a big deal, for the server, TPM is only a name, you can use really IBM crypto processors.

Mike Bond: So do you have any plans to use the TPM API inside one of those, or your own API?

Reply: Indeed we do. This year's offering, it will be for the client mainly it's not a problem. For the servers still we are considering this is an experiment, and also companies are shaping the TPM servers, and we need to see how big these TPM servers are. But in any case, TPM uses this external storage with only some handlers protected inside TPM, and where most of the things are outside, of course it becomes slower, but especially for the client market, it's not a problem at all. Yes, the idea is that for in the future, I think, if you look at this room, everybody has a laptop so for the client things you don't share a lot.

Kenny Paterson: You should also bear in mind that the MyProxy approach already concentrates user credentials inside, so the trusted computing approach in some sense can be worse than what's already done.

Bruno Crispo: What you suggested is that the identity that actually has generated in the grid map should be from the TPM, right?

Reply: Yes, our TPM does the auditing process, and so you see here, the size really doesn't matter, it's a total, and then periodically the TPM can sign the result, and store it, it should be stored outside, in permanent, persistent storage, and then auditing will rehash everything.