Digital Data Security: Management of identity, trust and privacy in a digital world

Software Group

Welcome to the podcast on digital data security. Christian Achermann is interviewing Jan Camenisch, scientist at the IBM Research Lab in Rüschlikon.

Christian Achermann: “Could you provide us with some information about yourself and your function in IBM?”

Jan Camenisch: “I am a research staff member here and I am a cryptographer. But I am also a project leader for the European project Primelife. This project deals with the protection of personal information on the internet, with the management of identity, trust and privacy in a digital world.”

Christian Achermann: “Nowadays, when engaging in online-services one often has to provide a lot of personal data. What kind of risks are inherent in this practice?”

Jan Camenisch: “On the one hand there is the risk that the data one reveals may end up in the wrong hands, either because it simply gets lost, as we keep reading in the press, or because it is misused by employees of the company to whom you reveal the data. On the other hand, it also includes the risk that the data one reveals can be used for profiling, so that for instance, if you reveal information about your self on a social network, then that information can also be used by a prospective employer to decide whether or not to employ you.”

Christian Achermann: “In the latest edition of THINK!, IBM’s customer magazine, one can read that you and your team are working on a future oriented solution to protect sensitive data, also known as the identity mixer. Could you give us some information about the current status of this project and the functionality of your solution?”

Jan Camenisch: “With this solution, we aim to address the problem of revealing too much information in three ways: first of all we are dealing with trying to minimize the data that people have to reveal; secondly we try to help users to establish trust in their communication partners online; and thirdly we try to give control over their data back to the users. Here is an example of data minimization: if you have an electronic identity card and you want to go to a bar for a beer, you often need to prove that you are old enough to have that beer. Now with a digital electronic identity card this could mean that you reveal all the information on the identity card, including all your personal data. With our technology you could just reveal to the barkeeper that you are older than 18 and nothing else. This is data minimization. On the other hand, when you go to a bar you have to be sure that this really is a bar and that you are really talking to a barkeeper. Of course in the case of the bar, this is easy. But on the internet you’re never sure with which site you are communicating, or whether or not to trust it. What we are developing means that you can easily establish trust.

And concerning revealing data about yourself, which of course in some cases is unavoidable, we first inform the user what will happen with their data, whether it will be stored for 10 years, whether it will be deleted right after the transaction, and who is allowed to do what with the data.
Some of the solutions are already available for downloading; some basic code is available. On the other hand we are still building and expanding, so we are looking into standardization and into user interfaces to make the technology accessible to as many people as possible, and also to allow the industry to implement these technologies in their solutions as it becomes a standard solution."

Christian Achermann: "What difficulties did you face during the development process? What did you do in order to prevent such inconveniences?"

Jan Camenisch: "We have been developing these solutions for more than 10 years, and when we first started it was mainly like the mathematical cryptographic challenges that we have to deal with. If I have a digital identity card that confirms my date of birth, how can I use that card to convince a barkeeper that I am older than 18 without revealing my date of birth? How can we build such cryptographic mechanisms? Once we came up with solutions, the much harder part was explaining to people how this would work, so that these colleagues could try to come up with user interfaces whereby people can intuitively use these technologies. I think this is the most important part. Without good user interfaces, such technology will never be implemented, and I think we are still in the middle of research in this respect. We have some first solutions, but I think we can achieve much more."

Christian Achermann: "Looking into the future, how will your solution be further developed over the coming months or years?"

Jan Camenisch: "I would say that we are pretty much done with the basic technology with the cryptographic algorithms. We know how to issue electronic identity cards and how to issue certificates. When it comes to the next layer above this, how to transfer the data, we are about to standardize things and produce communication standards and protocols. Here we are talking about standardization bodies. Higher up towards the user interfaces, we have first solutions, but further research is needed in this area. Also, when we consider how people are actually using the internet these days, for instance social networks, and wikis where they provide loads of personal data, our technology does not readily apply here, and we still have to do some research to figure out how we can best protect people so that a future employer cannot necessarily see the pictures of the latest drinking party."

Christian Achermann: "To conclude, given the fact that so far no similar product exists on the market, how can one best protect his or her own data? Could you make some suggestions?"

Jan Camenisch: "I guess, the best thing you can do is to be very careful with whom you are communicating and what data you are releasing to that party. You could try to read their privacy policies, but sometimes they are very hard to find. Otherwise I suppose I would use one time credit cards and e-mail addresses, and not give correct personal information where it is not necessary. Of course, if you want something shipped to your home address you need to give your real home address."

Christian Achermann: “Thank you very much for your time, and for the extensive amount of information you have given us.”

Brand names from other companies/manufacturers will be accredited. You can obtain contract conditions and prices from the IBM offices and the IBM Business Partners. The product information reflects the current stand. The subject and scope of the services are defined exclusively according to the relevant contracts.

The publication on hand is for general information only.