NETWORKWORLD

This story appeared on Network World at
http://www.networkworld.com/news/2008/062008-dutch-launch-open-source-smart-card.html

Dutch launch open-source smart card software project

By Jeremy Kirk , IDG News Service , 06/20/2008

A Dutch charity is funding an open-source project to design smart card software that offers stronger protection of personal data in light of security vulnerabilities found with cards used today in the U.S., U.K. and Netherlands.

NLnet Foundation will give €150,000 ($234,000) to Radboud University in Nijmegen, Netherlands, for the project, which will run through 2010, said Valer Mischenko, the foundation's general director.

The research and the code will be published for peer review, an open-source development model that can offer a stronger security model than undocumented, proprietary systems that dominate the smart-card market, Mischenko said. Companies will be able to use the software in future products, as it will be licensed under the GNU General Public License.

The need for more secure systems is clear. Researchers revealed last year security vulnerabilities in the Mifare Classic RFID (radio frequency identification) chip, which is used in up to 2 billion smart cards used for building access and public transportation systems worldwide.

Related Content

The researchers figured out how the Mifare Classic's encryption algorithm worked, allowing them to obtain the 48-bit encryption keys the cards used. With that information, it's possible to create a clone of the card or, in some cases, add money to the card for public transport systems, said Bart Jacobs, information security

professor at Radboud University.

The Mifare card chips "are from the 90s," Jacobs said. "At the time when they were developed, there was little computing power on those chips."

Using more complex encryption algorithms requires more computing power, which potentially means that a person could have to stand at a turnstile longer during a transaction. One of the aims of the new research is to strengthen that encryption but still have the transaction take a second or less, Jacobs said.

"You don't want to stand before a gate 10 seconds before it opens," Jacobs said.

Another aim is increased privacy. London's transport agency, Transport for London (TFL), uses Mifare chips in its contactless payment system known as the Oyster card. Customers have a couple of options when getting the card: they can register it with TFL, which offers benefits such as free replacement if the card lost, or buy an unregistered one.

If the card is registered, some of the person's travel record is stored by TFL databases, Jacobs said. That's a potential privacy risk if the data is misused. Jacobs said the project also aims to create card that can still offer special, personalized benefits for the rider but also not unnecessarily transmit more information than needed to a centralized database.

"Our point is that you can get these benefits without sacrificing privacy," Jacobs said. "We'd like to try this out."

A person's public transport history could also be used for marketing or other commercial purposes which may suit some interests but not necessarily be in the best interest of privacy, Jacobs said.

"In our improved card, the card behaves more like a paper ticket," Jacobs said. "It is electronic, but hides its identity and only says to a gate 'I'm allowed to make that trip'."

Related Content

The research, headed up by Jacobs and Wouter Teepe, will start in July in the university's Digital Security Group. Jacobs said within about six months the researchers should have a good idea if a stronger algorithm will be technically feasible and practical in use.

All of the research will be open source and licensed under the GNU General Public License, Mischenko said.

The IDG News Service is a Network World affiliate.