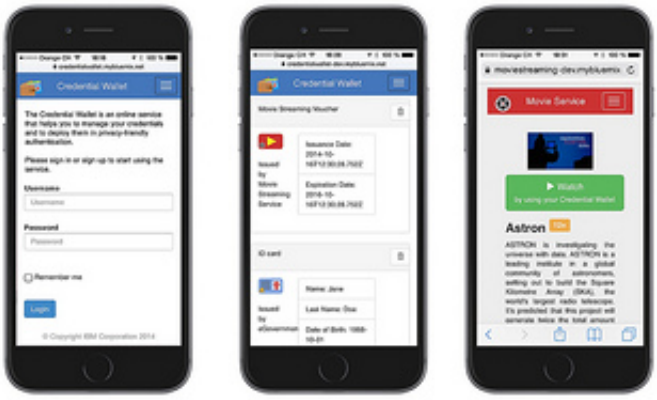
Cryptographic algorithm can prevent unwanted sharing of personal data, including credit card numbers

January 29 2015



Identity Mixer on Mobile

IBM researchers today announced plans for a cloud-based technology that holds potential to help consumers better protect online personal data, including date of birth, home address and credit card numbers.

The technology, called Identity Mixer, uses a cryptographic algorithm to encrypt the certified identity attributes of a user, such as their age, nationality, address and credit card number in a way that allows the user to reveal only selected pieces to third parties. Identity Mixer can be used within a digital wallet, which contains credentials certified by a trusted third party, such as a government-issued electronic identity card. It's

important to note that the issuer of the credentials has no knowledge of how and when they are being used.

"Identity Mixer enables users to choose precisely which data to share, and with whom", said Christina Peters, IBM's Chief Privacy Officer. "Now web service providers can improve their risk profile and enhance trust with customers, and it's all in the cloud, making it easy for developers to program."

According to comScore, the average person spends nearly 25 hours per month using the Internet, accessing dozens of different Internet services, including banking, shopping and social networks. For virtually every service, users have to create a personal profile with a username and password—or for stronger security—cryptographic certificates. Although such tools can offer sufficient security for many purposes, they do not typically provide any level of privacy for the users, causing them to reveal more personal data than is necessary, which can be costly if it falls into the wrong hands.

For example, consider a video streaming service that offers films with age restrictions. To stream a 12+ movie, Alice needs to prove that she is at least 12 years of age and that she lives within the appropriate region. The typical way to do this would require Alice to enter her full date of birth and address, but this reveals more about her than is necessary to complete the transaction. Identity Mixer can simply confirm that Alice is at least 12 without disclosing the month, date and year of her birth and reveal merely that she lives in the correct region (i.e. region 1). This ensures that even if the video streaming service is hacked, Alice's personal data remains safe.

Similarly, if Alice needed to use her credit card to purchase a movie, the video streaming service would only learn that Alice's credit card is valid and that it can accept payment, never revealing the actual number or

expiration date.

Previously available for download and demonstrated to work on smart cards, Identity Mixer is now being made available to developers as an easy-to-use web service in IBM Bluemix, IBM's new platform-as-a-service (PaaS) cloud that combines the strength of IBM software, third-party and open technologies. Beginning this spring, Bluemix subscribers will be able to experiment with Identity Mixer within their own applications and web services. Using simple pull-down menus, developers can choose the types of data that they wish to secure and Bluemix will provide the code, which can then be embedded in their services.

"Identity Mixer incorporates more than a decade of research to bring the concept of minimal disclosure of identity-related data to reality, and now it is ready to use for both computers and mobile device transactions," said Dr. Jan Camenisch, cryptographer and co-inventor of Identity Mixer at IBM Research.

"We wanted individuals to have control over what they reveal about themselves,"said, Dr. Anna Lysyanskaya, a co-inventor of Identity Mixer, who is currently a professor of computer science at Brown University. "With Identity Mixer now in the cloud, developers have a very strong cryptographic tool that makes privacy practical; it is a piece of software that you can incorporate into any identity management service enabling the service to verify that an individual is an authorized user without revealing any other personal information."

European and Australian Pilot Programs Demonstrate Identity Mixer Potential

To demonstrate the new cloud version of Identity Mixer, IBM scientists

are collaborating with academic and industrial partners in Europe and Australia in a new pilot project called Authentication and Authorization for Entrusted Unions (AU2EU). In a two-year, 8.6-million euro pilot, scientists will test Identity Mixer in two scenarios: in Germany with the Deutsches Rotes Kreuz (DRK, or the German Red Cross), and with the Commonwealth Scientific and Industrial Research Organisation (CSIRO), Australia's national science agency.

As a major provider for regional home emergency call and social services in Germany, the DRK delivers tailored social care services to their customers 24/7, including emergency services, assisted mobility, housekeeping and nursing assistance. The organization has four million volunteers and professional staff, 52 hospitals and more than 500 nursing homes operated worldwide.

In the AU2EU pilot, 20 DRK test participants in the southwest of Germany will be equipped with sensors for in-home activity and status monitoring. The data gathered from these sensors will be transferred to a dedicated cloud server, where the data will be analyzed to determine the type of assistance required. In addition, DRK field representatives will be provided with a mobile device to collect and register sensitive customer data, such as medical records, medication and family contacts, to establish a service contract. Identity Mixer will be used to keep all of this data confidential and private. The technology will be implemented by NEC Europe and Tunstall Healthcare.

"Our goal today, as it has been for 150 years, is to offer help to victims of conflicts and disasters as well as to other vulnerable people and to provide support at home, transport and mobility aids to help people when they face a crisis in their daily lives. New technologies play an increasingly important role in realizing this help, particularly for our home emergency alarm service," said Caroline Greiner, the district manager of the German Red Cross for Rhein-Neckar/Heidelberg e.V.

"Here we offer services to senior citizens that allow them to remain at home and in conformable and familiar settings. The privacy technology we are testing in AU2EU will ensure that these aids are provided both efficiently and securely to protect the personal data of our customers to a high degree."

A second pilot will support one of the keys to Australia's agricultural productivity and related export trade: its freedom from exotic diseases, particularly in animals. To maintain the nation's disease-free status, the Australian government, along with key partners, has developed an emergency rapid response plan to take action quickly before an outbreak spreads. This plan involves swiftly bringing together government, academic and other research organizations, along with industry partners into a secure, trustworthy online collaborative environment that facilitates evidence-based decision making. Using Identity Mixer, the pilot will help facilitate the secure sharing of sensitive information in a timely matter across several remote locations and among collaborating partners.

"Speed and responding rapidly to disease incidents are absolutely vital towards saving the lives of both humans and animals," said John Zic, principal research scientist, CSIRO. "Using the advanced technologies in this pilot, we expect to see gains in the ability to respond, while still maintaining the security, privacy and trust required to be effective."

Peters adds, "Identity Mixer is an example of why legislation around data privacy across the globe should enable—not stifle—innovation. It demonstrates that innovation leads to better data privacy: privacy that is more secure for the consumer with tools that are more accessible and easier to implement for the provider."

Provided by IBM