Innovation Center

Digital – and secure

München, 07/27/2015

In search of mobile and low-risk solutions for internet users, IT experts at LMU are building up a network that links computer scientists with commercial enterprises to provide effective security architectures for secure digital communication.

Transmission and exchange of data needs secure communication channels. Sensitive and confidential information should not be susceptible to eavesdropping by third parties, but its designated addressee should ideally be able to access it from anywhere at all times. The principle of confidentiality of written correspondence was established thousands of years ago – for reasons that have lost none of their force. Moreover, the need to ensure accessibility, confidentiality and integrity of electronic data provided the impetus for the birth of modern information theory and should be of primary concern to all data specialists and security administrators today. However, the growing complexity of our digital world with a huge number of devices currently in use are making this fundamental performance criterion ever more difficult to fulfil, and clever cybercriminals are only too willing to exploit security loopholes.

Not surprisingly, for commercial enterprises, data security stands at the top of the agenda. This in turn explains why one of the four core fields of research at LMU's new Innovation Center "The Mobile Internet" will focus on computer security. In this network, IT experts at LMU plan to bring science and business together to develop innovative answers – for industrial firms and for society at large – to the security challenges by the proliferation of mobile devices, apps and online services. Three important corporations have already joined the venture, which will be led by Prof. Dr. Claudia Linnhoff-Popien, who holds the Chair in Mobile and Distributed Systems at LMU's Institute of Informatics.

The project is part of the Zentrum Digitalisierung.Bayern (ZD.B) initiative announced on 27. July by Bavaria's Minister for Economics Ilse Aigner and Science Minister Ludwig Spaenle. The ZD.B is designed to create a common framework for the integration of all state-supported activities relating to digitalization in Bavaria by providing a platform that facilitates research, collaboration and commercial innovation. The new Innovation Center at LMU will receive some 5 million euros in financial support during the next six years from the Bavarian Economics Ministry. Industrial partners will also contribute funding the venture.

"In the old days, it was enough to build high walls."

The researchers in Claudia Linnhoff-Popien's department are well versed in the field of computer security. "Cybersecurity has always been a central integrative theme of our research. The solutions that we offer must be as secure as possible. Anything less would put us out of business," Linnhoff-Popien asserts. "We have now taken this commitment a step further, and have designated

Cybersecurity – together with the Mobile Internet, Logistics and Tracking, and the Smart City – as one of the thematic pillars of this major project. After all, the security of internal and external exchange of confidential commercial information is a matter of fundamental importance for the business world."

"In the old days, it was enough to build high walls," says Sebastian Feld, a researcher in Linnhoff-Popien's department and Scientific Coordinator of the new Innovation Center. "But in the era of Advanced Persistent Threats, that won't work." APTs are targeted, highly specific cyberattacks designed to tap into sensitive data streams for long periods of time. "Unless firms are willing to share information with each other, they will not be in a position to ensure the immunity of their IT systems," Feld says. "The problem is analogous to that faced by developers of new antibiotics," Linnhoff-Popien adds: One has to stay one step ahead of the pathogens, which means finding a new drug before they develop resistance to the current agent.

Highly effective platforms

The IT experts at LMU have already developed several highly effective platforms for specific applications. One is the online social-network architecture "Vegas", which is "decentralized and secure," as Feld emphasizes, and is based on the concept of 'privacy by design': Personal data – individually encrypted – are stored on distributed devices, and encrypted exchanges between users are routed not through a central server, but via decentralized communication channels, which can be monitored by the sender and receiver.

The platform Die SchulApp is another example. With this program, LMU researchers have created a secure tool for confidential communication between schools, pupils and parents. Much of the information transmitted on such networks consists of highly sensitive personal data relating to individuals who are legally minors. Hence, the need for very high security standards arises. In this case, the LMU specialists achieve this goal by combining highly effective encryption of all transmission channels with sophisticated management of access rights and server-side app-access management for users. A further important feature is the secure authentication of all participants, which is achieved by the exchange of intuitive virtual keys from smartphone to smartphone when people meet.

The system uses QR barcodes for this purpose, and intelligent log-ins make it possible to unlock specific terminals – ensuring that each message reaches the right recipients. "Security must be built into every component. Every chain is only as strong as its weakest link," says Linnhoff-Popien. "For example, parents are recruited into the security architecture of Die SchulApp via their handwritten signature on a piece of paper – something that has not been implemented before."

The Bavarian Ministry for Education and Culture, in cooperation with the State Data Protection Officer, has subjected the outcome of this model project to rigorous tests and recently licensed the system, as the first of its kind, for use in schools. Meanwhile, Claudia Linnhoff-Popien has a long list of other interested parties who would like to use the platform. Adapting it to the needs of new users is "very easy", she says.

Linnhoff-Popien is also convinced that these concepts can be refined for use by commercial enterprises. "Although it was designed with the interests of private individuals in mind, a communications platform like "Vegas" can in principle be modified to provide the levels of data security demanded by the commercial sector," she says, "and something similar to Die SchulApp could also be used for staff communications or by project groups." She and her colleagues are currently engaged in consultations with potential commercial users, with a view to obtaining a comprehensive picture of their needs. With this information in hand, they can then provide each with an appropriately tailored platform.

According to Linnhoff-Popien, the Innovation Center and her whole department work on the principle of 'upfront delivery'. "The innovations we develop always represent proof-of-concepts and preliminary work for future custom-made systems. We set out to design platforms that meet a perceived need." The researchers in the new Center also hope to come up with solutions specifically for medium-sized enterprises. "And as researchers, we also seek to close gaps that we discover in the course of our own work," Sebastian Feld adds.

The shortest route from A to B

Feld and his colleagues are currently developing a routing service that takes privacy concerns seriously. "We want to build a navigation system that is compatible with the protection of privacy," he says. Each query is framed in such a way that neither the user's location nor her destination is directly specified. "I want to discover the shortest route from A to B without giving any information that would allow the service provider to determine where A and B actually are. It sounds paradoxical, but it can be done." The trick lies in obfuscation. "We don't enter A as, let's say, Oettingenstrasse 67. Instead, we define a radius of search, within which we do the routing. Then we ask a routing service for a radius within which B lies, and again do the rest ourselves." Implementation will be "a bit tricky", because the same principle is used to locate sites of traffic congestion without give one's current location. "It's a hot topic," says Feld – in a highly competitive market: These days, almost everyone makes use of routing services.

Three large enterprises have already been recruited as commercial partners in the new Innovation Center: Allianz SE is involved in the Cybersecurity section, Siemens AG in Engineering of Distributed Systems, while Flughafen München GmbH, the company that runs Munich's airport, is particularly interested in the digitalization of contacts with customers and the tracking of baggage. When asked why his firm decided to participate in the work of the Innovation Center, Ralf Schneider, Chief Information Officer (CIO) for Allianz SE said, "the fact that the world is ever more dominated by digital technology does not mean that the human factor is any less important. On the contrary, where innovation is concerned, we are dependent on human creativity. And creativity doesn't just happen by sitting down in front of a blank sheet of paper; it requires interaction with others. That, in my view, is the key to success, and the planned Innovation Center is a prototype for the implementation of this concept. Moreover, in the case of Cybersecurity, the value of close cooperation is quite obvious."