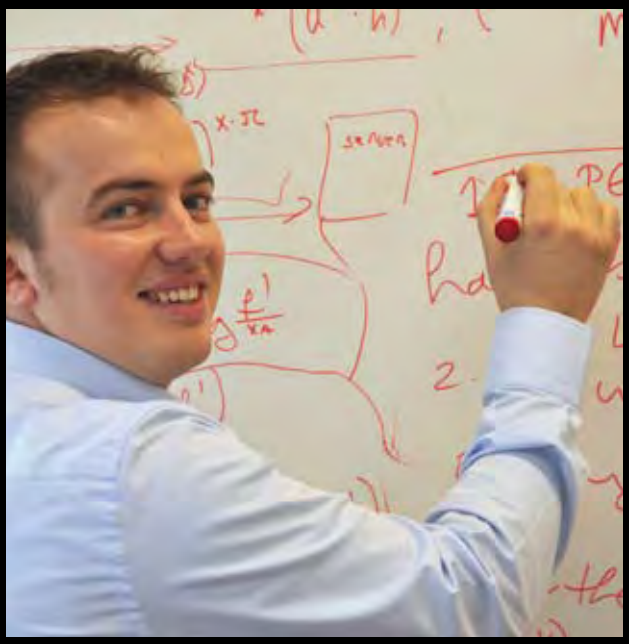
WHO SHOULD KNOW EVERYTHING ABOUT YOUR KNEE INJURY?



LUAN IBRAIMI

Encryption schemes in modern healthcare applications involving privacy-sensitive medical data call for new approaches that can address the complex scenarios that could occur. The search for a data-centric strategy, including a formula for defining access policies for the same data, appears to be very promising.

During the first year of his PhD study at the University of Twente and during his second year at Philips Research, Luan Ibraimi carefully formulated his research objectives within the CTIT programme: Integrated Security and Privacy in a Networked World (Istrice). He is currently studying a new approach that will enable secure storage and controlled sharing of patient health records in different scenarios. A scheme is proposed whereby patients can encrypt their own health records according to specific access policies. Two trusted authorities are distinguishable within this scheme. The first obviously involves healthcare workers in the professional domain. Examples include general practitioners, specialist physicians, personal fitness coaches and even insurance company representatives.

UNTRUSTED SERVERS

People in the social domain also have an interest in closely following the health history of particular patients. Examples include family representatives or close friends. "The scheme allows patients to store their personal health records in a protected form, even on untrusted commercial servers", Ibraimi states. "It is suitable for modern healthcare settings, as it helps patients to share their records securely, with users from various domains." Patients specify only the attributes that recipients need to have in order to access their data. A recipient therefore does not even need to know the exact identity of the user. Prof. Willem Jonker is supervising Ibraimi's project, together with Prof. Pieter Hartel, head of the research group on Distributed and Embedded Security (DIES), which is also involved in the project.
Jonker explains, "Only doctors who have credentials that satisfy the policy can gain access to the data. In emergency situations, the system must be able to grant first-aid workers access to the data as well, if necessary."
"I am very much in favour of using the data-centric approach that is at the centre of all this, instead of the current system management strategies. For example, who should know the details of a knee injury you had one year ago? Your general practitioner: yes! Your fitness coach: yes! Your employer: probably not. The same applies to the insurance company; it depends on the actual situation. As an outcome of confidential conversations with their general practitioners, patients are able to specify which individuals can gain access to their data. We refer to this specification as the policy. We attach the policy to the actual data."

ATTACK SCENARIOS

Ibraimi's work currently consists of defining, constructing and verifying encryption schemes emerging from this approach. Applying known mathematical techniques, he has already filed one patent application. Another is on the way.
Ibraimi explains, "After defining the algorithms, I use attack scenarios in order to prove that they can be resisted in a proven manner. I distinguish between attacks coming from outside and from within the healthcare setting itself. Security against external attacks is easier to prove than is security against internal attacks."
"For example, the technique of computing discrete logarithms is used to show that an attack is not possible. This is done by comparing the attack to a known mathematical problem that is currently unsolvable. If this can be done, the attack can be classified as NP-hard, meaning that no problems can arise in the type of attack mentioned before." Willem Jonker very much hopes that the work of Luan Ibraimi and his colleagues, both at the University Twente and at Philips Research, will contribute to the international standards for personal health records, which are currently under construction.
Jonker observes, "There is still much work to be done. The international standardization process is permanently under construction. We write proposals based on our work to contribute to this process, obviously in the hope that our approach will ultimately prove best suited for the job."

"UNDERSTANDING THE APPLICATION IS OF MAJOR IMPORTANCE"

Willem Jonker: "Luan spent the second year of his PhD study at Philips Research in Eindhoven, where I coordinate research for the Lifestyle sector. The topics we address include lifestyle management and preventive health. Working at Philips Research, Luan gained a feeling for the real problems in this kind of medical systems. Understanding the application is of major importance. By regularly meeting researchers who work on the frontlines on a daily basis, he developed a good sense of the scientific questions that are currently at hand."
"Although research driven by scientific curiosity is also necessary, I prefer a more applied strategy. Such strategies fit well within the CTIT institute for several reasons: healthcare is a public goal, the research has multidisciplinary elements, like ethics and legal issues, and the accumulation of knowledge can bridge the gap with activities that are attractive to industry. This is obviously very interesting to us here in Twente, given that we are an entrepreneurial university."