Ensuring the security of digital information

May 31 2017

Jiqiang Lu with the GPGPU used to crack the A5/1 cipher. Credit: A*STAR Institute for Infocomm Research

Every day we store and transfer sensitive digital data, post personal information on social media, and provide valuable details to companies when we use their services. Keeping secure the 2.5 quintillion (2.5 million billion) bytes of data created every day from outside attack is a mammoth task. The potential for breaching security is vast, due to a plethora of available services and the many weak links that appear in the chain whenever data is moved. A further consideration is who should have access to data, taking the issue beyond technology into the social and political realm.

These challenges demand a huge global effort from computer

technicians and researchers across the world. Research groups at A*STAR are using their technical expertise to monitor online services, identify vulnerable areas of data management, and develop software and hardware that keep data secure. Their work is not only defending data against attack, but also maintaining easy access to it for authorized users.

Managing mobiles

Arguably, the first line of defense against data misuse should be implemented in the Global System for Mobile Communications (GSM), the world's most widely-used wireless telephony technology. With a 90 per cent share of the market, around 4.5 billion customers rely on the security of GSM to protect their communications.

"GSM was first deployed 25 years ago and has become the global standard for mobile communications," says Jiqiang Lu at the A*STAR Institute for Infocomm Research (I2R).

The A5/1 stream cipher, the encryption scheme that GSM uses to protect data, has been successfully attacked before to test its security, but almost all the attacks were hypothetical in the sense of their impact on the real-world security of GSM—they either required a large amount of complex data or had a long attack time, meaning they could be mitigated and blocked by existing GSM security protocols. Lu and co-workers decided to investigate whether a detailed and fast-acting attack on the GSM A5/1 cipher could reveal fundamental weaknesses in the system. Using a computer setup costing just US$15,000 in 2013, the researchers employed a powerful algorithm to explore the A5/1 cryptosystem, and obtained 984 gigabytes of information about the system structure over 55 days. They used this information to launch attacks that pulled data from the GSM in just 9 seconds—usually too quick for interception by security protocols—and illustrated that A5/1 would be vulnerable if it were to be attacked by sufficiently skilled hackers.

"The GSM should immediately upgrade its encryption algorithm to a stronger one," says Lu.

Containing the cloud

While Lu's team continue to protect our data as it flies around the global mobile network, another group at I2R which includes Jia Xu is examining the cloud storage providers that have revolutionized how we archive and share data. By entrusting large organizations to store multiple copies of our data on cloud servers around the world, we are freed from worrying about our phone, laptop or USB drive being lost, stolen or broken. But how can we be sure that these organizations will keep our data secure?

Xu and co-workers have designed cryptographic algorithms for cloud storage that not only protect the integrity of data, but also control who can access it.

"The core challenge in cloud storage is to balance three factors: efficiency, security, and usability," says Xu. "Cloud providers would like their services to be almost as efficient and low-cost as when no security features are implemented, while customers want the user interface to be as simple to use as possible." The research community is attempting to identify security vulnerabilities in existing cloud services, and to design new hardware and software solutions to resolve them.

Some security weaknesses arise from so-called deduplication techniques, which identify and remove duplicated copies of the same file, allowing cloud providers such as Dropbox to save server storage space and network bandwidth. Xu and co-workers identified severe security vulnerabilities in certain types of deduplication that could be exploited using attacking software.

Dropbox disabled cross-user deduplication in 2012. However, the new algorithms developed by Xu and the team will allow deduplication to be used alongside robust encryption, thereby improving efficiency while protecting data stored in the cloud.

The value of our data

Most of us have made large amounts of information available to organizations through shopping online and posting on social media. These activities have created extremely large datasets, known as Big Data, which can be analyzed to reveal human behavior patterns and trends. This valuable information is often sold to other organizations.

"Companies are hungry for more data, to enable them to better understand and profile users," says Lux Anantharaman who heads the Business Analytics Translation center in I2R. "They know the power of Big Data to provide targeted ads, known as personalized marketing, but profiling can also lead to price discrimination called personalized pricing, which most users are not aware of. For example, some airline websites price tickets differently based on the user's device operating system—Mac OS users get charged more."

Anantharaman is concerned that most users are not aware of the value of their data, or the fact that when they use 'free' online services they are actually 'paying' for them with their data. Companies then explore the data with analytical computing tools and use the information, along with the latest insights on human behavior from social scientists and economists, to shape the choices offered to their customers.

"The 'big' keep accumulating more and more data about the 'small'," says Anantharaman. "We, the small, are slowly becoming aware of this fact, but generally we feel helpless and resigned about it. Moreover, government regulations haven't kept pace with technology, and often

take the side of big organizations, doing a disservice to the users. For example, recent US government measures allow internet service providers to access a user's browsing history without the user's permission."

Anantharaman is adamant that the best way to overcome these difficulties is by educating users and improving government regulation. "This might sound odd from a technology person, but Big Data is not just about technology, it is about how data are used, which is a legal and social issue," he says. "For this reason, our research focuses not just on technological mechanisms, but also explores how regulations and education can help users better understand the power and pitfalls of Big Data privacy."

Quantum complications

While we grapple with data safety in the computing systems that we already use, other scientists are developing technology that could completely transform the field of data security for the devices of tomorrow. In contrast to ordinary computers whose logical 'bits' can only take values of 0 or 1, quantum computers use 'qubits' that can have values of 0, 1 or a combination of both values. This capability opens up an entirely new domain of logic and mathematics, allowing quantum computers to solve complex problems in a fraction of the time it would take a conventional machine. This revolution will arrive with great benefits, but will bring its own problems, as Leonid Krivitsky at the A*STAR Data Storage Institute explains:

"Many cryptography systems rely on hard problems such as prime factorization—the fact that it is very difficult to figure out the prime factors of a given number. However, theoretical work has shown that the factorization problem could be solved very quickly using a quantum computer. So, once a universal quantum computer is built, it could hack

ciphers which were previously thought to be unbreakable."

This might seem alarming, but there is no reason to panic. Functional quantum computers are still a long way off, and to counteract the potential threats, many groups around the world are contributing to the growing field of quantum cryptography, which will redefine our protocols of secure communication. In fact, the new cryptography algorithms made available by quantum computers could provide ultra-high data security long before any risks become a concern.

"I foresee the use of a quantum communication channel as a backup resource for highly sensitive transactions, where security is more important than the transmission speed," says Krivitsky.

For now, though, the challenge is to physically build a stable quantum computer. Krivitsky and co-workers are exploring the possibility of using tiny defects in synthetic diamonds to act as nodes which process and store quantum information.

"We place several diamonds on a single chip and communicate with optical links, similar to those which form the background of the internet," says Krivitsky. "Our innovations will enable transmission of quantum information over long distances and contribute to the development of a worldwide quantum network."

Safeguarding the future

The task of keeping our data secure is clearly a complicated and interdisciplinary challenge. A*STAR researchers are not only developing new technical initiatives, but also working at the forefront of global efforts to raise awareness of data security. By looking for chinks in the armor of global systems like GSM and cloud storage, educating the public about the commercial value of their data, and planning for the

future paradigm shift that might be brought about by quantum computers, it is reassuring to know that the brightest minds at A*STAR are focused on keeping our data safe.

Provided by Agency for Science, Technology and Research (A*STAR), Singapore