Publication: Asian Scientist
Date: 11 June 2014
Headline: Keeping data under lock and key

Keeping Data Under Lock And Key

PUBLISHED ON JUNE 11, 2014
BY SINGAPORE MANAGEMENT UNIVERSITY | EDITORIALS

In light of the recent revelations on mass surveillance programmes, SMU Professor Pang Hwee Hwa's research into enhancing data privacy may bring relief to both companies and individuals alike.

AsianScientist (Jun 11, 2014) – By Alan Aw – In 2013, former US National Security Agency contractor Edward Snowden attracted public attention for revealing over two million surveillance programme files belonging to intelligence agencies from Australia, the United Kingdom and United States. Hailed a patriot by some and a traitor by others, the whistle-blower showed the world that governments are capable of mass-surveillance programmes without the public's knowledge or consent.

> Director of the School of Information Systems (SIS) Postgraduate Research Programmes at the Singapore Management University (SMU), Professor Pang Hwee Hwa notes: "Suppose that the police want to search your house. They would need to obtain a search warrant for it. However, imagine that the police sneak into your house with the search warrant, and take away your possessions without your knowledge. If this practice is unacceptable, then why is it all right for governments to possess our personal data without our knowledge?" he asks.

Keeping your trump card hidden

A researcher of data privacy, Professor Pang, who is also SMU's Director of Postgraduate Research Programmes, was initially trained in the field of database management. However, the challenge of overcoming confounding mathematical methods and abstract algorithms attracted him to the field of data privacy in recent years.

Publication: Asian Scientist
Date: 11 June 2014
Headline: Keeping data under lock and key

> Drawing an analogy between his research and a card trick, Professor Pang explains: “Assuming that you have four cards facing down, and no one can see them. One of them is the ace, which represents the article that you want me to retrieve for you. This could be a classified document or personal email. Traditionally, if you submit a request or query to retrieve an article from a database, you need to make the information transparent. In other words, you would allow me to uncover the cards, and convey that you want the ace.
>
> “However, the transparency of this request discloses the identity of the cards, hence allowing an observer to learn about your personal information. To prevent that, you must conceal or encrypt your query or request. But once you do that, I must present you all four cards for you to find the ace yourself, since only you know the identity of what you conceal. This is all right when we are dealing with only four cards. But what if there are millions of cards from which we have to locate the ace?”

The solution, explains Professor Pang, lies in the exploitation of randomness. Over the years, cryptographers who study data protection and encryption methods have found that encoding information in a randomised way reduces its susceptibility to hacking.

This insight was crucial to Professor Pang’s research collaboration with fellow colleague and cryptographer Associate Professor Ding Xuhua. Both of them demonstrated a method of randomising the encryption of data and user requests so that individuals were able to access an article in a database without revealing the content. Not only were observers unable to learn about the information being requested, they also cannot emulate the user request because the encrypted request could only be generated via a secret known to the user.

Data security concerns in practice

From Apple’s iCloud to Microsoft’s Office 365, database and cloud services abound to provide data management for companies that handle huge volumes of data. Yet concerns over data privacy – further exacerbated by public concerns over mass-surveillance programmes – impede the adoption of these services.

As Professor Pang explains, these concerns are not unfounded. Current practices require at least part of the Database Management System (DBMS) to be trusted. This means that in a cascade of data processing steps that are found in any standard DBMS, at least one step leaves the user data and request transparent to the DBMS, which includes the system administrator.

Publication: Asian Scientist
Date: 11 June 2014
Headline: Keeping data under lock and key

> "Current database management models require us to trust the companies that hold on to our information. But Snowden's case serves as a warning for us to err on the side of caution by encrypting user data and requests throughout the system," he says.

Even though his recent research findings support a completely encrypted DBMS, Professor Pang emphasises that much work remains before the results can be employed commercially. Additionally, he acknowledges that ensuring data privacy is not a one-man show.

Explaining the importance of other disciplines, especially law, he cites a recent high-profile case in which British multinational defence company BAE Systems aborted plans to adopt Microsoft's Office 365.

> "As reported, this was due to concerns that the US Patriot Act would prevent Microsoft from guaranteeing BAE's data would not leak out of Europe," he adds.

A balancing act

According to Professor Pang, current legislation coupled with existing industry standards of data privacy will determine the level of trust that companies and consumers are willing to place in database service providers. That, in turn, will drive greater efforts and investments towards the development and deployment of stronger privacy protection solutions.

> "Data privacy is ultimately a balancing act. We want to satisfy users with an efficient level of data retrieval that is matched by a competent level of privacy," he says.
>
> "We have seen governments harnessing our data for good ends, but we also want to know when they are accessing our private information. Only then can our anxieties and fears over unacknowledged surveillance be allayed."

Asian Scientist Magazine is a media partner of the Singapore Management University Office of Research.