Debunking the myth of password security

November 4 2016, by Nurfilzah Rohaidi

When U.S. presidential hopeful Hillary Clinton was found to have used a private email server for government business as Secretary of State, there was a collective gasp of disbelief. That disbelief quickly turned into horror when it was later revealed that she did not even protect her office computer with a password.

These lapses in computer security can be seen as downright negligent, in a time when major data breaches and leaks dominate international headlines on a regular basis. But it also draws attention to a more compelling question: just how secure are text-based passwords, really?

Associate Professor Gao Debin, a security researcher from the Singapore Management University (SMU) School of Information Systems, believes that there should be alternatives to the ubiquitous, text-based user authentication method. "People tend to pick simple, easy-to-crack passwords, such as their date of birth or worse, 'password'. These are not very secure, naturally leaving their computers and data vulnerable to the 'bad guys'," he says.

And this issue is a timely one. A recent massive data leak of 272.3 million email passwords by Russian hackers, which included scores of Google, Yahoo and Microsoft email accounts, was made possible by preying on less secure third-party websites whose users had recycled their email-password combinations.

Typing your way in

To address the growing concern of text-based password vulnerabilities, researchers have developed new methods of user authentication, such as keystroke biometrics. Keystroke biometrics captures typing patterns and rhythms as a means of identification. This concept is based on previous studies that show typing patterns are unique to each individual, and cannot be easily imitated.

However, gatekeeping via keyboard biometrics isn't foolproof, says Professor Gao, as attackers may attempt to imitate the typing patterns of their victim. The potential for this to happen is an area that Professor Gao is exploring in his research.

"Specifically, I work on attacks and defences. I look into new attacking techniques that the attacker would use in order to exploit a particular application," he says. "I also work on the defence mechanisms—how we can detect those attacks and stop them from happening."

Crafty as they are, attackers can infer the typing patterns of their victims in several ways. One scenario is Google Instant, a Javascript application which can be reverse engineered to reveal this information. Professor Gao and colleagues addressed this possibility in a conference proceedings paper, "Keystroke Timing Analysis of On-the-fly Web Apps", for the Applied Cryptography and Network Security: 11th International Conference 2013.

"When you type in a search query on Google, the result shows up immediately while you are typing, even before you hit the enter key or click on the search button. Therefore, for every single key that you press on the keyboard, there is a corresponding message being sent to the Google server," reveals Professor Gao, who adds that the same technology is being used on Facebook and Twitter, among other websites.

"Servers using such technology could potentially log down the timing of every single message, which would correspond precisely to your typing dynamics."

The imitation game

Inter-keystroke timing, or the time it takes between two consecutive key presses, is the most commonly used type of data for keystroke biometrics. Professor Gao and colleagues set out to question the "uniqueness property" of keystroke biometrics—the extent to which systems can be fooled by attackers imitating their victims' typing patterns.

Recruiting 84 SMU students as attackers, the researchers first gave each participant 30-45 minutes of training with a feedback software program, Mimesis, which they had developed. The program gives positive or negative feedback to the student so that, through incremental adjustments, they can closely imitate how their victim types.

Consider a scenario where a biometrics database is compromised; software such as Mimesis could be used to extract victims' typing parameters, which can then be used for malicious purposes.

"For example, it will tell you that the way that you type right now is slightly different from the victim's typing; or the inter-keystroke timing between A and S is shorter than what the victim types, so you better slow down a little bit when you are typing these two letters," Professor Gao elaborates.

The results show that when a victim's typing pattern is known, imitation is possible—contrary to the findings of previous studies. The students could easily log into systems by impersonating their would-be victims, and 14 of them managed to do so with an almost 100% success rate over

a total of 200 attempts.

Interestingly, even if the attacker had partial information about their victim—perhaps a handful of typing samples captured by a key-logger as the victim is authenticating—they could nevertheless still achieve a reasonably high false acceptance rate.

Professor Gao presented this research at the 20th Annual Network & Distributed System Security Symposium 2013 in San Diego, California. His conference proceedings paper, "I Can Be You: Questioning the Use of Keystroke Dynamics as Biometrics", bagged the Best Paper Award.

Designing better, more usable interfaces

From their experiments, the researchers also learned a number of fascinating things: for one, the easier the password, the easier the imitation. Male students were also found to be better than female students at imitation. However, various factors such as typing consistency, type of keyboard, and imitation strategy had much less influence on the imitation outcome than expected.

Findings such as these could potentially prompt a re-think of current keystroke biometrics-based authentication systems, Professor Gao believes. With his work, he hopes to spread awareness about the weaknesses of keystroke biometrics, allowing companies to configure their web services in such a way that provides functionality without compromising on end user privacy.

Provided by Singapore Management University