New technology that identifies users vulnerable to cyber attack based on behavioral and psychological characteristics

January 20 2015

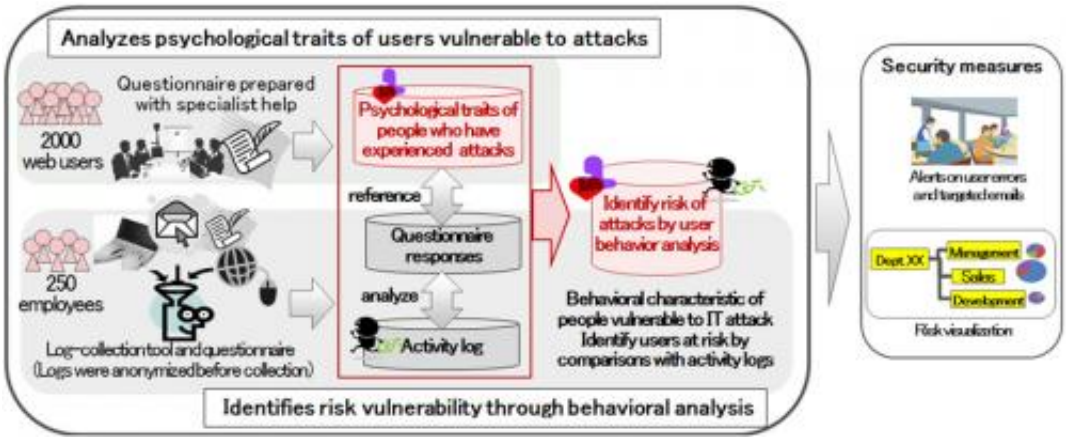

Figure 1: Technologies for identifying users vulnerable to cyber attacks

Fujitsu Limited and Fujitsu Laboratories Ltd. have announced the development of the industry's first technology for identifying users vulnerable to cyber attacks based on the ways they use their computers, such as their e-mail and web activities. This will make it possible to implement security measures tailored to individuals and organizations.

While there are numerous security measures already in existence, the weakness that most cyber attacks and data breaches take advantage of is human error, such as, for example, when a user carelessly clicks on a malicious link in a faked e-mail message. Because this depends on

individual traits, it is difficult to develop a standardized security measure to defend against it.

Fujitsu and Fujitsu Laboratories have used online questionnaires to identify the relationship between the psychological traits and behavior of people likely to suffer three kinds of attack: virus infections, scams, and data leakage. At the same time, based on activity logs on PCs, such as when the PCs freeze, they have developed a technology for calculating different users' risks of being victimized.

This technology could be used to precisely tailor security measures, such as, for example, by displaying individualized warning messages to users who often click on URLs in suspicious e-mail messages without checking them carefully, or escalating the threat level of suspicious e-mails sent between departments with virus-prone users.

Details of this technology are being presented at the 32nd Symposium on Cryptography and Information Security (SCIS2015), opening January 20 in Kitakyushu, Fukuoka Prefecture. Research for parts of this technology was conducted under contract for the Ministry of Internal Affairs and Communications for a project named "R&D of Detective and Analytical Technology against Advanced Cyber-attack ."

Background

In recent years, cyber attacks have been growing increasingly sophisticated, with attacks designed to exploit the psychological vulnerabilities of targeted users to defraud them or infect their PCs with viruses, such as by setting traps in email messages or websites designed to appear to be from trusted sources in line with the targeted user's interests or job duties. These kinds of attacks are often difficult to distinguish from ordinary network access, and are difficult to detect using conventional email filters and firewalls. Moreover, the accidental

actions that are the main cause of information leaks will not simply go away. Under these circumstances, it is all the more important to be able to quickly identify those users who are most at risk of being victimized and to develop protective security measures tailored to the individual or organization.

Issues

There have been past attempts to analyze the behavioral and psychological traits of users at risk of cyber attacks through questionnaires, but actually applying that information to security measures within an organization required making determinations every time a questionnaire was conducted. In addition, because this method can only pick out psychological traits at the time the questionnaire is conducted, the problem is that it cannot respond to risks that vary depending on time of day or level of busyness.

About the Technology

Fujitsu and Fujitsu Laboratories have developed the industry's first technology that makes use of social-psychology knowledge and identifies users at risk of cyber attacks based on the ways they use their computers (Figure 1).

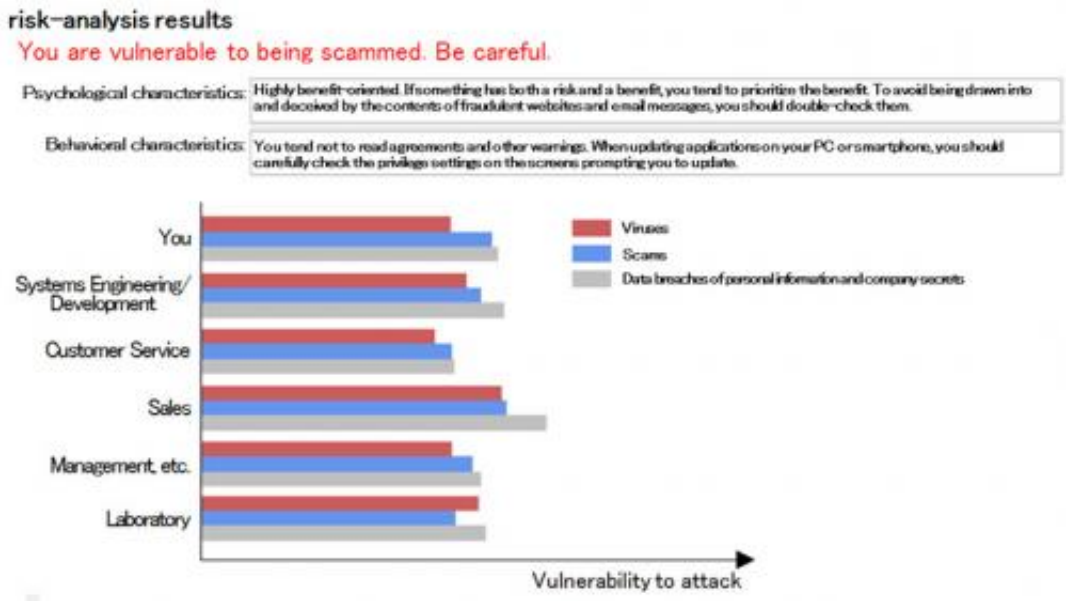

Figure 2: Calculations of IT attack risks

Key features of the technology are as follows.

(1) Analyzes psychological traits of users vulnerable to attacks

Using an online questionnaire created with the help of experts in social psychology, the companies have analyzed the psychological traits of people vulnerable to three kinds of attacks: virus infections, scams, and data leakage. Participants consisted of approximately 2,000 employees throughout Japan ranging in age from their 20s to their 60s, male and female, who use their own PC to do most of their work, with half of them having previously experienced an attack. The results of the analysis showed, for example, that people who prioritized benefits over risks (benefit-oriented people) were more vulnerable to virus attacks, and that people who were highly confident in their own ability to use a computer were at higher risk for data leakage.

(2) Identifies risk vulnerability through behavioral analysis

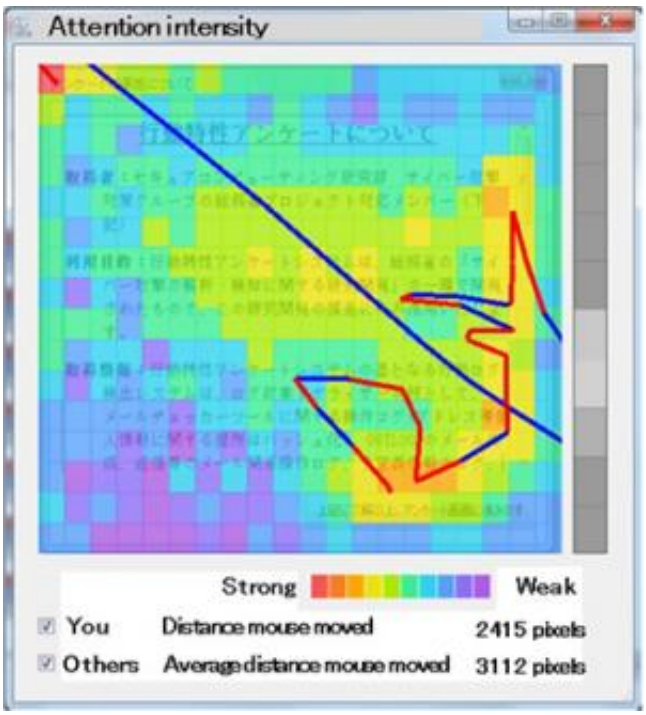

Figure 3: Attentive behavior in reading privacy policies

The companies developed a technology that calculates a user's risk of suffering from an attack as a result of their behavior by clarifying the connections between behavioral characteristics when using a computer and the psychological traits that make them vulnerable to cyber attacks. The companies developed a tool that logs activity on a user's computer (email traffic, web accesses, keyboard and mouse actions), and a tool that creates false errors, such as the computer freezing up. Approximately 250 employees of Fujitsu filled out questionnaires, and this information was used to analyze and quantify the relationship between the psychological traits and behavior of a user vulnerable to

attacks. For example, it was found that users who are highly confident in their ability to use a computer would often perform keyboard actions when the false freezes occurred, whereas benefit-oriented users would spend little time reading privacy policies (Figure 3).

Results

This technology reveals the security risks that individuals and organizations create, raises users' literacy on IT, and is the first step in devising proactive security measures tailored to the organization. For example, preventing data leakage via phishing emails by displaying warning messages to individual users who click links without checking the URLs carefully, or that escalate the threat level of suspicious email messages sent between departments with people who are especially vulnerable to being scammed.

Fujitsu and Fujitsu Laboratories aim to have a commercial implementation of this technology in 2016, and are working to detect users in conditions that are vulnerable to attacks more accurately, and to develop effective security technologies that connect to the psychological and behavioral traits of users.

Provided by Fujitsu

Citation: New technology that identifies users vulnerable to cyber attack based on behavioral and psychological characteristics (2015, January 20) retrieved 20 March 2024 from https://phys.org/news/2015-01-technology-users-vulnerable-cyber-based.html