Security, Privacy, Policy, and Dependability Roundup

Lee Garber

SECURITY

- Hackers compromised press release distribution service PR Newswire’s network and stole the usernames and passwords of some of the company’s customers, according to investigative security journalist Brian Krebs. He and security investigators found the purloined information on the same Internet servers that contained code stolen from Adobe Systems, indicating that the same hackers might have been involved in both incidents. The date and time stamps on the PR Newswire files—apparently involving the company’s customers in Europe, the Middle East, India, and Africa—show they were probably taken on or after 8 March 2013.

- Engineers Adam Crain and Chris Sistrunk discovered vulnerabilities in the communications protocol that electric and water companies use to monitor control stations. These companies use DNP3 for communications between elements in their supervisory control and data acquisition systems, while SCADA systems let them remotely monitor facilities from a control center. The engineers found no problems with the open source DNP3 application but found flaws when testing a DNP3-based program from a vendor that sells software to large SCADA vendors. Hackers without great technical expertise could exploit these flaws to cause widespread outages.

- A team of researchers from the University of Illinois at Chicago, the Technical University Eindhoven, Academia Sinica, the Chinese Culture University, the University of Pennsylvania, and Good Technology found a major flaw in the cryptography used in digital identity cards that Taiwan issues its citizens. Of the approximately 2 million identity cards’ 1,024-bit RSA keys the researchers studied, 184 were generated so inadequately that hackers could have broken them in a few hours using standard computers. For properly generated keys, this would require a supercomputer or botnet. The Taiwanese Citizen Digital Certificate program’s cryptography received certification based on the US National Institute of Standards and Technology’s (NIST’s) Federal Information Processing Standard 140-2. According to the researchers, their findings raise questions about some governments’ and other sensitive organizations’ cryptographic certifications.

- A panel of experts estimates that Japan needs 80,000 more information security workers, 30.2 percent more than the 265,000 it presently has. The government-appointed panel also said that 160,000 Japanese security professionals need additional training to get up to date on current threats. The group recommended that government officials review both the information security workers’ qualifications and the courses that universities and other institutions offer. Japan already provides several security-related training programs and hacking competitions, which the government’s Information-Technology Promotion Agency sponsors.

PRIVACY

- Facebook has changed its policies to let teenagers post status updates, videos, and images that anyone, not
Google will allow its user being aware of it. The tracking could occur without the drain on the handset’s battery means using much power. The lack of and accelerometer sensors—with- out using much power. The lack of drain on the handset’s battery means the tracking could occur without the user being aware of it.

Google will allow its advertisements to identify users who have rated goods and services highly on the company’s network of sites, without users’ explicit permis- sion. Under the new policy, Google could show these endorsements on the more than 2 million sites in its display advertising network. Thus, under default settings, if users follow a company on Google+ or praise an album on Google Play’s music service, their names, photos, and opinions could show up in advertise- ments. Users have expressed concern in the past—such as in the class-action lawsuit against Face- book—about companies using their statements in ads without explicit approval. Privacy advocates contend that companies should be allowed to put user endorsements in ads only if users opt in, rather than forcing them to opt out if they don’t want to participate.

Sophos’ most recent quarterly Spampionship study indicates that the US is the source of most of the world’s spam—14.6 percent. The next highest-ranking countries are Belarus with 5.1 percent, India and Italy with 4.7 percent, China with 4.6 percent, and Taiwan with 4.1 percent. However, when measured on a per capita basis, the leading spam sources are Belarus, Uruguay, Taiwan, Luxembourg, Macedonia, Peru, and Kuwait. According to Sophos, the reason so much spam comes from the US is its large num- ber of poorly secured computers that hackers can turn into zombies and use to send spam.

After months of development and study, NIST released its pre- liminary cybersecurity framework for critical infrastructure owners and operators in industries such as power generation, transportation, and telecommunications. NIST will open a 45-day public-comment period on the preliminary frame- work and plans to release the final document in February 2014. The preliminary framework outlines a consistent cybersecurity approach with steps that large and small com- panies in various industries could customize and adapt as neces- sary. Once NIST releases the final cybersecurity framework, it will use incentives—such as grants and streamlined regulations—to try to persuade organizations to adopt the steps that the voluntary plan calls for.

The European Parliament is considering a measure that would require companies, including those headquartered in the US, to get approval from European privacy authorities before complying with US-based search warrants that affect Europeans. The new proposed law would force companies outside the EU that operate in Europe to comply with EU data protection rules. For instance, companies would need approval from an EU agency before releasing data on someone’s electronic communications. Viola- tors could be fined up to 5 percent of their global annual revenue.

Several major US colleges and universities have postponed early application deadlines for prospective students because of technical problems with The Common Application—a major online application system used by 517 colleges and universities worldwide. In August, the organization released a new ver- sion of its online system that had numerous problems affecting the ability of students to fill out forms, of high schools to send transcripts and recommendations, and of col- leges to download material to their computers. And recently, the web- site crashed for several hours. Some schools are looking for ways to bypass The Common Application, such as by accepting paper forms or using an online competitor, the Universal College Application.

Rogers Communications, a major Canadian telecommunications company, has blamed software problems for crashing part of its cellular system for five hours across the country. The issues affected the company’s net- work equipment and interrupted its voice and texting services, including those offered by the company’s Fido and Chatr divisions. The company, which has approximately 10 million wireless customers, says it’s trying to determine what exactly caused the problems.