A Consultant's View

Vol. XX No.▪10 October 2013

NSA Snooping – So what?

Recently, it was revealed that the NSA was snooping on a lot of emails and phone calls even from people within this country. For most of us, that snooping isn't a big deal. However, for nearly every corporate security officer, the news brought a major headache. If the NSA can get at our business emails, read our databases out in the cloud, and listen in on our phone calls, so can a well financed competitor. The risks are huge.

The problem isn't the NSA snooping. The problem is that the NSA has placed "backdoors" into nearly every public email service, cloud provider, VIOP phone service, etc. controlled by a US company. A number of technical experts recently wrote, "The reality is that backdoors and covert access mechanisms are fragile and often exploitable by organized criminals, hackers, and the military and intelligence services of other governments." Anything that has a "backdoor" is not secure. If the NSA can get to it, so can someone else. Government mandated "backdoors" in other countries are already being used by criminals.

If a system is built with a data access that is supposed to be used only for special purposes, that access will be used by some unauthorized person for another purpose. That is true of every software ever written. If you want some data to be secret, do not have a path where it can be accessed.

A Backdoor Makes a System Not Secure

Recently, Groklaw, a blog on law, shut down. The founder stated that the blog relied on email and lawyers have a requirement to keep their communications secret. With the revelations about NSA snooping, the founder came to the conclusion that there was no way to continue to operate. The revelations have shown that nearly any public email service does not meet the privacy requirements of lawyers. Those email services that had sufficient encryption to have good privacy such as Lavabit and Silent Mail have shut down. Nearly every layer of the email protocol has problems.

The discussion of how Google, Microsoft, and others are providing access to the NSA for snooping means that every cloud implementation out there is suspect (as well as all the network switches).

One more time, American businesses are being warned that the only proper way to plan for data security is to plan for the storage to be "hacked". Unfriendly people will get into your data. Now, what plans do you need to make to deal with it?

Some plans are: encrypt everything that will go to a public server. All email going in and out of the US will be read. Those emails that are encrypted will be saved hoping that the NSA will be able to break the encryption later. Use as long of a key on the encryption that you can. It is better to use third party, open source encryption software than anything provided by a major commercial enterprise as the NSA is supposed to have "back doors" into the encryption software provided by major commercial enterprises.

Chase Dropping Gift Cards

Recently, Chase ended its selling of gift cards. This is an important change. Sales of gift cards have been growing year by year. For a bank such as Chase to get out of that business, there has to be a good reason. The implications for merchants are that they will need to pick up more of the cost of gift cards through fees or running their own service.

The announcement by Chase didn't say it, but there is an important reason: the Feds have capped the fees that can be charged per swipe. That means that gift cards can't be as profitable to the banks as they have been in the past. Not only were the fees capped, but now a judge has ordered the Feds to lower them further. The costs of the gift card system had been covered through those higher swipe fees. Now that those fees are reduced, the merchants will need to pay for gift card services some other way.

Gift card systems are expensive to build. While credit and debit systems are a lot more expensive to build, they get far more traffic. The cost of a gift card system is spread over a lot fewer cards and much less traffic. These are costs that merchants will need to pay. There will be more pressure to push any customer support costs back to the merchants.

The Chase announcement means that merchants will do well to reconsider the type of gift card they offer. The Chase cards were "open loop" and the money could be used anywhere. If the merchant is going to pay for more of the cost of a gift card system, then it makes sense to use the gift cards to drive traffic back to the stores. "Closed loop" systems do a better job of that.

A Consultant's View is published by Prairie Trail Software, Inc.,

Making *Information* from Streams of Data

1-800-618-4199

www.prairietrail.com

Risky World

On June 13, in the maximum security wing of a Florida prison, all the doors opened at once. Researchers have found security bugs in many prison computer systems and have shown how people outside the prison could open the doors. Many prison computers are connected to the internet with no protection.

Prairie Trail Software, Inc

3821 Beaumont Lane
Plano, TX 75023

Address Service Requested

Prairie Trail Software, Inc.

Making *Information* from Streams of Data

Custom Gift and Loyalty Solutions

For the Retail and Restaurant Trade

We provide technology for

Merchant Services

We pull the whole system together
- or just the parts you need

Gift and Loyalty Card Servers

Database Design and Management

Web Services and Portals

Dial up and IP Servers

Terminal Software

Custom solutions to meet your needs

Call 1800-618-4199
www.prairietrail.com