A Consultant's View

Vol. XXI No. 3 March 2014

Lessons from the Target Breach

Last year's attack on Target shows some serious problems with the credit card network. A key lesson is that if a credit card image exists in memory of any PC POS system, it will be stolen. The push for upgrading to EMV is only a bandage on the problem, not a complete solution.

A technical analysis of the virus that got to Target shows a number of factors. One is that the virus scans memory for anything that looks like a credit card track image. That has important implications. PCI requirements have (hopefully) eliminated the card track images on disk. However, this virus can capture the card track images that are in the input buffer and in the buffer used by the request message sent to the authorizer.

There are only two solutions that will eliminate this problem. One is to send each input byte to the host as it is read in and never have the full track data in memory at once. This solution still leaves card track images within host and network computers where they can be captured. The other solution is to encrypt the card image inside the card reader. End to end encryption is the only way to prevent viruses from getting card data.

However, that is a very expensive solution. The biggest problem with that solution is that most host systems and protocols are not designed to handle encrypted card track information. In order to make that solution happen, all those systems will need to be redesigned, recoded, and recertified.

The push by Visa to adopt EMV is only a bandage. All it does is to make such stolen card numbers harder to use at a face to face checkout lane by requiring the person presenting the card to know some extra piece of information. It does nothing for online sales (which are the fastest growing sales). Because it does not help with the future, it is a tacit agreement that credit card numbers will continue to be stolen.

No Network is Perfectly Secure

The lead security standards architect for the PCI Council testified that EMV would not have prevented the Target leak.

The current system assumes that we can design perfectly secure networks. That assumption is false because we are all human. At the current rate, we can be sure that eventually, someone will figure out how to get inside the Visa network (most likely through human engineering). The current system has deep flaws and will continue to be broken into.

Those flaws in the current system were highlighted in the Congressional hearings. The general manager for the PCI Council testified that passwords for the network and device access are the weak point of the whole system. Back when VeriFone devices were the dominant credit card device, the hacker magazine published the system password that most devices used. Today, such passwords still get out into the hacker community.

The network can still be hacked and will be hacked again in the future.

Amateur Bankers

As the west was being settled, it was a fairly lawless place. Often, the richest person in a small town would be the only person with a safe. Thus, he became the banker for the town. As Texas became a state, those were chartered as State Banks and often continued as simply one person lending money to his neighbors. These lasted until the oil bust of the 1980's when most of the last of these went under. As they were state chartered, the depositors got no money back.

We are seeing something very similar with the Bitcoin craze. That whole area is full of amateur bankers. Many of them started as gaming servers, not financial service providers. The result is that they did not have the systems and protections in place to be able to handle professional criminals. There are no charters or insurance behind those banks.

During the 1980's, Texas forced all remaining state chartered banks to switch to Federal charters with the attendant insurance, required processes and systems, and federal oversight of how they operated. The result was that the banks had to change their internal operations and add a lot more controls. They had to become professional bankers.

Bitcoin banks can continue. However, the Bitcoin system would benefit from the experiences of those who are fighting the criminals on a daily basis. We do not need to regulate Bitcoin, but we may want to regulate the Bitcoin exchanges and banks. Depositors and exchange customers may eventually demand better systems and some type of insurance.

Financial systems eventually require professionals running the place.

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

Dan Greer in a talk on security mentioned that at one time, we tried to protect organizations. Then, we tried to protect departments, then individual computers. Every time the risk goes up, the unit to protect gets smaller. We are now at the point where we need to protect individual data items such as card swipes.

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