By Johl J. Kennedy, Co-Founder and CIO for Crystal IT, Inc.
October 1, 2010

www.crystalit.us
888.875.3646

IT Security and Smart Cards

Identity theft…loss of intellectual property…data loss…when are we going to get a handle on IT security? I can tell you that it won't happen until we open our eyes to what we are currently doing and make the changes accordingly.

Pick up any news line on any given day and the headlines relating to IT security breaches are scary:

> Data Theft from Firms Topped a Trillion Dollars in 2008, companies surveyed estimated they lost a combined 4.6 billion dollars worth of intellectual property, and spent approximately 600 million dollars repairing damage from data breaches…and that's only the ones that have actually been discovered and reported.
>
> How do breaches occur? According to the 2010 Data Breach Investigations Report, 48% involved privilege misuse. Related to the larger proportion of insiders, misuse sits atop the list of threat actions leading to breaches in 2009.
>
> My personal favorite which puts it all into perspective and proves that we better take action before some astronomical incident happens cites 103 Different Countries Breached. Let me clarify…that is 103 governments who only seek out the best in their country to lead IT initiatives and protect highly classified information, all outfoxed. Simply put, this tells us that what the world is doing right now to secure sensitive data is just not working.

The truth is far worse than Hollywood portrayed in the Bruce Willis movie *Live Free Die Hard, 2007*. If you recall, John McClane takes on an Internet-based terrorist organization that is systematically shutting down the United States. Are we at the brink of this potentially happening? Could it possibly be global?

Although there are many areas that could be addressed within IT security, none I think has as large of an impact to us as this one:

The use of Smart Cards and the reason why we cannot stop or even slow down the rise of data loss.

There is a documented video done by Wired with Chris Tarnovsky, an Independent Contractor, hacking one of the generations of a Smart Card chip. He goes into the process he used to hack a chip and gain access, which allowed him to even watch the process as it decrypted the data. In another article demonstrating a Smart Card hacking trick, a student at the University of Virginia found a way to hack into MiFare Classic, one of the most common cards in the entry-level Smart Card market. The exploit affected up to 2 billion Smart Cards that open doors and board public transportation systems.

After having us use and implement this technology for a few years and watching the product life-cycle progression, it should be clear to see that it is in a cyclical state: Hackers find flaws in the technology; the Smart Card industry rushes to try to find ways to circumvent the flaws and then releases a fix; hackers find *new* flaws. This is insanity. As Albert Einstein once said, "Insanity is doing the same thing over and over again and expecting a different result."

Is that not what we are doing when we continue to use Smart Cards for sensitive data and security? Time and time again it fails…and fails at an alarming rate. Meanwhile, the security industry continues to try to find new ways to implement this technology – putting even *more* sensitive data on these cards.

So let's just jump into the number one flaw in Smart Card technology that, no matter how hard we try, we can't overcome or circumvent? We are storing sensitive information on a small chip/card that has the ability to disappear and wind up half way around the globe to be hacked into within weeks or even days. This is a flaw and a feature that *cannot* be corrected. Quite frankly, we should have never used Smart Cards for storing sensitivity data and/or security as a whole. Ironically, this is the major selling point for the technology.

When looking at the architecture of Smart Cards, the ability to share information stored within the card between vendors is one of its best selling features and is also its biggest security problems. As everyone is aware, Smart Cards are encrypted. What is not so obvious….the encryption key to unlocking the encrypted data is stored on the chip embedded within the Smart Card itself. Since Smart Cards are in circulation for both physical and logical security access, the potential for compromise is immense. This "flaw" not only affects the targeted company attacked but could affect any organization that was sold that particular chip design.

Today, we have government policies, legislation and laws being passed that require a flawed security technology, Smart Cards, as an integral part of our IT security platform moving forward. After speaking to technical experts across the world, it is apparent that everyone is falling into this category…so don't think it's just the United States.

To this day, two years after these findings, we are still seeing mass deployment at an alarming rate of this unsecure, breach-prone technology. Many falsely believe their "new and improved" next-generation Smart Cards are not vulnerable to the risk of those in the days past. For example, in an article written in August of 2010, Concerns raised over security of new German ID cards, the Minister of Interior, Thomas de Maiziere is quoted as saying, "With these new ID card, we have the highest-ever level of security for all legally binding online activities". Yet, with simple spying Malware, they can be hacked. This time, the government's current loss is only at $30.5 million for deploying an inadequate technology – with later unknown costs associated with identity theft and data loss because the cards are not yet in circulation.

When discussing Smart Cards with other IT security experts, their first question is always the same, "What can we do to make them safe and secure for our needs?" My response remains, "Don't store sensitive data on them, and most definitely don't use them for identity verification" (where the user's identity is validated based on information found on that card).

A little user feedback can go a long way if you truly listen to what is being said. Last year, I had the pleasure of touring multiple military bases from various branches and spoke with officials required to utilize Smart Cards for their physical and logical access security. The number one user gripe was …… any guesses? Leaving the card in a workstation terminal and then not having it in the morning when the card is needed to gain base access. Who has had access to the base overnight while the card was left within that terminal – imagine if it was lost or stolen. What is the number one flaw again?

So where do we go from here. First thing first, we need to stop implementing something that we know is part of the problem. Smart Cards must be replaced and taken out of circulation to stop the threat embedded within them. There is hesitation to do such because of the financial burden, the man hours wasted, the inconvenience in replacing them all and the negative publicity that goes along with it. However, the damage that continues by Smart Card use cannot yet be measured. By embracing new emerging IT security technologies, we are able to protect data without jeopardizing the security of our nations, industries, and people as a whole.

References:
Data Theft from Firms Topped a Trillion Dollars in 2008 http://www.google.com/hostednews/afp/article/ALeqM5jZcC6eKWlbhXG-xvRYDJKZgcKPng
2010 Data Breach Investigations Report http://www.verizonbusiness.com/resources/reports/rp_2010-data-breach-report_en_xg.pdf
103 Different Countries Breached: http://www.timesonline.co.uk/tol/news/uk/crime/article5996253.ece
Documented Video http://www.wired.com/video/security/security/9525752001/hack-a-sattv-smart-card/1813637610
Smart Card Hacking Trick http://www.financetechnews.com/smartcard-hacking-trick/
Government Policies: GSA Smart Card Standards and Interoperability http://www.idmanagement.gov/smartcard/
Concerns Raised Over Security of New German ID Cards http://www.dw-world.de/dw/article/0,,5945076,00.html