XceedID™
Xceeding The Ordinary

Old Proximity Technology Provides No Security

Whether you are a security manufacturer, security integrator or end user of security products, you have a responsibility to utilize products that are cost effective without compromising security features. As security professionals if you can implement proven, reliable, access card and reader technology that offers security for the same price as a similar product that provides no security which product would you use?

Today in North America, and for a decade in Europe, 13.56 MHz contactless smart card technology is next generation proximity. Older proximity technology, such as the familiar prox card and reader products a majority of companies use, offer *no* security. To illustrate, the radio frequency (RF) communication between the most popular proximity credential and the respective reader is broadcast *in the clear*. That is, the communication is a license plate (a static number) transaction of a given number from the card to the reader. Anyone skilled in the art of RFID could, with appropriate readily available equipment, *listen* to this communication and duplicate the transaction.

In contrast, with secure contactless smart card technology (such as XceedID® ISO-X™, MIFARE™, or DESFire™) the communication between card and reader is *authenticated*. This means that prior to communicating a number (which changes with every transaction), there is actually a three pass mutual authentication. The card and reader actually pre-communicate to ensure that they belong to each other. Using these security measures renders attempts to *listen* to the transaction useless because the message is scrambled. Deciphering this type of secure communication is not a trivial process.

As an analogy, most people have had some experience with internet commerce. Today, most sites offering something for sale employ, at a minimum, SSL (secure socket layer) security to ensure you have a secure environment for the transaction. Would anyone today transact business on a site that was not secure? Of course not. Why then would anyone that claims to be a professional in the security business continue to promote the use of products to protect their assets that do not employ basic security measures?

There are many additional value-add benefits to contactless smart cards. Currently the most widespread application in security, beyond use on a standard RF Reader, is the storage of biometric templates on the smart card. Other uses include applications on the card such as cashless vending, logical access, etc.

At the most fundamental level, for use in access control to open doors, contactless smart card technology is the new generation of proximity. The user experience is the same for old prox cards and new contactless smart cards. Simply present a card near a reader and the reader “beeps” and you are either granted or denied access. However, with one technology you have a secure transaction and with the other there is *no* security. As security professionals in the new millennium which technology should be the standard for every project? I know how most professionals would respond. What do you think?

Oh, and one more crucial point, the cost for contactless smart cards and readers is virtually the same as old proximity and in some cases even less for cards. If anyone tells you differently they simply aren’t in the game.

John Menzel, CEO and president of XceedID Corporation.