Access Control With High Security Credentials

Nicklas Lindstrom and Michael Kapusta
Department of Automatic Control, Lund University

Have you ever lost your house-key and thus been forced to change the lock, a most expansive and hassling endeavor. Now lets change the scope! What if a company- or government-employee lost their key and that organization had hundreds of other users using the same key? But most Companies and Governments use smart cards and not keys right? Well unfortunately in most cases using a smart-card is a lot less safe for the company than simply loosing a key. With the latest technology in electronic access control these security issues can be solved!

Developing electronic security

Developing security regardless of its format is a constant cat and mouse game were adversaries are either in the midst of trying to crack your solution, or they may have already cracked it. A cryptographic algorithm may be uncrackable from a mathematical perspective but as long as a human being is the one developing the solution, a human error is always feasible.

How can a developer create a secure solution, when the developer per definition is what makes the solution unsecure? The answer to that question is that the developer lets other non-associated developers test the solution until it's deemed secure before using it in a security context, thus making the solution an **open-source solution**. A open-source solution is never secret, thus whomever wants to will be able to gain detailed knowledge about how the solution works. The latest technology in electronic access mends a wide scope of different open-sourced security solution to create a secure electronic access solution.

Most smart cards are not safe

Most smart cards currently used on the market are closed-source solutions, this means that they are based on technologies that have not been widely tested on non-associated developers. A closed-source solution is a secret solution and unless you are the one developing the solution you should not be able to gain knowledge about how the solution works. Attackers have proven that close-source solutions never remain secrets as they eventually are disclosed because of human errors in the closed-source solutions. Thus enabling the human error to manifest as major security issues within the smart cards solutions. Many smart cards used on the market are deemed unsafe, thus giving the users a false sense of security.

Your smartphone is the new key

The United States Department of Defense (DOD) recognizes the issues of creating a system binding credentials of the users to a specific piece of identification. Thus the DOD put a lot effort to come up with secure open-source solutions to the given issue.

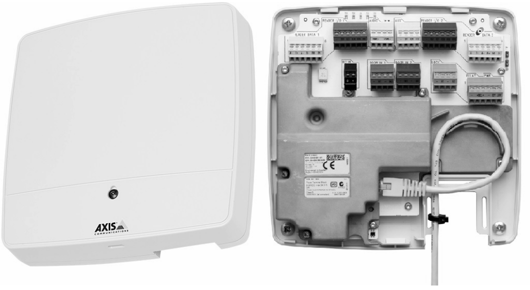
One of the open-sourced solutions developed by DOD is named **Derived-CIV**. Derived-CIV describes the structure of a secure authentication protocol between a smart-phone and a computer-system. To clarify, Derived-CIV describes how a smart phone can act as a key and a computer-system as the lock that opens the door. The Derived-CIV solution does however need cryptographic help to be securely implemented. Cryptography help that can be given by the same library of solutions that secures the internet for us on daily basis, also known as **OpenSSL**. OpenSSL is a library of open-source solutions which are used to enable protection against eavesdropping between computers. Thus OpenSSL is used by your web browser whenever your connection needs to be encrypted. A big part of OpenSSL is the fact that two parties via encryption can authenticate each other, authentication in the sense of proving each others identities. OpenSSL authentication is for example used so that you can be sure that you are browsing the actual website of your bank and not a fake one, as your bank can identify itself.

The electronic lock

The computer system to act as the lock must be able to handle both a multitude of people and doors, what better to do this than the **A1001 Network Door Controller** developed by Axis Communications. The A1001 Network Door Controller is a open-source platform that enables readers, door locks and user identities to be manged simply by browsing it from your web browser.

By developing a solution that combines Derived-CIV and OpenSSL, the A1001 can assert that a users smart phone is the correct one, thus opening the door.

The future of access control is key free, smart card free and most importantly safe!



Axis A1001 Network Door Controller.