As published on M2MNOW

Convenience, the Bane of Security and Privacy

19 October, 2015 at 7:00 AM

This is about an issue which I believe is the ultimate cause of many if not all technology challenges we face today, particularly in the area of Security and Privacy. The issue is that almost everyone exposed to technology either as user, service provider, manufacturer or developer, when faced with a choice between right and convenient, will chose the latter. And that is where the trouble starts. Below I have given a few examples of where it has lead us.

Image courtesy of David Castillo Dominici at FreeDigitalPhotos.net

Data Breaches as a result of Buffer Overflows

Data breaches, excluding those resulting from social engineering, have one thing in common, namely buffer overflows. These buffer overflows occur, because someone conveniently forgot to check that the variable being copied actually fits into the destination memory reserved. Granted, it is very inconvenient and tedious for a developer to have to write the code to perform these checks and then to handle the exceptions, but it really pays off. During my time in one of the major banks in London, I was once responsible for the development of a piece of software, which should not ever crash or be breached or else… My rule was simple. 'Everything gets checked and no use of clever side-effects or anything else obscure'. I can still hear the complaints from my team today. They told me it was difficult and was going to take a long time, most inconvenient to a project manager but it resulted in a piece of software which never failed and was never breached.

Connected Cars

Earlier this year, in preparation for the Las Vegas Black Hat conference, a group of researchers broke into a car remotely, while it was on the road. The break-in occurred via the car's infotainment system. From there the researchers were able to take control over the car. Why was this possible? In this car the infotainment system was not sufficiently segregated from the other services, unlike cars offered by some competitors. Why did that happen? Most likely the development team was under time-pressure to deliver and therefore conveniently omitted implementing a strictly segregated, secure system as too hard, too costly or too time consuming, with the argument that implementing it properly will put the delivery time line at risk.

Contactless Payment Cards

Image courtesy of tiramisustudio at FreeDigitalPhotos.net

A prime example of mistaken user convenience, as well as service provider convenience, is the NFC contactless payment card. While the banking industry maintains these cards are secure, the UK Consumer Association "Which?" showed in April 2015 that it is possible to skim card information from NFC enabled contactless payment cards for use online. A UK newspaper article from late last year highlights a flaw which showed how payment cards might be tricked into transferring large sums to a fraudster. Securing these cards is, in my view, not possible without mandating a real-time connection to from the payment terminal to some trusted server. This is hard, costly and rather inconvenient to implement and operate, hence unlikely to happen.

Is the IoT different?

With the IoT it might have been different, but in reality it is not. Almost all of us are happily careering headlong down the path of convenience at the expense of security and privacy. The FBI recommendation to give up on some of the convenience and keep IoT devices in its broadest definition far away from any network, is surely a good indication how bad is has become.