Information Security Now – 43

IoT Security - Fixing the Problem

John Mitchell

Being worried that my new fridge would unilaterally put me a diet and having read about criminals compromising cars' keyless entry systems, plus having seen the video of that jeep being run off the road after its engine management system had been remotely compromised, I asked my vehicle's manufacturer whether my car was firewalled? The answer was no, but I need not worry because everything was encrypted. Ditto with the fridge, washing machine, central heating and my burglar alarm system. Well, if encryption was the answer, then we would not have suffered fridges being compromised to send spam, or cars being driven off the road. Before fixing a problem, you need to understand it.

Anything to do with IT security tends to be based around the CIA triage of confidentiality, integrity & availability. The Internet of Things (IoT) is no different. My house is effectively firewalled through my router and any internal devices connected to my private home network are behind this firewall. Because it is a software firewall, it is not the best protection in the world and any weaknesses will be known to the hackers, but much like a burglar alarm it may send them elsewhere where the pickings are easier. Likewise, my attached computing devices have their own firewalls, so access to them now requires the hacker to circumnavigate two firewalls. Nothing like a bit of protection in depth. But what about my other devices, such the central heating, fridge, coffee machine and burglar alarm? Here the protection is less secure in that they are totally reliant on the firewall in my router, plus the standard one factor authentication at log-in. So, confidentiality is undoubtedly a problem, but what about integrity and availability? The compromised fridge sending spam emails illustrates the integrity problem. If code can be so easily amended, or overwritten, then almost any connected device can be altered to do whatever the hacker wants it to do. It is, after all, based on a general-purpose chip. The final part of the triage, availability, is a key factor for my central heating and burglar alarm. I can probably manage with the fridge, or coffee machine being disconnected from the internet, but not these. Simply knocking out my router makes every device on my home network unavailable to me from outside; a denial of service attack. These problems assume that my devices are in a private network behind a firewall, but my car is effectively accessed through a public network without such a shield. Protection of driverless vehicles will be a nightmare.

Now that we know what the problems are, let us examine what the solutions may be. Basically, we need to apply risk management techniques, but with a skew towards the consequence part of the equation, rather than the likelihood. This is because of my pessimism in our inability to prevent hackers from gaining access. So, let's assume that the hackers have got through. What can they do and what is the fall-out?

Thinking of my home network first. I am unusual in having two routers from separate service providers, so both routers must be knocked out for a complete denial of service. Perhaps this is the way that homes should go in the future? An additional cost it may be, but then it becomes a standard cost-benefit appraisal. Are you willing to pay (say) an additional few hundred pounds per year for service availability? On the integrity side, perhaps all internal code should be signed with an electronic signature, so that every time the software is loaded the signature is checked? Thus, if the code is altered without authority the signature is invalidated and a message is sent to the manufacturer alerting them to the hack. In fact, it could go further by immediately overwriting the corrupted code with the authorised version, as is currently the case with my web site's front page. You will notice that this is fast detection/correction, rather than prevention; because I am assuming that the hackers will invariably find a way around my prevention mechanisms. Having dealt with availability and integrity I now come to the problem of confidentiality, which is all about identification, authentication and privilege allocation. Most devices will be using a chip containing an operating system and an application. Control of the OS will provide for control over the application, so protection here is paramount. Most systems come with an engineering back-door so this must be disabled. Administrator privileges must be withdrawn and the barebones OS should only provide for the running of the application. The application itself will most likely provide for some user interaction. For example, my fridge may require my personalised list of goodies so that it can automatically place an order with my victuals supplier when things are running low. As there are several members of my family, each with differing requirements, then there may be several different log-in credentials (my coffee machine can already manage several different profiles). So, we now come to the authentication dilemma. Single factor authentication through a traditional password is no longer good enough. Two, or even three factor authentication is becoming common, but I do not want separate tokens for each connected device. Neither do I want the potential hazard of single sign-on, which could mean all my devices being compromised if one of them is. No, I want a different sign-on for each user of each separate device, but I don't want to have separate tokens for each one. The answer would appear to be digital signatures using a public key infrastructure (KPI). Well, the best of luck there, but perhaps our Chartered Institute for IT could help in influencing a common solution?

Now, although all the above are discussed with reference to my home network sitting behind a firewall, they could be extended to include devices on a public network without such protection. If we assume that the hackers will always get through, then fast detection/correction of attempts to amend code, or data, should be included in any device. Service unavailability, can be dealt with in the context of risk management. If the service becomes unavailable what is the consequence? In many cases, it may not matter too much, but if it is a driverless car, then you need to fail-safe and stop the vehicle. Grid-lock on the M25 once more?

John is Managing Director of LHS Business Control, a corporate governance consultancy. He is a member of BCS Council, it's Risk Audit & Finance Committee and is an active member of the Information Risk Management and Assurance (IRMA) specialist group. He can be contacted at: john@lhscontrol.com, www.lhscontrol.com, or on +44 (0)7774 145638.