Working Paper 1

Cyber Security and Building Services

David Fisk
Laing O'Rourke Centre for Systems & Innovation

Summary

Extending the power of building management systems has led to the wide adoption of proprietary 'enterprise' software platforms. The PC user is only too familiar with the vulnerability of networked computers to malicious software. But it is only recently that attention has been paid to the possibility of virus damage to process controllers. The hazard to BMS function is real but the risk is difficult to assess. Pressures on BMS procurement and upgrades aimed at improving functionality bring with them increased exposure to risk of a successful attack. The key defence is to ensure a ‘fall-back‘ ‘black start‘ capability.

1 Introduction

Users of PC’s are only too familiar with viruses and invest $2B each year in virus protection software. Viruses exist because of two factors. First software providers need platforms that can be upgraded and modified to avoid becoming ‘electronic concrete’. Second there is the malicious streak in human nature. Few employees could write the computer code for Word but they can, care of Microsoft’s Macro language, Visual Basic for Applications, that comes shipped with Office, write a Word macro that will delete recipients’ hard disks when they open the attachment! Why have a word macro language that is that powerful? Presumably, it is because Microsoft could. So a standard PC has the capability to accept instructions, not just from the keyboard but from the network to which it is connected. Being morality free it cannot tell malicious instructions from the benign. All this is familiar with the owners of the world’s billion PC’s. But isn’t the buildings Building Management Systems – once a hard wired data logger box – now a PC as well?

2 Cyber security and process controllers

Original 1980’s BMS were dedicated hard-wired machines. But once data communication protocols were available it became plausible to use the same software platforms that were being used by the enterprise’s own network. That enabled satellite outstations with real computing power and the capability for outstations to receive instructions that changed or loaded programs as well as executing them. But software engineering seemed so obsessed with the idea of malicious software getting access to corporate and personal data that the idea
that the same hacking techniques could be used to cause hardware to malfunction was hardly every spoken about.

In 2010 a PC in Iran began to repeatedly reboot itself. That would sound familiar to PC owners who have suffered a virus attack. What was not familiar was that the virus, now labelled Stuxnet, turned out to be enormous – around 15,000 lines of code (Weinberg 2011). These days with hard drives so large and download speeds so fast who would have noticed it spreading through a network? But the other odd thing about it was that it only sought to communicate on a Windows network with other devices that were running Step7 the Siemens systems used in programmable logic controllers. Siemens are of course one of the world’s largest manufacturers of controls and control systems. Their devices are everywhere. They dominate much of the Smart Grid market. Industrial controllers are not themselves usually connected to the internet, just to keep them quarantined. But Stuxnet had another feature. It installed itself on any USB drive inserted in the infected system and then, like flu, went where ever the drive went next. Let us hope that conference data projector you last used was clean! But so what? What was it supposed to do? Unfortunately staring at 15,000 lines of code you can only tell what it will do when it does it. The suspicion is that it stopped the Iran uranium enrichment programme for a while in 2009. Civilians will never know.

3 Smart Grid Vulnerability

Stuxnet is now supposedly patched. Which is all well to the good since software systems engineering is tending to move away from a quarantined control systems to fully integrated information systems embedded in enterprise software. But the idea is out – viruses can infect plant controllers. The current Big Threat is the Smart Grid. ‘Smart’ is the New Dumb as they would say in Vogue. Power engineers have been here before. The massive North American power failure in 2003 was initiated by an unexceptional grid line fault. But the failure to contain it to one US State was due to a failure in the IT system that supported the regional systems control. That was a software glitch, called a running bug, which overloaded data terminals until their screens were refreshing slower than lines were tripping out. So power engineers have had their warning software can wreck hardware. So have other systems engineers. The NY telephone system remained up in the four day black out – unfortunately the telephone key pads in coin boxes were run by mains power so the systems were useless.

Smart Grids rapid roll outs are the kind of fluffy things we have learnt to expect in EC Ministerial declarations. These promise us demand side management with the BMS eventually dealing directly with the power network’s own software network. But the US Government estimate that the business for cyber security on the Smart Grid is around $21B over the next 5 years. ASHRAE is already involved in some of the standards. So it is time to sit up.

Stuxnet got through a vulnerability in the Windows platform. That has been fixed. But support for Windows XP SP2 ended last July if that is what is steaming the old BMS in the basement. It is best not even to mention Vista Release to
Manufacturing. ICT Departments upgrade their systems almost every day. But is this true for BMS? Because high profile hardware hacking has gone for high profile targets (such as the Port of Houston, the Washington rail network, and a nuclear power station in Ohio just to mention three! (Flannagan 2011) ) modest building services have hardly had a mention. But the coin is beginning to drop that enthusiasm for all things digital (there is even a dedicated acronym CAFM - Computer Aided Facilities Management) is opening up heavily serviced buildings to the risk of attack.

Designing a system that is more robust while being more powerful is not impossible. The historical data from the BMS (pump run times etc) that might be useful to enterprise software can be located in a server sitting between firewalls to the enterprise and BMS systems. That also enables ‘each to his own’ when it comes to the engineering. But at the moment we are a long way off a secure ‘Web of Things’. And of course there is the service engineer and the now ubiquitous laptop plugged into the system from time to time.

For the process engineer there is a lot of good geek advice on the Web. The Siemens patch for Stuxnet (Siemens 2011) gives a flavour. It is not for those faint hearted facilities managers who rely on their kids to reboot the home computer! Unfortunately the Web also contains a lot of less helpful advice. The hard-wired password in Siemens’ controllers that let the virus ‘in’ was on the Web in 2009!

4 Worst Case Defences

Surely the engineering truth is that we should not rely on the computer industry to ever solve virus attack, though we can rely on them to charge us for trying. Software companies do try their utmost to contain the menace. Microsoft is only too aware that Apple trade on the superior virus resistance of the latter’s products. But, just as every home cannot be really protected from the determined burglar without the house ceasing to be a home, ‘bad things’ will happen. Software engineering is by its nature a ‘compliance’ culture (just like building services engineering!) in an engineering science where there is a counter-strategy to every strategy and a lot of socially autistic hackers. There are also a lot of buildings occupied by high profile or not very popular businesses. If so what to do about the BMS threat, beyond paying for more software? On an aircraft carrier there are very sophisticated computer-GPS positioning systems, but the Captain also has a sextant in a drawer in his cabin – ‘just in case’ the enemy jam the signal. Maybe we need to audit our systems to understand how many have minimal ‘just in case’ functionality for the worst case scenario? The enterprise data centre might be firewall protected but can its AC system be hardwired restarted if its firmware has been corrupted? The standby generator may have tripped in because the Smart Grid has just tripped out, but just how did it do that and were there virtual keystrokes on the BMS that would have turned it straight off again? What floor area and particularly key circulation spaces are naturally lit when the emergency lighting refuses to acknowledge there is an emergency? Don’t let us even mention the lift controllers. Yet even in the Italian Job, when Michael Caine has disabled the entire Milanese traffic
signals system, there were at least traffic cops around to try and do something. Not very effectively, but at least they had a whistle.

The only truly secure computer is one that is never connected to the external world through any device. But unless it is an Airbus auto-pilot, this is also the most useless. Even the disconnected computer may be vulnerable to certain kinds of stand-off, electromagnetic attacks that disable circuitry. The battle between the industry and the hackers is an example of the asymmetric warfare that is more usually discussed in the context of counter-terrorism. The industry has to guard against all future possible vulnerabilities in systems which may have a 10-20 year lifecycle whilst the hacker only has to find a single entry point.

So cyber security is a hazard but how big a threat? For major infrastructure the threat is real and Governments are committed to doing something about it – though rather unnerving for services engineers, it is the Foreign Office not DECC or DCLG who have made the most running in the UK. No wonder it is an FCO issue. The entire water supply to Kuwait City in the First Gulf war was knocked out within the first hours of hostilities by a single smart bomb that detonated in the waterworks control room. Everything else on site remained pristine and intact. Now it seems you would not even need to cause that amount of damage to get that amount of effect. A virus despatched thousands of miles away could just lock down the system for you. So, out of civilian control, we must surely assume that the techniques to implement hardware attacks through software are going to become ever more sophisticated and prevalent - arms proliferation of a different kind. There is a modern habit of spending days ranking threats rather than just deploying quietly the good old explorer’s adage of hope for the best (after all modern supervisory control and acquisition (SCADA) systems are brilliant) but plan for the worst (they can just die it seems so what then is still working?). Buildings services are much easier to assess than many process plant or grids so maybe we should just get on with it.

5 Conclusion

Stuxnet is disabled, but the war is not over. In 2008 a virus now called Conficker began to infect computer systems. Within 18 months it had spread to 8 million computers worldwide (Bowden 2010). Maybe that includes the one on which this paper is written, because to date no one knows what it will do, and PC owners are unlikely to know they have it. Like good old Windows Updates but in reverse, the virus (elevated up the nasty software taxonomy to a ‘worm’) receives patches from ‘out there’ that close vulnerabilities to the anti-malware programmes you have bought, all while it sits quietly on your hard drive. Not that this neat feature matters all that much on those machines where it has already disabled Windows Automatic Update without the owner noticing!

Tomorrow Conficker might wake up. Will your building’s lights go out, or just flash on and off a Xmas tree for all to see? Where, come to mention it, was the CEO when it happened? In the lift?
Acknowledgements

The author is grateful for a number of discussions with colleagues in the control and power industries and helpful comments from staff at the Imperial Institute for Security Institute (http://www3.imperial.ac.uk/securityinstitute)

6 References

Bowden M 2010 The Enemy Within The Atlantic June
Flanagan S 2011 Critical Infrastructure Program May Southwest Power Pool CP Workshop
Kurtalji, N 2011 Cyber security Feb AutomatedBuildings.com
Weinberg S 2011 Is This the start of Cyber warfare? Nature 474 142 – 145

©David Fisk Imperial College London