New Data Security Guidelines for Smart Buildings and Utilities

Date	03/09/2012
Version	1.1
Authors	Anton Hofland & Bruce deGrazia

Introduction

Everyone in the real estate and utility industry, manufacturers and operators alike, is convinced of the benefits of computer control of buildings and utilities. At the recent RealComm/IBCom conference, which took place in June of 2012 in Las Vegas, speakers and exhibitors presented clear examples. Benefits were realised both in terms of comfort for those who spend large amounts of their daily time in that building, as well as the building's operators, who end up managing more efficiently and saving expenses, including energy expenses.

However, there is a huge Damocles sword hanging over the Intelligent Building and Utility industry --the sword of cyber-attack. The construction of control systems for buildings and utilities and their thoughtless connection to the internet, a huge target for hackers – both those wanting to make occupants and operators lives uncomfortable, and those looking to wreak havoc on the daily lives of all who occupy the buildings and depend on the utilities.

Recently found weaknesses

The stream of discovered weaknesses in computing equipment, systems and infrastructure is rapidly increasing. Serious problems have recently been discovered in the Tridium Niagara platform, which is a platform that is very popular in the Intelligent Building industry and has found wide adoption. As a result of these identified weaknesses many buildings and utilities are now at risk of a cyber-attack – an attack that would likely take an experienced hacker no more than a few minutes to perpetrate and do its damage.

Of course, it is not just Tridium systems that have well known and well publicized weaknesses. There are many such systems whose weaknesses are so well known in the hacker world that web sites exists where a potential attacker need only enter some details and be presented with all the information required to take over control over a building's systems.

At the annual Black Hat conference, which also took place in Las Vegas recently, an attack vector called Rakshasa was presented that uses the firmware of computer systems, disk drives or third party adapters to introduce so-called back doors into systems in a way that cannot be eradicated by any known solution. And while this type of attack is at present theoretical, its practical deployment is definitely well within the reach of Nation States. And unfortunately, no amount of technology will save you should this type of attack become reality.

Introduction to the Cyber Security Act

Clearly something needs to be done to avoid a catastrophic successful attack on building automation systems. Senator Joe Lieberman from Connecticut, representing a bi-partisan group of legislators, crafted an approach in the Cyber Security Act 2012, recently considered by the U.S. Senate.

The act calls for:

1. The establishment of a National Cyber Security Council which would be an interagency body with representatives from the Departments of Defense, Justice and Commerce as well as members from the intelligence fraternity and other appropriate

Federal Agencies with responsibility for security of critical infrastructure. The council would be chaired by the Department of Homeland Security.

2. A risk assessment which would determine which sectors are most at risk from cyber-attacks.

3. The creation of infrastructure categories most at risk.

4. The establishment of a public-private partnership to address the identified risks. This partnership would consist of industry led groups which would establish voluntary cyber security practices for each industry sector. These practices would then be reviewed by the National Cyber Security Council.

5. The incentivized adoption of the approved, sector specific cyber security practices. Incentives would include preferential treatment in awarding Federal contracts for those adopting the practices, the use of a certification mark for marketing purposes, and liability protection from any punitive damages in a lawsuit arising from a cyber-security incident. Also, security clearances would receive expedited treatment, threat information would be shared real-time with industry and there would be technical assistance from the Government with cyber issues.

6. The establishment of Cyber Security information exchanges where private sector and government can both post and obtain information about cyber-security threats and incidents.

7. The creation of a coordinated Cyber Security Research and Development program in which the private sector, along with universities and other institutes of research and higher education cooperate to develop new technologies.

In practice the Act would have meant that the various real estate and utility industry sectors would have had to coordinate with the trade organizations to influence the way in which practices are established in a sector. Further, as an initial step, those who operate buildings or utilities that would have been classified with almost 100% certainty as critical cyber infrastructure would have been wise to undertake a security assessment at the earliest opportunity. With the assessment in hand they would have been able to contribute and negotiate from a position of strength.

The status of the Cyber Security Act 2012

Why past tense? Politics. The Act did not get approved this year and will almost certainly not be approved until at least the end of this year or next – if at all. In the meantime, the risk of a cyber-attack increases on a daily basis. And as security is typically seen as an overhead instead of enabler, not many owners or operators are naturally inclined to voluntarily invest in security. Therefore, only some form of government regulation will convince the decision makers to pay heed. Until such time, we shall have to wait until the first significant incident.

Upping the Ante

In June of 2012 David Sanger of the NY Times published a book containing a very graphic description of how the creators of Stuxnet, a cyber-worm that attacked the Iranian Natanz enrichment facility in Iran, went about creating it. According to the book it was the brainchild of a U.S. – Israeli government led initiative that started in 2007 and which was specifically aimed

at the Siemens manufactured control systems which control the enrichment systems at the Natanz facility. The immediate consequences of the release of Stuxnet are documented in the book but the long term consequences of Stuxnet are still unknown. It seems the US and Israel have crossed the Rubicon. It is only a matter of time before we find out who else has. We do not necessarily run nuclear weapons research facilities, but an attack on our own critical infrastructure could be equally devastating.

The Possible Aftermath

There is an unfortunate tendency in the United States -- and in other parts of the West -- to overreact after a disaster, particularly an attack against critical infrastructure. The actions taken by the government after 9/11/2001 bear this out. The Cyber Security Act of 2012 as rejected by the Senate was actually a toned down version of the legislation originally introduced by Senator Lieberman. The bill as originally drafted contemplated a body of regulations with penalties for non-compliance rather than a voluntary scheme with incentives for certification.

If a cyber-attack occurs without legislation in place, the natural reaction will be to put in place the more draconian version of the Act. The best way to avoid this likelihood is for owners and operators to work through their trade associations to pass the Cyber Security Act as it now stands. Because of a procedural manoeuvre taken by the Senate Majority Leader, the bill is still alive and could be brought to the floor of the Senate again and passed in this session of Congress. Failure to do so risks dire consequences.

About the Authors

Anton Hofland, CEO 2024Sight has more than 20 years' experience in IT, IT infrastructure and enterprise networking, gained mostly in the financial industry. Before establishing 2024Sight he was the Head of IT for Arcapita Bank in Bahrain. Previously he has worked for several major financial institutions in the City of London. He has also worked in the area of telecommunications regulation and has experience in the telecommunications industry. Anton holds a M.Sc. in mathematics and computer science from Delft University, Netherlands.

Bruce deGrazia is the **Founder and President of GHSA** (Global Homeland Security Advisors), a leading marketing and government relations firm specializing in representing companies involved in homeland and cyber security. He has an extensive expertise in security and in particular cyber security from the perspective of government, industry, and trade associations. He is the co-founder of HSIA, the Homeland Security Industry Association. Previously he served as Vice President of Versar, Inc. and as Assistant Deputy Under Secretary of Defense for Environmental Quality. Prior to his appointment as ADUSD (EQ), he was an international and environmental attorney for United Technologies. Bruce deGrazia has degrees from DePaul University College of Law and the University of London. He has served as an officer in the United States Navy in Norfolk, Virginia and in the Philippines.