ARE SMART DEVICES A THREAT TO THE INTERNET OR EVEN WORSE OUR HEALTH AND SAFETY?

Gemserv

2

Can you imagine a time in the future where the Internet is not there anymore? If it was broken, or everyone in the world decided to turn it off? Every browser, every device suddenly reported “No Internet, check your network connection”. Close your eyes for a few seconds and think of it all gone, what would that mean to you?

Were your initial thoughts that you would finally have some peace; no-one could send social media messages or emails to you, your smartwatch is suddenly in a restful state; or, maybe you thought of the doom of not having access to online shopping, checking your security cameras, your bank balance and finding out when the next train / bus home is?

It wasn’t that long ago that this time existed, you may remember, like me, that you needed to stand at a bus stop wondering when a bus may arrive, use paper road maps printed on supersized books and try to understand client instructions on where they were based. Working in IT in the 1990’s, I remember typist staff raising fault calls on paper, placed into a tray to be resolved in the order they were laid. I remember making lots of tea (for everyone) whilst waiting for an updated DOS driver to download on the vendors dial-up bulletin board. Resolutions were written by hand and signed off by the client, then the ticket was filed in a cabinet with many others. This seems old fashioned today, and it is; why would we work this way now, when problems can be resolved sitting 500 miles or more away from the physical hardware and staff using technology?

The problem is the Internet that provides this style of remote working, and many, many other services goes wrong every day in some way. Have you ever noticed any major outage other than a local router fault or local cable fault? The Internet was designed to be resilient, you rarely notice faults happening. In security terms we call this **Availability**, making sure something is there and working. There are people that actively attack the Internet, for example, when trying to gain an advantage in the computer game Minecraft[1]. Other attacks happen daily such as border gateway protocol hijacks[2], maybe to aid information. I suspect the original ARPANET engineers, developers of TCP/IP and even Tim Berners-Lee all had one thing in common, they trusted everyone involved. In the 1960’s through to the early 2000’s the group of people involved was limited to their expertise and they had trust in each other.

The ‘information superhighway’, as it was then called, had another big advantage, it was designed to transfer data quickly. What was deemed quick then and now are indisputably very different, I certainly remember my 9600 baud modem struggling to load a single web page but it always did. This falls onto the second security term **Integrity**, making sure something performed as it was intended.

Due to the original trust each of those founders had, the Internet (millions of devices that connect together on one network) has evolved to be insecure by design. This is highlighted in the press almost everyday when information is lost or stolen[3]. Sites such as https://haveibeenpwned.com/ can show just how much information has been breached. This is the last of the major security terms, **Confidentiality**, and a major advantage or disadvantage of computing, the ability to copy everything. Once it is copied and in the wrong ownership it can never be uncopied hence why it is generally big news.

Whatever Internet connected devices are called (such as IoT or Smart), it is essential that they are designed to operate securely. Sadly, to date, this has not been the case for most manufacturers because functionality and usability are the primary design goals. To make matters worse, devices are becoming unsupported by the manufacturers as they move to better, more powerful designs. Think of a Smart LED light bulb that could be used for the next 20 years, will the manufacturers be identifying vulnerabilities and patching throughout its life? Possibly not. These devices are being integrated not only within home networks, but also they are increasingly becoming added onto corporate networks. These devices pose a threat to corporate network availability, integrity and confidentiality and if compromised in enough numbers they can become a threat to the Internet as a whole.

Despite this threat, my own concerns stretch further into the future. As Bruce Schneir wrote, “it used to be that things had computers in them, now there are computers with things attached to them”. Think of a car’s brake system that used to be a pedal linked to a hydraulic fluid system, pushing brake pads onto a disc. This is now a pedal sensor that instructs a computer to drive a motor to apply the brakes. Think about the integrity or availability of this essential system changing when parked, an inconvenience, now think about it happening whilst driving along at speed. Think about a train signalling system integrity or availability being compromised. A computer can be changed to be whatever a programmer (and criminals) want; with safety systems compromised lives are at risk. You may think that nobody would want to do this, triton could be the most

1 https://www.wired.com/story/mirai-botnet-minecraft-scam-brought-down-the-internet/?verso=true

2 https://www.youtube.com/watch?v=9NBv7IKrG1A

3 https://informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

murderous malware to date[4], it can happen. Another thought may be that the likelihood is low because these systems are not directly connected to the Internet, trouble is we love connecting everything to the Internet and the complexity of connected things grows every day.

Computer security matters, every device and supporting cloud service needs to be designed with security in mind as well as focusing on usability and functionality.

SECURITY PRINCIPLES

Strong Account controls:

- Default passwords changed on first time use;
- One user, one account;
- Disallow weak passwords;
- Protect stored passwords with hashing and salting;
- Use best practice methods when allowing users to reset passwords; and
- Advise when password changes are needed due to a suspected compromise.

Managed use of open source code:

- When using open source code make sure it is designed securely and records kept so updates can be monitored.

Use encryption everywhere:

- Encrypt devices;
- Reduce the possibility of data being stolen or changed on the device;
- End-to-end Encryption;
- Communications are encrypted from the sending device to the receiving device (not always via the Internet);
- Encrypt Internet communications;
- Data must be encrypted whenever it moves around the Internet; and
- Encrypt databases containing personal information.

Fail Secure:

- If a device fails, make sure it fails secure.

Think about the cloud interface:

- Cloud interfaces are monitored for security vulnerabilities; and
- Use two factor authentication.

Events and logs are monitored:

- Ensure applications produce security alerts and events for administrators.

Make sure devices are updated throughout their actual lifetime:

- Design devices to automatically update;
- Provide users the ability to allow updates to occur at a suitable time, making sure that all system components update when needed;
- Monitor health;
- Monitor for anomalies within the system;
- Warn users who are not keeping systems up to date;
- Operating systems and drivers; and
- Manage all aspects of the devices design.

Every interconnected device plays a growing part in our safety; it is essential to maintain the integrity and availability of these devices as well as the Internet as a whole.

Gemserv are keen to work with start-ups, manufacturers and general companies using or developing Internet connected devices to make them safer and secure. Please contact us for more information on how we can help.

Further guidance can be found at:

OWASP IoT

https://www.owasp.org/index.php/IoT_Security_Guidance

DCMS Secure by design

https://www.gov.uk/government/publications/secure-by-design

IOT Security Foundation

https://iotsecurityfoundation.org/

Bruce Schneier: Click Here to Kill Everybody

https://www.schneier.com/books/click_here/

4 https://www.technologyreview.com/s/613054/cybersecurity-critical-infrastructure-triton-malware/amp/

LONDON OFFICE

8 Fenchurch Place

London, EC3M 4AJ

Telephone: 020 7090 1091

bd@gemserv.com

@gemservinfosec

IRELAND OFFICE

Fitzwilliam Hall Business Centre

Fitzwilliam Place, Dublin 2

Telephone: +353 (0) 1 669 4630

@gemservireland

Company Reg. No: 4419878

Gemserv

INVESTORS IN PEOPLE | Gold Until 2020

bsi. ISO/IEC 27001 Information Security Management

GlobalGROUP ISO 14001 UKAS MANAGEMENT SYSTEMS 0039

LLOYD'S REGISTER LRQA ISO 9001 UKAS MANAGEMENT SYSTEMS 001

CYBER ESSENTIALS PLUS