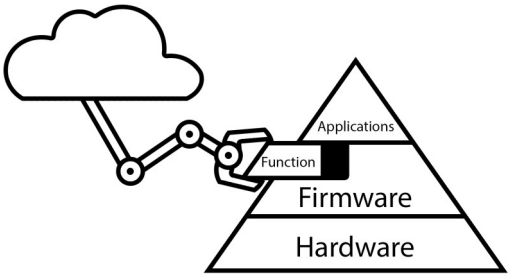
TMC's ADVISOR

Covering IT and Telecom from a Canadian Viewpoint — *February 2017 , Volume 1 Issue 2*

You Own It But It's Not Really Yours

By Peter Aggus



Traditionally when we bought a device, we owned it and we controlled it. Since software is leased rather than sold, that is no longer true. In fact, cases are increasing where manufacturers take control of devices that they have sold in order to change functionality. Your TV may lose some of the features it had when you bought it. In future, will your car refuse to allow you to travel where you want? Will your IT equipment refuse to process certain types of data? You are at risk from 'benevolent hacking' where firmware control supersedes your wishes. We look at risks and what you can do. Read More...

Inside

Willing Victims - By John Glover

Information Security is not JUST about the technology or the network or the Internet – It is more about the user sitting in the chair being a willing victim. As we have heard, "Why do robbers rob banks?" ANSWER - Because that is where the money is! Why do computer users become willing victims? ANSWER - Because we love convenience and are very complacent about personal responsibility when using computer and network capabilities safely. In other words, we do not practice SAFE HEX! Here are a few of our thoughts on the matter.

The Mobile Takeover - By Ellen Koskinen-Dodgson

The latest annual Cisco VNI Global Mobile Data Traffic Forecast is out and the results continue to surprise. They predict that by 2021, of the 7.6 billion people around the globe, more (on average) will use mobile phones (5.5 billion) than bank accounts (5.4 billion) or running water (5.3 billion). There are a number of drivers and they all contribute to our ever increasing demand for wireless communications and our decreasing attraction to landlines. Here are some cool stats and predictions.

Why Users Love and Hate the DMS - By Guy Robertson

Over the past 40 years, the Document Management System (DMS) has become increasingly important in many organizations. Properly designed, a DMS can store electronic images of documents and facilitate the efficient and secure indexing of vital documents that must be retained for any length of time. It also gives users opportunities for simple Google-style searches, such as "show me all documents that refer to blue Buicks". So why is it, when you mention DMS technology, you hear so many complaints and horror stories?

Radio Engineering Services

Are you looking to establish your radio network? Do you need help with the answers to:

- Is it better to use licenced or unlicensed frequencies?
- With unlicensed frequencies, will my installation fail when a new system is installed nearby?
- Is licenced 'too expensive'?
- Is my existing radio equipment reliable?
- How do I increase capacity on my current system?
- Are there health risks associated with installing a radio tower on our building?
- Can I rent space on someone else's tower?

Our survey reports are certified by one of our radio engineers, a P. Eng., licenced to make such statements.

E-mail: ellen@tmcconsulting.ca

or call: Ellen at 604-506-2905

 ISSN 2369-663X

You Own It But It's Not Really Yours *By Peter Aggus*

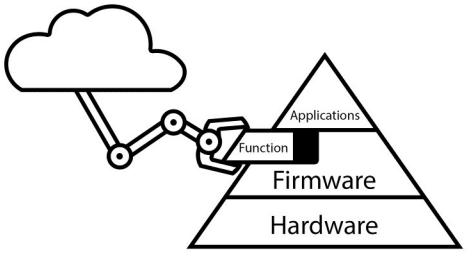
Traditionally when we bought a device, we owned it and we controlled it. Since software is leased rather than sold, that is no longer true. In fact, cases are increasing where manufacturers take control of devices that they have sold in order to change functionality. Your TV may lose some of the features it had when you bought it. In future, will your car refuse to allow you to travel where you want? Will your IT equipment refuse to process certain types of data? You are at risk from 'benevolent hacking' where firmware control supersedes your wishes. We look at risks and what you can do.

Computers

We were introduced to the concept of 'licensed' rather than 'owned' with computers. You may own the hardware but you only get the right to use the software. With that comes a requirement to keep the software updated. Sometimes these updates are simply to close security loopholes that have come to light or to correct bugs. However sometimes they are to deliberately alter the functionality. Updates used to be 'offered', meaning that installation was optional and done at a time convenient to the user. With ubiquitous network connectivity, such updates are increasingly non-optional and installed without user consent or knowledge.

Smart TVs

Last year, Microsoft lawyers pointed out to smart TV manufacturers that their OEM license for Skype applied to computer software not to TVs—hence smart TVs offering Skype as a feature were deemed illegal. A firmware 'upgrade' in the summer of 2016 removed Skype from the menu—even though it was printed on the TV box as a feature and, one might have thought, something that had been bought for use. None the less, the option was withdrawn.



Printers

You might have noticed that modern ink-jet printer cartridges contain a microchip. This permits the printer to read expiry dates and other data but it also allows the printers to reject third party cartridges, or ones that have been refilled.

Some 3rd party suppliers offer cloned chips designed to beat the barrier—so manufacturers have moved to non-reusable codes and pushed a firmware update to the printers to stop them using 3rd party cartridges. Lawyers are debating whether printer manufacturers can exclude 3rd party cartridges in this way.

Other Firmware Systems

There are many IT appliances that are controlled by firmware—and that firmware now often auto-updates on a periodic basis. There is no limit to the functionality changes that can be imposed by such updates and user expectations are never considered.

What You Need To Do

Read the 'small print' and see what is actually being imposed on you. Otherwise you may find that new behaviour of your devices is no longer what you expected when you bought them.

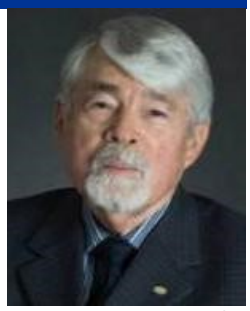
Also consider what information the firmware is allowed to disclose about the way you use the device—and this is not the normally excluded 'personal data'. Do your routers report traffic data, sites visited etc? Do your WiFi APs report lists of MAC addresses connecting to them? If you think this is far fetched, consider how advertisers finance so much of the 'free' connectivity these days.

One may also wonder about modern cars and what data they compile as part of their firmware upgrades...

This article is reproduced from the February 2017 edition of ***TMC's Advisor***

Peter, as an engineer & technology management consultant, has developed innovative & cost-effective solutions for clients in many industries.

Willing Victims *By John Glover*



Information Security is not JUST about the technology or the network or the Internet – It is more about the user sitting in the chair being a willing victim. As we have heard, "Why do robbers rob banks?" ANSWER - Because that is where the money is! Why do computer users become willing victims? ANSWER - Because we love convenience and are very complacent about personal responsibility when using computer and network capabilities safely. In other words, we do not practice SAFE HEX! Here are a few of our thoughts on the matter.

Where's the Risk?

With The Internet of Things (often referred to as The Internet of Everything) we are seeing a large increase in the target audience for hackers and other intruders. Now that we have the ability to access, via the Internet, domestic appliances and basic control apparatus (like door openers, baby monitors, remote web cam surveillance, heating, ventilation and air conditioning systems, building interior and exterior lighting, refrigerators, and yes, toasters, and the list goes on) we have an increased requirement for vigilance.

We need to install these devices with information security built in BEFORE deployment.

Isn't Safety Built-In?

No. Unfortunately, in the rush to market combined with the demand for reduced form factor (size) of most of these devices, information security does not often get into the design process before these devices are deployed.

There is a serious amount of engineering redesign required to make

many of these devices safe for prime time.

User Attitude

Couple this with an unreasonably trusting attitude on the part of many users. Users of technology are at risk from Internet tampering, or intrusion, or identity theft, and there is a very real likelihood that many will be compromised.

The cost for recovery is onerous and time consuming.

What to Do?

FIRST – Recognize that the use of the Internet comes with a responsibility to practice diligence and caution.

SECOND -- If the user is not aware of what is at risk, there is a need to invest some time and energy into learning the basics of privacy and personal protection.

THIRD – If it is worth avoiding the risk – get help.

Self Help

The web is full of great web sites that will gently lead even novice users down a safer path. Here are a few sites to get started practicing SAFE HEX!

1. The Privacy Professor: http://privacyprofessor.org/
2. https://www.canadapost.ca/cpo/mr/assets/pdf/aboutus/identitytheft_en.pdf
3. https://en.wikipedia.org/wiki/Data_breach

Finally -- LOOK BOTH WAYS WHEN CROSSING THE NET!

This article is reproduced from the February 2017 edition of ***TMC's Advisor***

John Glover assists national and international clients with governance, IT systems compliance auditing, IT risk assessment, information policy formulation and PCI data security.

The Mobile Takeover—*Projections 2021*

By Ellen Koskinen-Dodgson

The latest annual Cisco VNI Global Mobile Data Traffic Forecast is out and the results continue to surprise. They predict that by 2021, of the 7.6 billion people around the globe, more (on average) will use mobile phones (5.5 billion) than bank accounts (5.4 billion) or running water (5.3 billion). There are a number of drivers and they all contribute to our ever increasing demand for wireless communications and our decreasing attraction to landlines. Here are some cool stats and predictions.

Speed and Traffic

- Mobile connection speeds will grow to 20.4 Mbps
- 4G (4th generation) traffic will triple to 58% of connections and 79% of total traffic
- 5G is expected to roll out in 2020 and provide 1.5% of the total connections
- Mobile data will more than double to carry 20% of all IP traffic
- WiFi traffic will carry 49% of all IP traffic
- WiFi offload will reach 63% of total mobile data
- Global WiFi hotspots will grow to over 500 million—that should make WiFi network design even more complicated
- Machine-to-machine (M2M) will increase six-fold to 29% of total connections. This is the fastest growing connection type as IoT implementations grow.
- Total mobile traffic will increase seven-fold to 587 Exabytes (EB) annually. This is 122 times more than total traffic in 2011. (An Exabyte is billion GB)

Applications

- Video will grow almost nine-fold to 78% of all traffic
- Live video is just beginning to develop. It will grow 39-fold to 5% of all video
- Wearables will grow three-fold to 929 million devices with cellular connected devices growing six-fold to 69 million devices
- Virtual Reality headsets (VR immerses users in a simulated environment) will increase five-fold to nearly 100 million
- Augmented Reality (AR) is an overlay of technology on the real world, usually vision and hearing
- VR and AR are in the early stages of their development with eleven-fold and seven-fold increases in traffic respectively, with an aggregate total of 1900 Petabytes of annual traffic. A Petabyte is one million GB.

Prepare

Mobile and WiFi traffic will account for 79% of all IP traffic and this trend will continue. Perhaps it's time to look forward to a time where wired connections will be the exception, rather than the standard.

New applications will change our business processes, perhaps radically. Put on your futurist hat.

This article is reproduced from the February 2017 edition of ***TMC's Advisor***

Ellen Koskinen-Dodgson is President and Managing Partner of TMC IT and Telecom Consulting Inc. She is an IT and Telecommunications Management Consultant, electrical engineer, author, speaker, media resource and Expert Witness.

Why Users Love and Hate the DMS

By Guy Robertson

Over the past 40 years, the Document Management System (DMS) has become increasingly important in many organizations. Properly designed, a DMS can store electronic images of documents and facilitate the efficient and secure indexing of vital documents that must be retained for any length of time. It also gives users opportunities for simple Google-style searches, such as "show me all documents that refer to blue Buicks". So why is it, when you mention DMS technology, you hear so many

What Is It?

A document management system (DMS) is a computer system that stores electronic documents and images of paper documents for the purposes of space saving, fast retrieval, security and post-disaster recovery, and general convenience.

Why a DMS is Critical

Risk managers suggest that organizations implement a DMS to reduce legal and operational risks arising from lost documents. Some documents must be permanently and securely retained, and should be easily accessible.

Why It Is Loved?

A DMS can reduce staff workloads and improve an organization's efficiency and effectiveness. It can free up valuable space, and permit new office space designs. It can reduce legal and operational risks and lead to improved workplace safety and better morale.

The good points of a DMS are obvious to anyone who works in an office where the DMS works well. The ability to retrieve documents quickly gives users a powerful advantage.

Why It Is Hated?

Numerous complaints about DMS technology are linked to weaknesses in the metadata design. Metadata comprises a set of data that describes stored material. Think of metadata as a series of subject headings.

The most extreme example of a DMS failure is a manufacturer that wasn't interested in metadata. This meant that the system accepted new documents into storage but the documents could not be retrieved since the DMS included no search terms.

What to Do?

To make a DMS truly beneficial and to keep users happy, organizations should determine the purposes and structure of their DMS carefully.

They should select a trusted and reliable vendor An organization's records managers and IT staff should agree on the metadata that will guide users to specific files and documents. And everyone should agree on the contents of the DMS and its implementation schedule.

Many organizations do not contain sufficient specialized DMS expertise, so they seek consulting assistance to work with the client and the supplier and ensure that everyone's objectives are met. We have seen too many DMS implementation projects that fail, often at great expense to the client. Clients often blame the technology, but this is seldom the full truth.

The foundation of any DMS comprises its metadata , the integrity of its data, and its overall structure.

This article is reproduced from the February 2017 edition of ***TMC's Advisor***

Guy Robertson is a Senior Management Consultant at TMC who specializes in emergency planning and document management systems. A published author, he is an instructor at the Justice Institute of BC and at Langara College in Vancouver.