TMC's ADVISOR

Covering IT and Telecom from a Canadian Viewpoint — *February 2016 , Volume 3 Issue 2*

Looking Forward Issue

Microsoft's Hololens

Augmented and Virtual Reality

By Ellen Koskinen-Dodgson

It's time for CIO's to start thinking about augmented and virtual reality, enterprise edition.

The innovators - Ford, IKEA, and Marriott, to name a few - are already using one or the other and gaining benefits.

The vendors are on the verge of the big push to early adopters, too.

Read More

Inside

Death of Passwords

- By Peter Aggus

Password protection may be simple—but it's far from secure. Better technology has existed for years, but only recently are 'Token Authentication' and 'Biometrics' starting to become mainstream. Banks are embracing Chip & PIN technology ever more widely, computers incorporate Fingerprint Scanners, phones use Fingerprint and Retinal Scanners, and new passports include extensive biometric data for validation of identity. Here's a look at these new technology options and what we need to be aware of to make them work.

IoT Networks : Part 1 - HaLow

- By Bill Tracey

HaLow (pronounced halo) is the Wi-Fi Alliance's working name for the IEEE standard, 802.11ah. HaLow uses low power, can penetrate walls, and support thousands of devices per access point. What's not to love? Well, it connects these thousands of devices directly from your office to the Internet. Worried yet?

Hit by a Bus: What To Do When Key Employees Are Unavailable

- By Guy Robertson

Your IT manager is rear-ended – whiplash…pain…pain meds…he's not able to come to work. He's out for two weeks, and even when he returns, he'll probably not be 100%. What can you do when a key employee suddenly cannot come to work? Can another staff member fill in? Is

CIO for Hire

If you're smaller than $300 million in revenue, you likely don't have a CIO; you need one but you can't afford one.

CIO vs. IT Manager

- An IT Manager is an IT expert with a fair understanding of the business of their organization
- A CIO is a business executive with a fair understanding of using technology to drive business success
- An IT manager works with their IT team to plan and budget to accomplish user and IT goals
- A CIO works with the C-Suite—the COO, CEO, CFO, (etc.), to set priorities and budget

Clients can engage TMC to fill this requirement—a day or two per month can make a huge difference.

Contact Ellen for more information

ellen@tmcconsulting.ca or 604-506-2905.

 ISSN 2369-663X

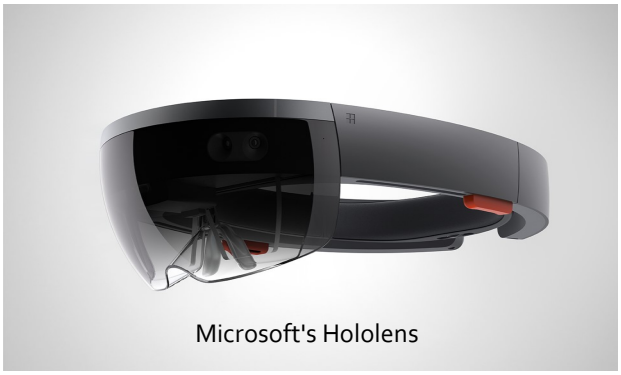
Augmented and Virtual Reality

By Ellen Koskinen-Dodgson

It's time for CIO's to start thinking about augmented and virtual reality, enterprise edition. The innovators - Ford, IKEA, and Marriott, to name a few - are already using one or the other and gaining benefits. The vendors are on the verge of the big push to early adopters, too.

What is It?

Virtual reality is generally considered to be an interactive 3D audio/visual environment through the use of helmets or goggles/headsets. Augmented reality allows you to see 'real' reality, augmented through the addition of information about your environment or objects within it.



Microsoft's Hololens

While AR/VR have been used in games for many years, it's at the early adopter stage in the business world. Microsoft's Hololens (see insert) is an example of current state-of-the-art technology.

Some Current Users

Ford uses an immersion lab for their design teams to mock up vehicle designs. IKEA uses an augmented reality app to allow customers to 'place' furniture into their home to see how it would look. Marriott Hotels has launched Vroom Service in a New York and a London hotel using Samsung headsets/headphones. This follows the earlier introduction of their 'Teleporter', a phone booth-like structure that allowed the addition of breeze, heat and mist to the audio/visual experience so you can 'feel' like you're at the beach in Hawaii.

Potential Uses

There are many potential business uses. The most likely 'killer app' for business will be built around collaboration. Rather than 2 dimensional videoconferencing, a user could 'be in the room', with the ability to look around at other attendees or down at their computer to look something up. Training will become another important use. Many specialty uses will develop as well, such as battlefield simulations, medical surgery simulations and product testing (a major step up from wind tunnel testing).

Issues

IT management need to think now about the implications:

Bandwidth: Most apps will be cloud based and will drive demand for bandwidth.

Content management and storage: You'd better have good control over your records management and document management as immersive, interactive AR/VR will require ever more effective data management. Think about the FOI implications.

Integration: AR/VR will need to inter-work with existing systems and databases. In order to support real-time experiences, data retrieval will need powerful processing as a 'laggy' experience will spoil the effect.

Cost

An interesting point is that the cost of AR/VR apps should spiral down as the competition for development will be fierce – similar to iPhone app development. Unfortunately, your need for bandwidth, storage, processing power and integration services will escalate.

This article is reproduced from the February 2016 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.

Death of Passwords

By Peter Aggus

Password protection may be simple—but it's far from secure. Better technology has existed for years, but only recently are 'Token Authentication' and 'Biometrics' starting to become mainstream. Banks are embracing Chip & PIN technology ever more widely, computers incorporate Fingerprint Scanners, phones use Fingerprint and Retinal Scanners, and new passports include extensive biometric data for

The Problem

Passwords are certainly a simple security measure but they are often easy to guess, when people choose something easy for them to remember—like their cat's name. The other big issue is that a password is easy for a 'hacker' to use. Its security hinges on 'knowledge' and, once the password is known to someone, they have open access to the protected systems.

Token Authentication

Security is improved by using physical 'tokens' where, like a key, 'possession' rather than 'knowledge' proves authorization. As long as the token is not easy to copy (like many house keys are) then Token Authentication is much more secure than a password.

Embedded chip technology has been around for years and is now used in car keys, bus passes and bank cards. A simple PIN is sometimes needed to unlock the card but the card itself is needed to complete the transaction. Knowing the PIN alone is of no use and the card or key is virtually impossible to replicate.

Chip & PIN technology is so much better than simple passwords that Barclays Bank in the UK decided to use it for login to online banking—replacing the old password system.

Barclays 'PINsentry' uses a regular chip-enabled card to generate a secure login code when the user's bank card is inserted. The user then types the code provided into the online banking login screen. This proves that they hold the card and know its PIN.

Biometrics

Retinal or fingerprint scanners used to be science fiction devices but are now in mainstream use for high security access. Unlike a password, you cannot 'forget' your fingerprint; and your fingerprint is unique.

However fingerprints alone are sometimes remarkably easy for 'forge' with some simple scanners being fooled by a photograph of a fingerprint taken from an object that the person has touched. Some simple iris scanners can likewise be fooled by a photograph of the person's eye.

Newer technology goes deeper than the skin and views a deep vein pattern using an infra-red laser.

Barclays Bank is now using this technique as a way of authenticating business transactions in preference to an old-fashioned signature. A small device next to the keyboard verifies the user's finger and adds a secure digital signature to the transaction.

Other biometric data, including voice, can also be used. Advanced facial recognition and skeletal analytics might have promise but even these advanced analysers can sometimes be fooled by a simple video replay. Perhaps 'Mission Impossible', when they used a photograph to defeat video surveillance, was not so far fetched.

The Future

Expect more biometrics—you can't forget them and they can be difficult to forge.

However the simpler systems may look good but the security provided is just an illusion if they are easy to fool.

The most secure systems at present use a combination of a physical token and biometric validation.

This article is reproduced from the February 2016 edition of ***TMC's Advisor***

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

IoT Networks : Part 1 - HaLow

By Bill Tracey

HaLow (pronounced halo) is the Wi-Fi Alliance's working name for the IEEE standard, 802.11ah. HaLow uses low power, can penetrate walls, and support thousands of devices per access point. What's not to love? Well, it connects these thousands of devices directly from your office to the Internet. Worried yet?

What Is It?

The new word of the day is HaLow (pronounced "halo"), the name given by the Wi-Fi Alliance to systems based on an extension of the IEEE standard 802.11ah.

How Does it Differ from other Wi-Fi?

Wi-Fi as most users know it operates in the 2.4 GHz (2,400 MHz) and 5 GHz bands. HaLow will operate mainly in the 900 MHz band, although it also can operate in the other two bands.

At 900 MHz radio signals will have extended range because they suffer less attenuation by walls, foliage, and similar obstacles. The lower data rate, extended range, and other features of HaLow contribute to lower power consumption and extended battery life.

What are the Intended Applications for HaLow?

HaLow is intended to support the Internet of Things (the IoT), which includes industrial and home automation, connected car, digital health care, and machine-to-machine (M2M) markets like Smart Metering and traffic signal controls. It aims at providing connectivity to thousands of devices under an access point, within a radius of about a kilometre. Range and other requirements, including extended battery life, can be improved by the use of Relay Access Points – but that's a topic for another article.

There will be many unintended consequences.

HaLow will allow devices to connect with Wi-Fi's ecosystem of more than 6.8 billion installed devices. Like all Wi-Fi devices, Wi-Fi HaLow devices will support IP-based connectivity to natively connect to the cloud, which will become increasingly important in reaching the full potential of the IoT. Dense device deployments will also benefit from Wi-Fi HaLow's ability to connect thousands of devices to a single access point. In short, it's important to recognize that Wi-Fi HaLow connects devices directly to the Internet, not just to another device.

Note that HaLow is intended for relatively low data rates – about 100 kbit/s. It will not normally support high-data-rate (e.g., cell phone) applications.

HaLow will be competitive with Bluetooth where extended range is desired. It will also compete with ZigBee (IEEE 802.15.4) and similar protocols used in industrial automation.

Availability

The Wi-Fi Alliance isn't planning on rolling out HaLow certifications until 2018.

By that time the terminal market will be heavily invested in Bluetooth and ZigBee (IEEE 802.15.4) technology, along with other similar protocols used in industrial automation.

In the next article, we will look at a comparison between the technologies to see if there is a core infrastructure that might be future-proof and capable of supporting all the technology players.

As always, it's important to know what's just around the corner – as the Scout Motto goes: 'Be Prepared'.

This article is reproduced from the February 2016 edition of ***TMC's Advisor***

Bill Tracey is a radio systems Design Engineer and consultant with over 25 years of experience with all types of radio systems. He is a trusted advisor to post-secondary, municipal, emergency services clients.

Hit by a Bus: What To Do When Key Employees Are Unavailable

By Guy Robertson

Your IT manager is rear-ended – whiplash…pain…pain meds…he's not able to come to work. He's out for two weeks, and even when he returns, he'll probably not be 100%. What can you do when a key employee suddenly cannot come to work? Can another staff member fill in? Is his job well documented so a contractor can parachute in? No? What can you do to protect yourself?

Background

Every day, in organizations of every type, people fail to show up for work. Sometimes it's a car accident, sometimes a family emergency. Sometimes they quit without notice or can't get to work because of a snow storm. No matter the cause, the problem is the same and the question remains – what are we going to do?

Succession Plan

A succession plan is not just for replacing retiring employees. The more critical use of succession planning is to cover unexpected replacements for key employees.

Your succession plan should provide practical answers to questions including:

- What do we need to know to continue our operations?
- Which employees know it now?
- What will happen if these employees are not available, temporarily or permanently?

Even with the most comprehensive systems documentation, you're vulnerable if key operations personnel are unavailable. Inevitably, there are gaps in documentation, and necessary procedures and specifications might exist only in the brain of the person that didn't show up to work today.

Knowledge Map

An effective succession plan will include a 'knowledge map' that indicates where knowledge about systems and operations is available. The foundation of a knowledge map can involve tasks such as:

- Keeping IT documentation as up-to-date as possible: some network drawings and applications lists are so old that they are dangerous. Verifying documentation accuracy is part of a succession plan.
- Keeping IT staffers up-to-date with your technology and processes: ongoing training and cross-training is essential. No employee becomes a 'black hole' into which information could disappear forever. Information transfer can also be a team-building and morale-building tool that makes your IT staffers feel closer to core operations.
- Developing effective ways of transferring information to an entire IT department, so that everyone knows who will do what if a key employee doesn't show up for work.

Testing

To verify your plan, you need to test it, just like with your disaster plan. Rather than telling people that they have to wait until someone is back from vacation, implement your succession plan to find out how well it works.

This article is reproduced from the February 2016 edition of ***TMC's Advisor***

Guy Robertson is a Senior Management Consultant at TMC who specializes in emergency management and disaster planning. He has written extensively on emergency planning and IT security—hundreds of articles as well as a book with worldwide sales.