KEYNOTE ADDRESS FOR THE 50th IEEE International Carnahan Conference on Security Technology, Orlando, 25 October 2016

Security Technology: 50 years on

Gordon L. Thomas, Chairman of the ICCST Executive Committee.

The aim of security technology is to address a specified or often unspecified threat; to provide identification; or to assist in crime investigation. As much as the technology has evolved over the period since we began, so has the nature of the threat. Back in 1967, the threat was mainly criminal attack against property and the person, isolated cases of terrorist attack and the ever present possibility of escape from custody.

The threat has drastically changed since. Frequently backed by the Islamist groups, Al Qaeda and so called ISIS (Islamic State in Iraq and Syria) terrorists are now active, worldwide. **They and their associated groups and individuals have perpetrated many hideous attacks, usually by engaging suicide bombers and frequently causing death and horrific injury to the innocent.** I won't say much more about the threat because that is not what this paper is about.

Security technology has ridden on the crest of the wave of developments elsewhere in science and technology. Lasers predated our first conference as does the transistor. I'll give you some of the key developments – you know about them anyway! In **1969**, the ARPAnet which led to the Internet, the WWW; and the CCD; in **1972,** the first CT scanner; in **1973**, the cell phone, MRI scanning; in **1978**, RSA public key encryption, GPS; in **1984**, DNA decoding; in **1991**, the digital camera; in **1994,** the web browser; in **1997**, the plasma display TV screen; in **2001**, the iPod; in **2003**, IEEE 802.11g Wi-Fi Standard; in **2005**, Google maps; in **2007**, the Apple iPhone.

Between 1966 and 1969, I did my PhD at London University - **see, I'm older than I look!** - I worked on one of few mainframe systems in London – an IBM 7090. This was a second generation, transistorised version of the IBM 709 series of vacuum tube computers. Used a 36-bit word length, with an address-space of a mere 32k words. It operated with a basic memory cycle of 2.2 μs or at less than 500 kHz. We here would all regard that as so slow as to be almost stationary! The computer which landed **Apollo 11 on the Moon, by the way, had 2k of RAM and 16 k of ROM.**

Typical machine clock rates now are upwards of 600MHz – a thousand times faster than that IBM machine I worked with - and memories of hundreds of GB are common – a million times more than 7090! And for example, the **Core Intel i5 processor runs at 3GHz and it's not the fastest.** It has, of course, been necessary to develop a battalion of computer and IT security techniques, not only to protect the individual user from computer fraud and identity theft, but also to secure data. **About half of the papers presented at the Carnahan conference in the past 7- 10 years have been in the subject of IT security.** They have ranged from advanced encryption techniques, including those for protection of voice over internet, to methods of detecting malware and preventing Trojan horse attacks.

Quantum cryptography, uses the uncertainty principle for the generation of cryptographic keys and their transmission. **If an attacker tries to steal the key, for example, by interception, the act of taking the key, damages it so that it cannot be used by the attacker.** It will eventually replace classical cryptography, at least in a range of extremely sensitive and important applications. It is not just theoretical concept. The Swiss company Id Quantique have developed a quantum computer, which uses a photon stream as the key and in 2007 they used it to transmit votes securely in the Geneva Canton elections.

An Australian group – **this September** - created a light trap by shining infrared lasers into ultra-cold atomic vapour. Apparently, the atoms absorbed some trapped light, but a substantial proportion of the **photons were frozen inside the atomic cloud**. The researchers likened the team's experiment at ANU to a scene from **Star Wars: The Force Awakens when the character Kylo Ren used the Force to stop a laser blast mid-air!** This ability could be crucial in optical computer development. So quantum computing is here to stay.

Cloud computing is a further recent development. It has four essential characteristics: elasticity and the ability to scale up and down; self-service provisioning and automatic de-provisioning; application programming interfaces (APIs); billing and metering of service usage in a pay-as-you-go model. **This flexibility is what is attracting individuals and businesses to move to the cloud. Already Amazon and Google are major users, as well as providers.**

Threats which apply to 'ground based' computing also apply in the cloud. Data leakage, insecure applications interfaces and malicious insiders may also be threats. **The main dangers in shared areas are where malicious users have access to the same part of a virtual machine as the genuine user.** Such users can impair other virtual machines and the genuine user's data. The key appears to be in **careful user authentication** and using this to provide security in moving from one virtual machine to another.

Nowadays, the mobile phone is a hugely complex piece of technology, with an amazing range of abilities. **IT didn't exist in the 60s.** It is in effect a highly sophisticated computer. The most useful are expensive so it is a target for thieves and data hackers, apart from being a potential trigger device for a bomb.

The **IoT, the Internet of Things,** is spreading as a reality. Computer-controlled devices in automobiles such as brakes, engine, locks, hood and truck releases, horn, heat, and dashboard have been shown to be vulnerable to attackers who have access to the onboard network. So are home based systems like air conditioning systems, domestic lighting, CCTV systems. The **Internet of Things Security Foundation was established in September 2015 to keep a watch on these issues.**

Biometrics is evolving in many areas. In the 19th century, fingerprint identification became an established tool in the fight against crime. There are two main applications for fingerprints: those found at scenes of crime, which are **used to identify the perpetrators**; and fingerprint records are use to **prove identity of individuals**, more often **not** in the context of crime, for example in access control. In the seventies, our team at the UK Home Office **studied their surface properties, electrical properties and topology.** We introduced several new techniques for fingerprint detection and these are still used worldwide.

Right up to the mid-seventies all the fingerprint comparison work was carried out manually by fingerprint experts. Papers presented at Carnahan in the **70s and 80s** showed how advanced comparison algorithms, based on the minutiae of individual fingerprints and implemented on fast computers**, some using array processors,** could produce, in a matter of seconds, a short list of potential matching fingerprints, leaving the fingerprint officer simply to check this list manually against the record prints. This was truly a revolution in security technology and crime detection. The first such system used operationally in the world was at Scotland Yard and was reported at this conference in 1977.

Biometrics has advanced on many other fronts. In the early years of the conference we saw the acceptance **in Wiesbaden of voice print acoustics** in criminal investigation, all work conducted on a PDP11 computer. **A paper reported last year in Taipei showed how to 'de-identify' the gender of a person from his or her speech.** The main purpose is to protect the identity of the speaker for privacy purposes.

Since our early days we've see personal identification through **iris scanning, first reported at our conference,** through **facial recognition** to **palm geometry** and even identification by **ear profiles, veins in the hand** and **human gait**! A number of these techniques are now part of our every day life; in, for example, access control, smart cards and some passport applications. **My computer allows me to log in with my fingerprint! Just as well they are not worn away just yet!** Again, powerful computers have been behind this.

An area in biometrics which has seen exciting advances in recent times is **facial recognition** which is not easy. It may be for a human being but not for a machine. In any scenario, the background can change, as can the lighting, and the perspective. **The face can change,** that is, the facial expression as well as its characteristics such as hair distribution, make-up, glasses etc. and its orientation Since a face can appear at any position in a picture the first step is to find it. This in itself is not a trivial problem.

Facial recognition is a topic which has benefitted, not only from the increased power of modern computers but also from clever algorithmic techniques. E.g. discrete wavelet transforms which have the advantage over the Fourier transform of preserving spatial as well as frequency information. **Neural networks and Support Vector Machines** have come into their own. In a paper in our 2009 conference, the authors reported an incredible obtained accuracy of 100% in detecting a subject in a video sequence. They used **wavelets** to parameterise the faces and **Support Vector Machines** to classify them.

Not only do we have reasonably reliable facial recognition but we are now moving into the arena of being able to automatically classify facial expressions. The pioneering work in this field was conducted in 1978 by **the psychologists, Paul Ekman and Wallace Friesen**.

Human **signatures are the oldest biometric** going back thousands of years. Automatic signature verification, is a widely discussed subject at Carnahan, again because of its importance in personal identification. One of the later topics has been the **development of synthetic signature**

databases. These are now widely used for algorithm development and overcome legal issues associated with real signatures. You can even have ‘forged’ synthetic signatures. **An interesting concept in itself!**

Physical security is vital to the protection of key national infrastructure. Physical security protects not only from the **bad guys getting in**, that is the terrorists or other criminals, but also from the **bad guys getting out,** eg from prisons. Over the past 50 years we have seen the most basic trip alarms develop into incredibly **sensitive perimeter detectors which use image analysis and zone analysis**. Once again, digital computer technology has been the platform on which these systems have been based. Infra-red, microwave, leaky feeder, vibration sensor, capacitative loop and various other sensors have been developed to be at the front end of these systems. And now, we are seeing wireless systems, powered by solar cells, which can transmit alarm data via the Internet! **Keith Harman is speaking next and he will elaborate**, better than me, I’m sure.

In order to obtain the best value system for an application, the Centre for Applied Science and Technology (CAST) in the UK Home Office conduct comparative testing of PIDS. **At our 2012 conference a paper by scientists at CAST reported recent work they had conducted on designing a standard against which wide area detection systems (WADS) can be evaluated.** My view is that this work represents a major step forward in evaluation and development.

Barriers are often regarded as the Cinderella of security technology, but they can be vitally important. **New types of bollard and automatically raised barriers** give protection against bomb carrying lorries, or trucks. More sophisticated walls and barbed wires deter prisoners from escape. Back in the mid-80s much work was reported here on **active barriers** which released **smoke clouds or CS gas** if compromised. That appears to have virtually dried up. Maybe someone should look again at that topic.

In its early conception, **close circuit television** as a security application, consisted of a single camera, usually trained on a door or some other access point and a guard looking at the screen. Because the vidicon cameras and the monitors, which 40 years ago were based on cathode ray tubes, were so expensive, the applications were few, mainly at embassies, high security prisons and for protecting very high value assets.

Since the mid-seventies and beyond, Carnahan has witnessed many developments in CCTV. Camera systems now rely on charge coupled devices which are produced by the thousand and are really cheap. **I saw one on eBay for $19, with full WiFi and night vision capability. I didn't buy it, by the way! I'm waiting for it to be cheaper!** Video tape recording has largely being replaced by digital recording, again because of the massive developments in computer memory technology: we now talk in **Terabytes**. And, of course those bulky monitors have been replaced by flat screens. All these advances mean that CCTV has become omnipresent, certainly in the UK.

In recent times, **terrorists have imposed a huge security burden on airlines and airport authorities.** Starting from the early x-ray scanners, which were cumbersome, slow and insensitive, we have seen the introduction of a range of sophisticated devices. The latest baggage x-ray scanners produce high resolution, 3D pictures which enable the identification of firearms and other weapons as well as concealed explosives. Some of the most advanced use CT techniques, first used as diagnostic tools in hospitals. Hand held and archway devices have also improved, mainly in reliability and sensitivity of detection and speed of throughput. Now the merest trace of an explosive can be quite easily detected. **Millimetre wave technology and quadrupole resonance techniques** are now also being brought into this arena.

In recent years, Carnahan has witnessed great advances in the **training for x-ray scanning operators** at airports. For example, in a 2008 paper, the authors point out that, in order to guarantee a reliable and effective recognition of threat objects, operator training is the key. They show that by far the most effective way of delivering such training is to make it individually tailored or adapted to the operator.

We have already covered a number of **applications of security technology**. But there are many others such as in e-banking, the protection of communications and indeed of individuals using social networks such as **Facebook** and **Twitter** as well as commercial and privately run websites. These needs simply did not exist in the early days of the Conference. But I also have in mind the widespread use of integrated systems of alarms and communications. The scale of such systems is increasing in size. We saw recently such a system being used to protect the Vatican State and we have seen others, for example, for the protection of police communication and data systems in Taiwan and Japan. **The authors of a paper we saw in 2013 described an integrated system they had developed for predicting terrorist attacks in urban environments.** It uses a real time reasoning layer which processes different information sources, e.g. from the police on the ground, sensor information such as CCTV cameras to predict a threat event. Very interesting!

So this concludes this brief traverse into areas of security technology that we have seen presented at the Carnahan Conference since its inception. What we see is what we might call **‘an advancing tide’** of developments across the whole area of this technology. I can see no topic which can be said to be stagnant, except active barriers.

So, where do we go from here? Some things are clear. There will be a continuing need to respond to the threat, even as that changes. There will be a continuing need to ‘stay ahead of the game’, that is there is a need to continue to outwit the intruder and to confound the terrorist, and to be at least one step ahead of them. There is a need for greater sensitivity and greater automation and greater integration in the use of systems. This being said, there will always be the need for human intervention when a decision has to be made on whether to respond to an alarm or to search someone at an airport. There are sure to be new internet applications and spectacular advances in IT. I can imagine that parallel processing - **and dare I say quantum computing -** will in the future come much more into their own. All this means that there will continue to be developments in the technology for many years, if not indefinitely. **I won’t attempt to look into the cloudy crystal ball of future technology. But I look forward to our panel discussion tomorrow!**

What I am saying is that there will continue to be a need for the Carnahan Conference. There may even be a greater future need for it than there is today.

Thank you.

Gordon Thomas
www.gordonlthomas.com