Hacking

By Kevin Curran

According to the National Crime Agency (NCA) Cyber Crime Assessment 2016 report cybercrime accounted for 53 per cent of all crimes in 2015. This percentage is rising steadily each year. We can expect to see cybercrime continue to develop into a highly lucrative and well organised enterprise. Cyber criminals whether state sponsored or not are even beginning to devote funds to research and development! It has become an industry. We all remember the bank robber from 100 years ago who replied when asked why he robbed banks with the response "because that is where the money is...". Well, criminals are increasingly moving online because that is where the money is. We are also seeing terrorist groups beginning to exploit cybercrime to fund their evil aims.

The latest demon online is ransomware. This is showing worrying trends. The Security vendor Malwarebytes used a 'honeypot' to attract attackers and they discovered an increase from 17% in 2015 to 259% in 2016. Ransomware of course is the nasty malware that holds peoples data files hostage until a payment is made in bitcoins. Imagine the future however when our smart home devices are held hostage and owners have to pay a fee to have access to their lights and Internet of Things (IoT) appliances. We will also see ransomware appearing on our smart cars, trucks, trains and planes. It is only a matter of time before we see people left helpless, on the side of the road unable to drive their vehicles until they pay a ransom. Cryptocurrencies like Bitcoin of course have enabled the rise of ransomware. In fact, experts predicts that by 2040 more crime will be committed by machines than by humans. This will arise as the human workforce moves towards more automation. What happens too when robots are hacked and change into suicide-bombing robots. The same applies to hijacking drones and perhaps using multitudes like flying bot armies to attack. We have already seen proof of concept WiFi hacking drones which can land on a roof and sit there intercepting WiFi, wireless keyboards and other data being passed over a network. It all comes down to practicing safe computing. It must always be remember that no one involved in the early Internet design ever foreseen the pervasiveness of its involvement in everyday life. That is why we have so many security & privacy issues today (Comer et al., 2012). This chapter highlights hacking, the tools, its widespread uptake and the implications for society.

Phising attacks

Phishing attacks aim to acquire sensitive information such as usernames, passwords, and banking details by simply masquerading as a trustworthy entity in a message. The word itself comes from fishing due to the similarity of using a bait in an attempt to catch a victim. It is an ideal attack vector especially when done properly. By properly, I mean with relevant supporting information which tricks the victim. Unsupported phishing attacks are generic so they often claim to come from bank x or y, company x, IT department Z etc but can be easily ignored except for the many newcomers to the web where there is no substitute for experience and they only get that through time and learn to identify what are phishing attacks. If most people are honest, they will admit to have clicked on at least one link in a phishing attack email. That may have led to nothing as they may have pulled out later in the process before inputting their credit card or personal details but none the less, if a correctly formatted email claiming to come from Paypal arrives in your inbox on Monday morning as you rush to get the kids out the door to school and you are aware of needing to pay for an item later that day with Paypal, then it is very easy to click on it 'to solve your problem'. Especially then the email starts with "Dear Kevin" or your proper name and has some other identifying information elsewhere.

That is why every time there is a large database hack online which leaks personal identifying information (even without credit card/banking details) all those people exposed in that data leak have now had crucial identifying personal information leaked which can be later used by scammers in phishing attacks. This does happen. There are millions of hacked leak database details for sale right now on the dark web scam markets. Phishing attacks are a real problem. One could say that the most deadly problem in most corporations right now are links in emails. There is no easy solution. Emails increase year on year and there are millions of potential people who can email you and millions of potential online site links so spam mechanisms (which are quite good) are struggling to block many phishing attacks. These phishing emails are able to generate random characters and modify their format so as to evade spam filters.

Employee behaviour is of course the root of successful phishing scams. If no one responds to a phishing email or opens an attachment then there would be no problem. The problem of course is that there is a small percentage who do. Experienced computer users tend to forget

that there are still many new users each day experiencing email for the first time and do not have the experience of determining a genuine email versus a scam. Some people are very honest and do not expect to encounter dishonest clever scams via email. They perhaps have lived a particular way of life encountering like-minded honest people and then they go online and one day receive an email which is either promising riches or claiming hardship so they respond. We have all read countless stories of especially older people being scammed for large amounts of money. We perhaps should therefore not be that surprised that phishing scams do work if you contact enough people.

Other measures against phishing include authenticating in-bound emails. This helps as many phishing attacks also contain malware attachments. Implementing a Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM) and Domain Message Authentication Reporting and Conformance (DMARC) can help guard against spear phishing and other attacks coming through spoofed email. These work together to validate the IP address and domain of the originating email server but sadly, not enough organisations adopt these standards. It also helps to have active scanning of all email in order to detect potential threats. Having ad-blocking enabled can also help as ransomware is distributed through malicious advertisements served up to users when they visit sites (Curran et al., 2015). Some organisations have implemented separate networks for employees surfing the web. Machine learning can also be used in scenarios such as email content detection and network profiling techniques. Misuse detection methods match test data with profiled anomalous patterns. Anomalous detection systems profile normal patterns to search for outliers and hybrid detection systems combine misuse and anomalous detection techniques to improve the detection rate and reduce the false-alarm rate. These are common approaches to apply machine learning in cybersecurity. Scan detection is used to detect the precursor of attacks so that it can lead to the earlier deterrence of attacks and profiling networks assists in active protection of systems through extraction, aggregation, and visualization tools.

How Distributed Denial of Service (DDoS) attacks work

DDOS attacks are hard to stop as free simple to use tools such as Low Orbit Ion Cannon (LOIC) and High Orbit Ion Cannon (HOIC) make it easy to flood sites with overwhelming amounts of dummy traffic created by custom scripts. You simply enter the URL of a website, and watch these free programs generate fake packets so as to overload a site's servers. You can watch the average site being brought to its knees in minutes. Of course a tool like these run from 1 or 1 PCs would not be enough to bring down an Internet giant however other distributed DDoS tools which are built on collections of compromised machines (DDOS botnets) can perform much larger synchronised DDOS flood attacks. Many networks are now built on the Internet Protocol Security (IPSec) which secures traffic within the network end to end. It provides services similar to HTTPS/TLS which does add an extra layer of security to their network infrastructure but it is not fool proof. It seems here for instance that it was bypassed as they may have exploited some known flaws in the Domain Name System (DNS) servers to expose the network to flooding. This is not as difficult as it sounds as there are tools online which help you identify known vulnerable DNS servers on the internet so that you can get maliciously route a stream of traffic from these DNS servers to on a company's network. It is another way to generate a flood of traffic without needing a botnet of zombie computers to do your flooding work. Remember, we are dealing with millions of requests per minute here. Very few websites can cope with such dedicated fraud requests. The problem of course is that it is very difficult in real-time to isolate real requests from genuine customers from the malicious DDOS flood requests. DDOS attacks will continue for the foreseeable future as long as unpatched systems remain online and easy to deploy DDOS tools exist. Unfortunately, a DDOS attack is the simplest of all hacking exploits to do (Prince, 2016). People also forget that it is relatively only recently that much network code was patched to stop DDOS syn attacks which flooded memory.

If you want to understand what really happens in a DDOS attack, then you just need to look into SYN flood attacks. A SYN flood is a denial-of-service attack in which an attacker sends a succession of SYN requests to a target's system in an attempt to consume enough server

resources to make the system unresponsive to legitimate traffic. Basically, normally when a client attempts to start a TCP connection to a server, the client and server exchanges a set of messages which normally take the following stages (1) The client requests a connection by sending a SYN (synchronize) message to the server. (2) The server acknowledges this request by sending SYN-ACK back to the client and (3) The client responds with an ACK, and the connection is established. This is called the famous TCP three-way handshake, and is the foundation for every connection established using the TCP protocol. A SYN flood attack works by not responding to the server with the expected ACK code. The malicious client can either simply not send the expected ACK, or by spoofing the source IP address in the SYN, causing the server to send the SYN-ACK to a false IP address - which will not send an ACK because it "knows" that it never sent a SYN. The server will wait for the acknowledgement for some time, as simple network congestion could also be the cause of the missing ACK, but in an attack increasingly large numbers of half-open connections will bind resources on the server until no new connections can be made, resulting in a denial of service to legitimate traffic. Some systems may also malfunction badly or even crash if other operating system functions are starved of resources in this way. A permanent denial-of-service (PDoS), also known loosely as phlashing, is an attack that damages a system so badly that it requires replacement or reinstallation of hardware. Unlike the distributed denial-of-service attack, a PDoS attack exploits security flaws which allow remote administration on the management interfaces of the victim's hardware, such as routers, printers, or other networking hardware. A distributed denial of service attack (DDoS) occurs when multiple systems flood the bandwidth or resources of a targeted system, usually one or more web servers. These systems are compromised by attackers using a variety of methods (IETF, 2016).

Malware can carry DDoS attack mechanisms; one of the better-known examples of this was MyDoom. A system may also be compromised with a trojan, allowing the attacker to download a zombie agent. Attackers can also break into systems using automated tools that exploit flaws in programs that listen for connections from remote hosts. This scenario primarily concerns systems acting as servers on the web. Stacheldraht is an example of a DDoS tool which uses a layered structure where the attacker uses a client program to connect to handlers, which are compromised systems that issue commands to the zombie agents, which in turn facilitate the DDoS attack. Agents are compromised via the handlers by the attacker, using automated routines to exploit vulnerabilities in programs that accept remote connections running on the

targeted remote hosts. Each handler can control up to a thousand agents. These collections of systems compromisers are known as botnets. DDoS tools like stacheldraht still use classic DoS attack methods centered on IP spoofing and amplification like smurf attacks and fraggle attacks (these are also known as bandwidth consumption attacks). SYN floods (also known as resource starvation attacks) may also be used. Newer tools can use DNS servers for DoS purposes. The major advantages to an attacker of using a distributed denial-of-service attack are that multiple machines can generate more attack traffic than one machine, multiple attack machines are harder to turn off than one attack machine, and that the behaviour of each attack machine can be stealthier, making it harder to track down and shut down. These attacker advantages cause challenges for defense mechanisms. For example, merely purchasing more incoming bandwidth than the current volume of the attack might not help, because the attacker might be able to simply add more attack machines.

While the filtering method discussed in this document does absolutely nothing to protect against flooding attacks which originate from valid prefixes (IP addresses), it will prohibit an attacker within the originating network from launching an attack of this nature using forged source addresses that do not conform to ingress filtering rules. All providers of Internet connectivity are urged to implement filtering described in this document to prohibit attackers from using forged source addresses which do not reside within a range of legitimately advertised prefixes. In other words, if an ISP is aggregating routing announcements for multiple downstream networks, strict traffic filtering should be used to prohibit traffic which claims to have originated from outside of these aggregated announcements. An additional benefit of implementing this type of filtering is that it enables the originator to be easily traced to its true source, since the attacker would have to use a valid, and legitimately reachable, source address (Lusson et al., 2012).

How can attacks like DDOS be prevented in the future?

Large companies need to constantly upgrade their DDOS flood defences. Some approaches that worked just a few years ago are now basically useless. For instance, in recent years, a common way to defend against these attacks was to try in real-time to identify spikes in traffic and then use a technique called 'blackholing'. This was in conjunction with a sites internet provider so that the incoming fake traffic is rerouted to the 'blackhole' however newer DDOS attacks change their profile much quicker so it becomes more and more difficult to simply identify which packet requests are nefarious. Companies should try to deal with DDOS traffic on the edge of their network immediately. They should be able to utilise a cloud solution so in the event of these large-scale flooding attacks, they have enough bandwidth to absorb them. You see bandwidth allows space to breath, cope and react (O'Flaherty & Curran, 2013).

A good place to start is to deploy DDOS prevention systems such as Google Project Shield[1] or services like Cloudflare provide. Google shield for instance is a suite of tools for activists and non-profits, including tools for evading web censorship and oppressive regimes. The biggest focus has been on DDoS attacks, a kind of brute-force action that can easily take down a small site without leaving any clues as to the culprits. DDoS has been a persistent problem for small-scale activists on the web, but Google's Project Shield offers free DDoS mitigation services to sites serving "media, elections, and human rights related content. The tool is built on Google's PageSpeed service, a frontend tool that offers developers faster loading times. Sites hosted by Project Shield would sit behind PageSpeed's infrastructure, allowing Google to pool resources if any one site fell victim to an attack. Unless an attack were strong enough to bring down all the PageSpeed sites, it wouldn't be able to bring down any of them. It's a similar model to existing DDoS services like Cloudflare, although the more recently launched PageSpeed service is working from a smaller base of sites. A smurf attack is one particular variant of a flooding DDoS attack which relies on misconfigured network devices to allow packets to be sent to all computer hosts on a particular network via the broadcast address of the network, rather than a specific machine. The network then serves as a smurf amplifier. In such an attack, the perpetrators will send large numbers of IP packets with the source address faked to appear

[1] http://www.google.com/ideas/projects/project-shield/

to be the address of the victim. To combat denial-of-service attacks on the Internet, services like the Smurf Amplifier Registry have given network service providers the ability to identify misconfigured networks and to take appropriate action such as filtering. Also some ISPs offer what is called a "wide channel" which provides again a sort of buffer or safety margin for customers to outstay a DDOS. However, a wide channel and filtering services are only effective if the filtration rules are kept up to date to fight the latest DDoS techniques. DDoS attacks used to be a modern day form of resistance. It is akin to the traditional 'Street Protests' except they are now "Internet Protests". Now however hackers are making money using Bitcoin to demand ransoms. We only hear about a fraction of the ransoms being paid out.

The most worrying trend in DDOS attacks has been the utilisation of IoT devices such as webcams which were compromised to create the largest known denial of service attack to date in 2016 against a site owned by Brian Krebs, the well-known security researcher (Deak et al, 2015). That site was brought to its knees and the Internet service provider had to 'cut him loose' to protect their other clients. You see the Internet was unfortunately not built from the ground up with security in mind so aspects of the infrastructure such as DNS's insecurities are a weakness.

Hacking the Internet of Things

There is an argument for people to keep things dumb when it comes to the Internet of Things. A basic rule of thumb in security is that the more devices you have exposed to the internet, then the more exposure you have to being hacked. It really means that you are more likely to have neglected devices which are not updated and hence more vulnerable. It is crucial that IT departments monitor their networks 24-7, looking for potential intrusions and unusual activity on the network but in reality how many do this and take appropriate actions. The sheer scale of deployment of these limited-function embedded devices in households and public areas can lead to unique attacks. There is also the worry of the domino effect where if one device becomes 'owned' - it can easily spread to the remainder of the cluster. The privacy issues arise due to the data collection mechanisms which may lead to user profiling and identification of individuals in unforeseen use case scenarios (McBrearty et al., 2017). The utmost care needs

to be taken when deploying IoT devices with regards their lifecycle, data collection mechanisms and overall security protocols.

We have now seen a major issue with IoT devices due to their implementation of default passwords which are known to hackers in addition to many of these devices have pre-installed unchangeable passwords which is utterly careless on behalf of the manufacturers. Only a few IoT manufacturers are considering the correct forms of cryptographic algorithms and modes needed in particular for IoT devices. The utmost care needs to be taken when deploying Internet Connected home appliances as these Internet Connected devices such as robots are simply not running very good security software on them especially as many of these connected devices have a limited memory size, limited battery life along with restricted processors. Traditional 'heavy' cryptography is difficult to deploy on a typical sensor hence the deployment of many insecure remote connected devices (Ksiazak et al., 2015). On devices like these, every pound matters with regards price margin and the more powerful the sensors & "processer" that are inside the device – the more expensive they cost therefore security is always a luxury for many home appliance manufacturers so the consumer loses out in the end. I mean "what are the odds" is what most people think when it comes to their being a victim of Internet fraud or intrusion in this particular case. There is evidence to date that many consumer IoT devices have neglected the end-to-end security aspect. We know that a core reason for this is that many of the embedded devices do not simply have enough computing power to implement all the relevant security layers and functionality necessary. There is then the actual heterogeneity of devices and the lack of industry or defacto standards for connecting these devices to the Internet.

Hacking Robots

One area we will see more robots tasked with in the future is security. In fact, already security intrusion detection robots have been developed by many companies including iRobot and robotext. These for the most part consist of smaller mobile robots with cameras and movement detection which move around a building looking for intrusion. The company which has gathered most headlines is this space has been Knightscope who are based in California. Their 'Dalek like' K5 robot is designed to detect anomalous behaviour, such as someone walking through a building at night, and report back to a remote security centre. The K5 uses four high definition cameras, sensors, a license-plate recognition camera, four microphones, a weather sensor for measuring barometric pressure, carbon dioxide levels, temperature, navigation equipment, and electric motors — all packed into its dome-shaped body with a big rechargeable battery and a computer. The K5 use Wi-Fi to communicate with other K5's and with people who can remotely monitor its cameras, microphones, and other sources of data. This is just one example of a modern robot with its various sensors and cameras. There is therefore always the risk of such robots being hacked therefore additional measures need to be taken such as implementing extra security authentication - perhaps facial recognition of the owner when opening panels. Costs can be higher than traditional systems and many solutions also have monthly fees. There is a real risk of privacy invasion - especially in the case of a robot which has complete freedom to roam inside the house, so we have to ensure that the surveillance footage is securely stored. The main issue however is to prevent remote hacks therefore owners need to ensure they keep the firmware & robot OS up-to-date and ensure long & complex passwords and other multifactor authentication methods are in place (Snodgrass & Curran, 2015).

One of the more famous studies on robot hacking to date was on a telesurgery robot called Raven II, which was developed at the University of Washington. Raven II has two surgical arms that are manipulated by a surgeon using a state-of-the-art control console which includes video and haptic feedback. The robot communicates with the control console using a standard communications protocol for remote surgery known as the Interoperable Telesurgery Protocol over public networks that are potentially accessible to anyone. A research team showed how they could change the commands sent by the operator to the robot by deleting, delaying or re-ordering them thus causing the robot’s movement to become jerky and difficult to control. They

also modified the degree it should rotate they were able to perform a denial of service attack on the robot as well. The motivation to build rigorous and secure robots should be there because it is quite possible that all involved in its design could be held liable if a horrendous weakness was found that led to personal distress or financial losses. Security should also not be an afterthought. There is a worry about hackers controlling home appliances in different scenarios such as having fun with compromised webcams, disabling microwaves to home alarms. Ultimately every device connected to the Web should be password protected. It should not be connected with the default out of the box password. A long complex password needs to be set. All devices should be updated as soon as updates are released, just like best practice on PCs and tablets. All devices which do not need to be connected to over the Internet should be disconnected. That seems obvious but many people enable remote connectivity "out of the box" when they have no intention of connecting to the device when away from home. Manufacturers should also release security updates once vulnerabilities are found but the incentive is simply not there for them to do it much of the time.

All robots connected to the network should be password protected. It should not be connected with the default out of the box password. A long complex password needs to be set. All devices should be updated as soon as updates are released, just like best practice on PCs and tablets. All robots which do not need to be connected to over the Internet should be disconnected. That seems obvious but many people enable remote connectivity "out of the box" when they have no intention of connecting to the device when away from home. Robot manufacturers should also release security updates once vulnerabilities are found but the incentive is simply not there for them to do it much of the time. Pressure should always be placed on manufacturers to deploy fixes for known vulnerabilities.

Hacking Cars

As electronics and related code become more integrated into modern vehicles, we are reaching a point where they will require similar protection as smartphone, tablets and traditional computers. There is a real worry about hackers controlling vehicles in different scenarios such as having fun with the songs being played, downloading rogue apps, disabling the vehicles ignition, to overriding braking systems. Similar to the early days of the Internet, security has not received a great deal of attention to date from car manufacturers. Researchers have demonstrated in controlled experiments that vehicles can be controlled via the telematics systems at great distances and they have successfully embedded malware over wireless connections. Modern smartcars in general are becoming more susceptible to electronic attacks which can be more effective than previous 'slim jim' type brute-force car opening attacks. In recent weeks, it has been disclosed that a £15 wireless device can be purchased online which amplifies a modern cars wireless entry system so that it the signal travels from the thief's device to the owners keys up to 100 yards away allowing them access to the car and ability to drive away in seconds Finally, a risk associated with rolling out technology in smartcars as opposed to other platforms is the potential of distraction leading to accidents due to poor design or malfunctions. Technology experts outside of aviation and medical products tend not to follow stringent testing methodologies but lazily rely on fixing problems as they arise. Therefore a mis-configured service in a fast moving smartcar can lead to death. A number of factors may lead to change however. The motivation to build rigorous and secure systems should be there because it is quite possible that all involved in its design could be held liable if a defect caused or even contributed to a collision.

Vehicles have evolved to contain a complex network of as many as 100 independent computers, electronic control units (ECUs). ECUs perform a variety of functions such as measuring the oxygen present in exhaust fumes and adjusting the fuel/oxygen mixture improving efficiency and reducing pollutants. Gradually these ECUs have become integrated into nearly every aspect of a vehicle’s functioning, including steering, cruise control, air bag deployment and braking. In an article published in IEEE Spectrum, the authors stated that an "S-class Mercedes-Benz requires over 20 million lines of code alone" and "has nearly as many ECUs as the new Airbus A380 (excluding the plane’s in-flight entertainment system)." They estimated that vehicles will soon "require 200 million to 300 million lines of software code." This more than anyone

statistic must surely demonstrate the vulnerable nature of the 20th century vehicle. In addition, not only do these ECUs connect to each another but they now can connect to the Internet, making vehicle computers as vulnerable to the same digital dangers widely known among other networked devices: Trojans, viruses, denial-of-service attacks and more. It is quite common for new vehicles to have numerous connectivity modes such as through cell phone networks and to the Internet via systems including OnStar, Ford Sync and others. They have Bluetooth connectivity, short-range wireless access for key fobs and tyre pressure sensor. Some support satellite radio and they also have inputs for DVDs, CDs, iPads and USB devices.

One of the earlier hacking studies was done by the Center for Automotive Embedded Systems Security, the Washington team which was able to bring a wide range of systems under external control, such as the engine, brakes, locks, instrument panel, radio and its display. The attackers posted messages, initiated annoying sounds and even left the driver powerless to control radio volume. They also attacked the Instrument Panel Cluster/Driver Information Center displaying cheeky messages and altered the fuel gauge and speedometer readings, adjusted panel illumination. Subsequent hacks took over the Engine Control Module which lead to uncontrollable engine revving, readout errors and complete disabling of the engine. Lately Chrysler jeeps have been hacked from many miles away. The almost universal controller area network bus on vehicles - known as the CAN bus makes such breaches possible. All modern vehicles possess 'On-Board Diagnostics' port which allow mechanics to diagnose faults and retrieve information on the vehicle's performance and in some cases change aspects such as the timing of the engine. This is becoming the main access point for hackers as everything can be changed using this port. Yes, important aspects such as the speed control, steering and brakes are all located on a separate vehicle network, there is still interconnectivity between both vehicle network backbones so that a breach in one can cause havoc in the other. It is presently still a difficult system to breach but as more and more exploits get shared on the Internet, there is much cause for worry. The vehicle mobile phone hardware providing a connection to the on-board computer system is also vulnerable to malware being installed which could allow a thief to unlock the car remotely and steal it. This is serious as is already talks of an app store for vehicle apps.

At this time, the biggest fear the driverless community have is an early autonomous or connected-vehicle traffic crash as it could prove to be calamitous. Bad publicity is a real risk for the deployment of innovative automotive technology and lately a poorly sourced news article made the rounds claiming that one driverless car had cut another driverless car of in traffic. The headlines wrote themselves but the truth of the matter really did not back the originating claimant. Of course when Antilock Braking Systems (ABS) were first introduced, negative publicity and poor consumer education delayed mass-market adoption. Similarly, when Electronic Stability Control (ESC) systems were rolled out, consumers did not fully understand how to make use of the technology. On the road, however, these systems delivered a clear, quantifiable reduction in fatalities. Once consumers understood how these systems worked, widespread adoption of ABS and more effective use of ESC followed. Driverless cars will also inevitably generate large amounts of data. This will be useful for many future uses such as crowdsourcing optimal routes or personal location based services however this can also lead to privacy concerns. Whether it is your insurance company, the automaker, or your local dealer, or even local law enforcement, all could have yet another means to track your every coming and going. Hackers may target this personal mobility data so as to capture data, modify records, instigate attacks on systems and/or tracking individual vehicles. We may also see denial of service attacks on vehicles. The possibilities are the core material in sci-fi movies.

The key to preventing these forms of privacy attacks are to remove identifying information and suppress data. Encryption of course must be used and where possible tamper-proof hardware and enforce user-defined privacy policies. The success of driverless cars depends in part on resolving the conflicts in privacy concerns between the stakeholders who will make decisions about how information is collected, archived, and distributed. What is to stop governments spying on their citizens or foreign governments and terrorist groups tracking individuals through their vehicles. Proof of concept hacks have shown how to listen in on vehicle conversations through the in-built Bluetooth hands-free system. This would reveal many secrets to interested parties. Some early prototypes are beginning to communicate with the grid, the cloud and other vehicles. It will not be long until smartcars by default will likely keep an activity log for service and debugging. Security for vehicles as in other sectors can be one of the areas in which cost savings can be made. There is always a rush to market and to date of course, most hacks have been primarily theoretical. This and other factors has led to security not receiving a great deal of attention to date from manufacturers. Even if functions such as the

speed control, steering and brakes are all located on a separate vehicle network, there can still be interconnectivity between both vehicle network backbones so that a breach in one might cause malfunctioning in the other. A risk associated with rolling out technology in vehicles as opposed to other platforms e.g. homes, offices is the potential of distraction leading to accidents due to poor design or malfunctions in the new product. Technology experts outside of aviation and medical products tend not to follow stringent testing methodologies but lazily rely on fixing problems as they arise (McKelvey et al., 2015).

Vehicle 'operating system' security currently resides with the manufacturers (i.e. you cannot install McAfee or Norton anti-virus) but it is advisable to familiarise oneself with aspects such as the remote shutdown feature. For instance, who and what can cause that system to shut the car down. Also, one should be careful when installing third-party electronic accessories as they may not be as rigorously designed as an original manufacturer feature. If you are extra paranoid, you may want to restrict access to the OBD-II diagnostic port. This is a key diagnostic port used by service mechanics but it is also a key attack vector to upload malicious code. Crucial components of the future will be the mobile networks, ad hoc (car to car) networks, vehicles to/from road sensors and satellite communications. We can expect a significant portion of the Internet to be consumed by vehicle communications. In the future, all smartcars will have network connectivity. It will possibly become part of the national MOT - that your 4g/wifi is active & working - otherwise you could be fail. This will allow them to receive firmware/software updates and synchronisation over the local home/network of music, GPS data etc. It is only a small step for much of the telemetry data associated with that vehicle to also be uploaded so as to allow a city to optimise traffic management. Therefore, not only will it be important to keep our communication gadgets updated but it will also be as important to keep our driverless cars updated to the latest OS rollout. Already, the most impressive car hack on the Chrysler was done due to a weakness in the mobile network connectivity service. A saving grace for now is there are not many motivations to stealing vehicles via a sophisticated hack because of the complexity involved and sophisticated tools needed. It is still easier to use a Slim Jim. However that will change in the days ahead and vehicle manufacturers and telematics installers need to concentrate on all the vulnerable entry points and insert firewalls to restrict access to integrated systems such as the mobile communications service, radio and music system and on-board diagnostics port. They urgently need to update the security of automotive computer systems starting yesterday.

The rise of Ransomware

Ransomware attacks are fast becoming par for the course. The biggest new cyber-crimes in recent times have undoubtedly being related to the rise in the crytocurrency Bitcoin. The use of an anonymous payment method allows criminals to now infiltrate the hard-drives of companies and individuals and hold their files ransom until a payment in Bitcoins is sent. This is known as Ransomware. Recently, we have seen a dramatic rise in Ransomware Denial of Service attacks using Bitcoin as the payment method. Here the hackers threaten to bring a site to its knees unless the ransom is paid. Again, this is a new avenue and a growing treat from home users and businesses right up to large scale ICS/SCADA systems as now the hackers can demand payment just to leave them in peace. Some early versions of cryptolocker ransomware did have weaknesses and fixes arose to overcome the poor encryption and retrieve files. Unfortunately, those days are over. The latest flavours are simply written more professionally and once those files are locked, they are locked pretty much forever. There are a lot of new cryptolockers in the wild of course and quality differs but anecdotal evidence online suggests that the majority of them are pretty unbreakable.

In an ideal world, we would like no-one to pay a ransom to the criminals. Paying the ransom not only enriches them but also could encourage them to further develop more sophisticated ransomware and target more victims. There is also no guarantee that the payment of a ransom results in the files being unlocked. This has been the case on many occasions. Payment of the ransom really comes down to the value of those files lost. If they are deemed worth the ransom then most people will simply end up paying. Quite often the ransom is far cheaper than the actual costs of losing access to those files.

The main strategy to ensure ransomware is ineffective is to have a proper staged backup plan in place. Files which are backed up offline can simply be substituted for encrypted files and no ransom need ever be paid. Other measures include authenticating in-bound emails. This helps as the majority of infections arise from opening ransomware attachments. Implementing a Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM) and Domain Message Authentication Reporting and Conformance (DMARC) can help guard against spear phishing and other attacks coming through spoofed email. These work together to validate the IP address and domain of the originating email server but sadly, not enough organisations adopt these standards. It also helps to have active scanning of all email in order to detect potential threats.

Having ad-blocking enabled can also help as ransomware is distributed through malicious advertisements served up to users when they visit sites. Some organisations have implemented separate networks for employees surfing the web. There are limited options once an attack is underway due to the rapid file overwriting which is also the main indicator that ransomware is present. Activity-monitoring tools can potentially scan for distinctive patterns that indicate this and take the system or entire network offline to prevent the spread of the virus. Later, disk forensics techniques can be employed to recover unencrypted files (McBride et al., 2015).

The number one preparation for potential ransomware infection is to employ a proper backup policy. The backups should be serialised, with previous versions of files stored. Of course, these backups should not be stored on network attached drives as ransomware can infect shared and removable media. Other preparations include deploying firewalls, active attachment scanning and web filtering in addition to IDS's and anti-malware. Best practice with regards timely patching of systems also helps. Restricting user privilege is important as malware executes with the same privileges as the victim is running with. Of course the most effective way for ransomware to gain a foothold on people's computers is when people to click on links. This can be done by placing these files online and tricking people into downloading them or more commonly, by sending people 'phishing emails'. Phishing emails are simply emails which can look legitimate either containing attachments or links which then lead people to clicking on them and installing the destructive software. The first line of defence to stop these attacks apart from the firewalls, anti-virus software and intrusion detection systems is to simply educate employees about the dangers of clicking on links. Only a fraction however will listen and learn. It generally takes people to make a mistake before they learn. That can be too late however. There is a new movement where security teams send phishing emails containing fake malware to their employees which when activated simply lead them to a site telling them about their mistake and educating them on the dangers of what they did. Education is crucial.

Conclusion

In computer security, being paranoid is considered a positive trait. Ultimately, trust no one. Encrypt all your data on the phone. Do not trust online cloud services like Dropbox. Encrypt it before it leaves your phone. Don't trust email providers like Hotmail, Gmail, Yahoo etc. Use PGP (Pretty Good Privacy) to encrypt all your email messages. Never trust public WiFi hotspots. Don't use torrent sites or illegal download sites. Do not use the phone for browsing.

It must always be remember that no one involved in the early Internet design ever foreseen the pervasiveness of its involvement in everyday life. That is why we have so many security & privacy issues today.

References

Ronan Comer, Nigel McKelvey, Kevin Curran (2012) Privacy and Facebook. The International Journal of Engineering & Technology, Vol. 2, No. 10, October 2012, pp: 1592-1604, ISSN: 2049-34444

Kevin Curran, Vivian Maynes, Declan Harkin (2015) Mobile Device Security. International Journal of Information and Computer Security, Vol. 6, No. 3, January 2015, pp: , ISSN: 1744-1765

Gabriel Deak, Kevin Curran, Joan Condell, Nik Bessis and Eleana Asimakopoulou (2013) IoT (Internet of Things) and DfPL (Device-free Passive Localisation) in a disaster management scenario, Simulation Modelling Practice and Theory, Vol. 34, No. 3, pp: 86-96, DOI: 10.1016/j.simpat.2013.03.005, ISSN: 1569-190X, Elsevier Publishing

IETF (2016) BCP Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing https://tools.ietf.org/html/bcp38

Piotr Ksiazak, William Farrelly, Kevin Curran (2015) A Lightweight Authentication Protocol for Secure Communications between Resource-Limited Devices and Wireless Sensor Networks. Vol. 8, No. 4, pp: 62-102, October-December 2015, DOI: 10.4018/IJISP.2014100104, ISSN: 1930-1650, IGI Global

Prince, M. (2016) How Cloudflare's Architecture Allows Us to Scale to Stop the Largest Attacks. Cloudflare, Oct 26th 2016, https://blog.cloudflare.com/how-cloudflares-architecture-allows-us-to-scale-to-stop-the-largest-attacks

Frédéric Lusson, Karen Bailey, Mark Leeney, Kevin Curran (2012) A Novel Approach to Digital Watermarking, Exploiting Colour Spaces. Signal Processing, Vol. 93, No. 5, pp: 1268-1294, ISSN: 0165-1684, http://dx.doi.org/10.1016/j.sigpro.2012.10.018

Shaun McBrearty, William Farrelly & Kevin Curran (2017) The Performance Cost of Preserving Data/Query Privacy Using Searchable Symmetric Encryption, Security & Communication Networks, (in pre-print), Vol. 9, No. 16

Brendan McBride, Nigel McKelvey, Kevin Curran (2015) Security issues with contactless bank cards. Journal of Information, Vol. 1, No. 3, DOI: 10.18488/journal.104/2015.1.3/104.3.53.58, pp: 53-55, 2015

Nigel McKelvey, Cathal Diver, Kevin Curran (2015) Drones and Privacy. International Journal of Handheld Computing Research, Vol. 6, No. 1, pp: 44-57, July-September 2015, DOI: 10.4018/IJHCR.2015010104, ISSN: 1947-9158

Ronan O'Flaherty, Kevin Curran (2013) Detecting Anonymising Proxy Usage on the Internet. Wireless Personal Communications, Vol. 72, No. , pp:, ISSN: 0929-6212, DOI: 10.1007/s11277-013-1451-y, Springer

Andrew Snodgrass, Kevin Curran (2015) A Novel Cue based Picture Word Shape Character Password Creation Scheme. International Journal of Digital Crime and Forensics (IJDCF), Vol. 7, No. 3, pp: 37-59, July-September 2015, DOI: 10.4018/IJDCF.2015070103, ISSN: 1941-6210