



The Skynet system. Photo courtesy of EADS.

The secret satellite

In this age of technology, security has taken on a different meaning. Helen Jameson investigates what encryption actually is, why it is so important and new developments that have been made.

When I think about how many passwords, pin-codes, card numbers and identification numbers I have to remember on an everyday basis I find it incredible that I remember them all! However, at the same time, I fully recognise that they are a necessary (perhaps not evil) but part of our lives. The advent of the Internet, mobile communications, new ways of banking, personal

computers and further features that now are a big part of our lives, have created a need for heightened security that was not required a hundred - even fifty or sixty years ago. In an age where our lives are so often dependant on these technological advancements, the systems that we use must be as secure as they possibly can to guard against theft of personal

information...and assets.

Corporations must be constantly checking that the information circulating across their data networks is confidential and that it never falls into the wrong hands. The massive growth of earth-bound security applications is very well known. We deal with it and are aware of it everyday but satellites are no different and it is a necessity that must also be applied to them and their networks to ensure that the users' of the satellites are protected and that their data and that the satellite itself does not fall into the wrong hands. To protect the satellites that are so vital to us we must use encryption and security techniques.

The word cryptography is derived from the Greek word meaning 'hidden' and verb meaning 'write'. It is the study of message secrecy and has a long history stretching back as far as the Egyptians. Several mechanical encryption and decryption devices were invented in the early twentieth century such as the famous Enigma machine and rotor machines. However, the development of digital computers and electronics after World War II made the possibility of encryption much more complex.

Encryption is the process of transforming information to make it unreadable to anyone except those who possess the specific knowledge (key) to decipher it. It is used by militaries, governments and protects civilian systems such as the Internet and ATM machines. However, attacks on the systems are frequent despite state-of-the-art security software.

Computer security

Nowadays, we all use computers in some form or other every day of our lives. The computer age has brought us knowledge, efficiency and we come to rely on computers perhaps a little more than we would like to admit. Computer security is an increasingly important consideration these days, thanks to networking and the Internet which mean that our computers are more interconnected than ever before.

Ciphers are used to encrypt information that is passed from computer to computer. A cipher is an algorithm for performing encryption and decryption and requires well-defined steps to follow in a procedure. A cipher is basically a code and the operation of the cipher depends on a

key. The encrypting procedure is varied depending on the key that changes the detailed operation of the algorithm. A key has to be selected before using a cipher to encrypt a message or it will be difficult, or perhaps impossible, to decode the cipher into readable plain text.

In order to protect the systems from hackers and maintain confidentiality, there are two main types of encryption system:

Symmetric-key encryption

In symmetric-key encryption, each computer has a secret key or code that it can use to encrypt a packet of information before it is sent over the network to another computer. Symmetric-key requires that you know which computers will be talking to each other so you can install the key on each one. Symmetric-key encryption is essentially the same as a secret code that each of the two computers must know in order to decode the information. The code provides the key to decoding the message.

Public-key encryption

Public-key encryption uses a combination of a private (symmetric) key and a public key. The private key is known only to your computer, whilst the public key is given by your computer to any computer that wants to communicate securely with it. To decode an encrypted message, a computer must use the public key, provided by the originating computer and its own private key. To implement public-key encryption on a large scale, such as a secure web server might need, requires a different approach. They will require a digital certificate which is a piece of information that confirms that the web server is trusted by an independent source known as a certificate authority. The certificate authority serves a middleman that both computers trust and confirms that the computer is who it says it is and then provides the public keys of each computer to the other.

Satellite television

Satellite television operators must be able to maintain control of their networks to continue to offer their customers a high quality of service and they use encryption to do this. DTH operators use a 'descrambler' that will decode the encrypted signal to reveal the picture and sound



Photo courtesy of Lockheed Martin.

to the viewer. It is a means of protecting operators from losing customers. Programmers are constantly concerned that their signals may be stolen from them through piracy. For most satellite communications applications, private key (symmetric-key) encryption is most popular. The Digital Encryption System is common. Public and private encryption techniques are highly effective in protecting the user from interception and it has been argued that even without encryption the use of a specialised receiver in itself provides a low level of security. However, with low-cost commercial services such as DTH TV this is not the case and so encryption is a normal part of the operation.

The actual techniques that are used do their job very well but the problem with encryption is protecting the key adequately. The techniques are repetitive and so the key must be changed on a regular basis to prevent interception by pirates. If the new keys are distributed over the

same link that must be protected, pirates may access them if they have managed to override the key once. Therefore, smart cards and chips have been introduced to add another layer of security. The user must have a decryption device, a key and a smart card in order to use their system. If a system is compromised, a new card may be sent out to all authorised users. Another means of protection may be connecting to a telephone line to receive new key data for example.

Commercial satellite security

The question of security in commercial satellites was raised again in April 2007, when Intelsat issued a statement with regard to the unauthorised use of one of its satellites by the Liberation Tigers of Tamil Eelam (LTTE), a Sri Lanka-based terrorist group. Intelsat officials, including its technical experts, met with Sri Lanka's ambassador, Bernard Goonetilleke, on 10 April 2007 to dis-

cuss the steps Intelsat is taking to address the unauthorised use of one of its satellites by the LTTE. During the meeting, Intelsat's General Counsel, Phillip Spector said, "Intelsat does not tolerate terrorists or others operating illegally on its satellites. Since we first learned of the LTTE's signal piracy, we have been actively pursuing a number of technical alternatives to halt the transmissions. We are clear in our resolve to ending this terrorist organisation's unauthorised use of our satellite."

The Sri Lankan Embassy and Intelsat agree that these illegal transmissions by the LTTE are a violation of Sri Lankan and US laws. Following the discussion, Ambassador Goonetilleke said "I am satisfied that Intelsat is taking these unauthorised transmissions very seriously, and believe it will do all that it can to stop the terrorist transmissions. I am confident that Intelsat will continue to co-operate with the Sri Lankan authorities in this matter.

A report undertaken by Surrey Space Centre in the UK entitled 'On-Board Security Services in Small Satellites' states that there have been other attacks in recent times. The Embry Riddle Aeronautical University obtained National Oceanic and Atmospheric Administration satellite imagery with only basic apparatus. In addition, researchers from a Japanese University were able to access information from LandSat, NASA's earth observation satellite. There is concern that NASA's Space Internet project will see users and scientists directly accessing the satellite to garner information. This gives enormous flexibility but can also lead to illegal use of data and unauthorised access.

Surprisingly, few earth observation satellites have on-board security. The encryption techniques tend to be used for the data that is beamed down to the ground station. For secured, on-board communications it is imperative that the uplink and downlink is protected. All security methods should be in place – confidentiality, integrity, authentication, non-repudiation and access-control – to provide comprehensive protection. The constant monitoring of the uplink or telecommand is also of great importance in order to protect the satellite from being taken over by unauthorised entities. The preferred algorithm for satellite communications, which is now widely deployed, is the Advanced Encryption Standard

(AES). This algorithm supports a large range of block and key sizes and is now used for classified information.

Aside from all these details, the satellite must have the ability to detect and correct a fault on board the satellite before any data is beamed back to the ground station is essential. If not, the satellite is open to interception.

Quantum cryptography

We are always going to try to heighten our security levels and new, and perhaps unexpected, developments are making our ears prick up. Quantum mechanics have given rise to a new form of cryptography, quantum cryptography. Here, quantum mechanics are used to provide secure communications. MagiQ Technologies, a New York-based company specialise in quantum information solutions. Their Quantum Private Network (QPN) is based on the AES.

The security of Quantum Cryptography lies in its ability to exchange the encryption key with absolute security. By sending the key encoded at the single photon level on a photon-by-photon basis, quantum mechanics guarantees that the act of an eavesdropper intercepting a photon, even if it is just to observe or to read it, irretrievably changes the information encoded on that photon. Therefore, the eavesdropper can neither copy nor clone a photon nor read the information encoded on the photon without modifying it, a process that is provably detectable. The use of quantum keys and truly random numbers makes data encryption uncompromisingly secure. This new type of cryptography has attracted the military and commercial sectors alike.

Last year, they unveiled their QPN 8505, a next generation quantum cryptography system that relies on the laws of physics rather than the computational difficulties of breaking keys. It is easily integrated into existing digital computing network infrastructures and incorporates real-time key generation for absolute security in detecting compromised keys and, in providing real-time detection. It is targeted at government applications including military intelligence gathering and homeland defence but is also suitable for financial services, telecommunications carriers and disaster recovery.

Work is being carried out by various agencies to see whether quantum cryptography can

be used in space technology. If so, the possibilities could be endless.

Military satellite

The military sector itself has seen significant developments in secure satellite manufacturing. In this line of work, secure satellite communications are imperative and close attention is paid to the developments that are made. High frequency satellites are now providing highly secure satellite communications. In the theatre of war, where highly confidential intelligence is passed from person to person, security is paramount.

Lockheed Martin recently announced that it has delivered ahead of schedule the flight structure for the third space vehicle in the Advanced Extremely High Frequency (AEHF) programme to the company's Mississippi facility for integration with its propulsion subsystem which is essential for moving the satellite when conducting on-orbit operations and re-positioning. AEHF satellites will provide global, highly secure, protected, survivable communications for warfighters in all services within the US Department of Defense.

AEHF satellites are based on Lockheed Martin's flight-proven A2100 geosynchronous spacecraft series and will deliver 10 times greater total capacity and channel data rates six times higher than that of Milstar II communications satellites. The higher data rates permit transmission of tactical military communications such as real-time video, battlefield maps and targeting data.

The Advanced EHF Programme is the follow-on to the DoD's Milstar highly secure communication satellite programme, which currently has a four-satellite operational constellation. The last Milstar satellite was successfully launched in April 2003.

As envisioned by the Pentagon, the fully operational Advanced EHF constellation will consist of four crosslinked satellites providing coverage of the Earth from 65 degrees north latitude to 65 degrees south. These satellites will provide more data throughput capability and coverage flexibility to regional and global military operations than ever before. A fifth satellite built could be used as a spare or launched to provide additional capability to the envisioned

constellation.

To accomplish this, Advanced EHF adds new higher data rate modes to the low data rate and medium data rate modes of Milstar II satellites. The higher data rate modes will provide data rates up to 8.2 million bits of data per second (Mbps) to future Advanced EHF Army terminals. That rate is more than 150 times faster than the 56 kilobit-per-second modems of today's personal computers. Each Advanced EHF satellite employs more than 50 communications channels via multiple, simultaneous downlinks. For global communications, the Advanced EHF system uses inter-satellite crosslinks, eliminating the need to route messages via terrestrial systems.

Lockheed Martin is currently under contract to provide three Advanced EHF satellites and command control system to its customer, the Military Satellite Communications Systems Wing at the Air Force's Space and Missile Systems Center, Los Angeles, California. The contract for a third AEHF spacecraft was awarded early last year.

With the propulsion module and payload in place, the team will begin final assembly, integration and test in preparation for launch in April 2008. Development of the second AEHF satellite is following close behind and proceeding on schedule for launch in April 2009.

Ground-breaking military satellite

Skyнет 5 is the ground breaking next-generation military satellite communications programme to provide end-to-end, resilient, secure Beyond Line of Sight communications services, including welfare, to the UK MoD and other non-UK MoD and multinational customers until 2020.

The programme provides delivery of information services between the UK's Defence Fixed Network and in-theatre networks and users. Secure communications services will be delivered by the owner and operator - Paradigm Secure Communications with the system, including the satellites, designed and built by Astrium Satellites. Both companies are wholly owned by Astrium, a subsidiary of EADS (European Aeronautic Defence and Space Company).

Astrium is also prime contractor on the Ariane 5 launchers in charge of manufacturing and recently signed an agreement with

Arianespace to step up production of Ariane 5 launchers.

The MoD contract, which is now worth £3.6 million was placed with Paradigm in October 2003. It is the UK MoD's largest and most complex Public Finance Initiative (PFI) contract to date.

The deal was restructured at the end of 2005 exploiting the opportunity of risk retirement and better financial conditions, resulting in the addition of a third satellite.

The UK MoD considered the launch, testing and commissioning of the satellite to be a major milestone for the armed forces. Brigadier Simon Shadbolt, Director of Equipment Capability for the Ministry of Defence remarked that the satellite replaces Skynet 4 and reflects the increase in capability that is required in modern day conflicts worldwide.

Skynet 5A assures reliable and resilient communications and will help the armed forces to tackle new and emerging threats.

Communications for troops in the field

The satellite will provide communications for troops deployed in Iraq and Afghanistan and feedback has already been positive with troops noticing the increased capacity and capability of the system. Skynet 5 in fact delivers 2.5 times the capability the Skynet 4 system delivered and gives troops and commanding officers flexibility and easier management of information. The drive towards information management is vital and the UK MoD must be able to manage and exploit information at all levels of conflict. Skynet 5 is part of getting the information and imagery where it needs to go and perhaps move on to a more network centric warfare with a battlefield that is connected.

At present, the army faces budgetary constraints with regard to bandwidth and incrementally increase when it is necessary. However, the need to disseminate information is of top priority but the need to reduce rather than increase the amount of networks used by the MoD is also of great importance. It is recognised that the demand for bandwidth will always be high but, at the end of the contract, the need for capacity will be reviewed by the MoD and decisions will then be taken on whether further capacity will be needed.

Skynet 5A is the first of a three satellite constellation heralding a new era in military communications and will be the highest power X-band satellite in orbit. Built to support the most challenging missions Skynet 5A is nuclear and laser hardened to demanding NATO standards. The Skynet 5 satellites are based on Astrium's Eurostar E3000 satellite platform with a 34m solar array span and a launch mass of 4.7 tonnes.

The world leading anti jamming antenna is extremely effective against hostile or non-hostile interference. All transmit beams are steerable and the active antenna forms multiple complex receive beam patterns to maximise terminal performance.

Paradigm will operate the latest state-of-the-art military X-Band satellites and an extensive ground infrastructure from sites in Wiltshire or Hampshire.

In addition to complete X-Band packages, Paradigm is able to offer capacity, coverage augmentation, anchoring, back-haul services, as well as terminal leasing.

Paradigm is currently providing services to support MoD operations and welfare in Iraq, Afghanistan and the Balkans. Welfare services include free messages between UK military personnel deployed on operations and their families at home. In addition, Paradigm is also providing services to NATO, France, Germany, Canada, Portugal and the Netherlands.

The need for security

Satellite systems can provide extremely secure communications. They are both reliable and resilient and with the correctly considered encryption and security techniques they can be made highly secure. The satellite industry is constantly striving to make their communications more secure than ever.

The threats posed by those who are constantly trying to keep up and crack the codes will continue to grow. It is a game of cat and mouse that both commercial and civil entities are trying to win. We all know how important it is to prevent ourselves from becoming victims of those who intercept our personal information. Our reliance on satellites may not always be obvious but those systems that are in place to protect them, in turn protect us.