QINETIQ

Secure Data Transfer

In 1904, as the Russian fleet prepared for conflict with Japan, the British ship HMS Diana stationed in the Suez Canal was able to intercept Russian naval wireless signals for the first time in history. An intelligence report on those signals shows that not only were the Royal Navy interpreters unimpressed with their adversaries' slow workrate, they were also particularly critical of the poor standard of grammar and spelling.

Transfer request

Today, the ability to intercept data transfer provides an opportunity for even richer insight. Maintaining global national security is still a contest of wills but technology is changing its character and with it, the vulnerabilities that must be addressed. As defence and security practices have become more digital, the volume of data transferred between organisations, forces, and individuals has also increased. Whether it is raw senor data, commands, or situation analysis, every snippet has a value to the enemy. The ability to rapidly share data has therefore become both an advantage and a weakness.

Maintaining the integrity of data as it passes through the nodes of global defence and security has always been a priority but it is harder now than ever before. The technology available to intercept signals has become smarter and more sophisticated. The technologies employed to prevent interception, and to detect it quickly need to keep up. There are several novel technologies that offer a way to improve the current situation. The first is based on optical technology, the second is quantum-based, and the third is an existing commercial approach that could be relevant for future defence and security applications.

Optical communication

The use of optical technology to send and receive data is a well-established practice in many environments. The adoption of superfast broadband Internet services has relied on fibre optic cabling to ramp up transfer speeds from tens of megabits to several gigabits per second. That kind of speed has the power to transform the world of defence, which currently has to rely on much slower connections – sometimes just 10s of kilobytes per second. But importantly it also provides a way to boost the security of data transfer through an inherent low probability of interception.

Today's defence forces tend to rely on radio frequency (RF) transmissions to share information. That means broadcasting data over a pre-determined frequency, and encrypting it to prevent other parties (who may be able to intercept it), from being able to understand the content. Research is now underway to develop the use of military free space optical communication to offer a direct route from origin to recipient and reduce the need for RF transmissions in some defence and security scenarios. This involves firing a laser through the air from one point to another and sending data down the beam straight to the recipient. Not only does that offer much faster data transfer speeds but it also reduces the opportunities for interception and therefore the need for complex and time-consuming cryptography at either end of the transmission. It also offers zero risk of any conflict with another party using the same part of the RF spectrum because the laser is beamed direct from one location to another. Whilst this is not intended to replace RF communication, which remains effective in many circumstances, there are some obvious scenarios where a direct and secure transfer of data makes much more sense. For example, defence and security have become global endeavours over the last two decades and collaborative efforts with other nations are now a requirement for success, not an option. Sharing information between different assets from many nations, such as two ships working together in the same waters, requires both nations to share cryptographic information – something neither will want to do if they can help it. In this scenario, the ability to share data directly, quickly, securely and without the need for encryption removes the issue entirely.

Free space optical communication is not without its challenges. Line of sight is a requirement for success, and maintaining a link between moving platforms can present problems. It also suits communication between just two points, not multiple points, so optical communications cannot suit all use cases. But research and development continues regardless. A ground trial of military use-cases is due to take place in October and it plans to demonstrate that more than a gigabit per second speed is possible using this method, so watch this space.

Quantum Key Distribution

Optical communication is not simply a viable emerging technology for data transfer. It also allows for other approaches that can add to the security of data sharing. One such approach is Quantum Key Distribution.

One of those is Quantum Key Distribution (QKD) – the use of quantum physics to create a highly secure way of maintaining encryption. To understand why this is potentially important to future defence and security data transfer it is worth dipping into the basics of cryptography.

Today, secure communication is protected using symmetric cryptography. A key is used to determine how to mangle data prior to transfer and at the other end the same key is used to determine how the data was mangled so those steps can be reversed. This means that a secure way of distributing these keys is needed and a common way of achieving this today is by using asymmetric cryptography. This uses the same principle to protect a key during its distribution but different keys are used to mangle and 'unmangle' the data. As a result, the encrypting key can be shared publicly because no one will be able to decrypt the message without the decrypting one as well. It's like having two keys to your front door – one to lock it and a separate one to open it. The lock-up key can be left lying around and it won't compromise the security of your home. Only the person with the unlock key can get in.

Unfortunately the development of viable quantum computers is likely to have a dramatic impact on current asymmetric cryptography algorithms since they were never designed with this sort of threat in mind. Organisations such as NIST have already begun the development and review of new asymmetric algorithms designed to resist the attacks posed by quantum computers. However the acceptance of one of these into the Federal Standard is likely to take a substantial period of time, perhaps even comparable to the time taken to develop a QC.

QKD uses quantum effects to protect a key during its distribution. This distribution is usually made through optical communications, for example, optical fibre or via lasers between satellites and ground stations. If someone intercepts and eavesdrops on the message, the physical properties of that message change at the quantum level - meaning we can easily tell that the message has been compromised. While this can be implemented today, there are still a number of engineering challenges to be tackled before we can build a workable system. These include bandwidth and portability issues along with, of course, all of the inherent challenges in building quantum encrypted satellite comms systems. But the science is sound - it has been demonstrated outside of a lab, and it offers the cryptographic properties required to build suitable cryptosystems.

Organisations such as the European Space Agency (ESA) are investing heavily in the development of quantum encryption satellites, and many governments around the world are funding research into quantum-enabled communications infrastructure. So, QKD might not be in active use today but defence and security organisations cannot simply view it as a 'solution to a problem that doesn't yet exist'.

Blockchain

Blockchain is essentially a digitally distributed database containing a record of transactions that is shared across multiple owners and cannot be altered without all the owners being aware that a change has made and where that change has occurred. Blockchain is widely used to underpin successful crypto currencies, acting as a register of transactions impervious to clandestine manipulation. It is an engine for data integrity upon which every party can rely.

Maintaining data integrity in defence systems is a key component of security, from supply chain and asset management, to situational awareness and command and control information tracking. This is particularly true in a high-end conflict where adversaries may contest the electromagnetic spectrum. So it would make sense that Blockchain – which is designed specifically to protect the integrity of data – should have a significant role to play in securing critical transmissions. Certainly many have suggested as such.

But that is not necessarily the case today. In 2018 the National Institute of Standards and Technology published a paper which posed six key requirements for there to be a viable use case for applying Blockchain technology to a given scenario. These include that more than one entity will contribute data; sensitive information will not be stored; and, critically, that there is no clear owner who should be in in control of the data store itself. Because defence and security environments are characterised by a truly linear system of authority, and an implicit trust between the users and that authority, this last criteria in particular will not be currently be met. There will always be a clear owner and an authority for the data store –and therefore any small advantages of implementing Blockchain technology today will be vastly outweighed by the cost and complexity of implementation.

That does not mean it will be not be relevant further down the line. There are indeed several future scenarios we can envisage where this might be a more pertinent approach –particularly as we move to more distributed models of fighting and more military support for distributed civilian environments. The rise in robotics and autonomous systems, and the growth of agile command and control systems are both worthy of consideration because they are predicated on the automated transfer of data between many assets at similar levels in an operation, not simply up and down the chain of command. In that scenario – a high integrity log of data sharing and corresponding actions has merit. For now though, Blockchain technology is not a viable solution for securing data transfer.

Securing the transfer of data is already an essential part of maintaining national security and delivering successful operations but it is becoming harder. Competing with increasingly sophisticated attacks from a range of adversaries requires constant review of opportunities to neutralise their impact. Emerging technologies could hold some of the answers but it is far from clear which ones, if any, will help defence and security organisations maintain total control of their data.