Is your data actually secure?

Do high profile government and corporate data losses suggest that we're losing our grip on data protection and security? Michael Barrett, MD at Nexus Industrial Memory thinks not, and explains what that means for the military

Every few months, some sort of data breach makes the headlines. Sometimes it's a corporation whose data has been breached, like Uber. Other times it's a government.

Every time it raises question marks about how secure data is, and – specifically in the case of governmental data breaches – makes people wonder if the government in question has what it takes to keep data secure.

So here's the reality: Government communication, particularly when it is at a high level, is extremely secure and becoming more and more so with every year that passes.

The same is true of military communications and data encryption, an area in which we do a lot of work. In fact, that's one of the key reasons why our flagship product – Datakey portable data carriers – exists: to ensure that official secrets remain just that.

Where Hollywood reflects real life

Most of us have seen a film where 'data encryption' takes place. Maybe it's in a James Bond movie, or Doctor Who or a murder mystery on TV. And whilst most depictions of data encryption in popular culture come with their fair share of flaws, the depiction of what actually is possible isn't far from the mark.

In countless TV shows and movies, you'll see a character using some sort of key to communicate or transfer data to another person or entity, who also possesses a similar piece of technology to receive and understand the data.

Typically, this sort of technology is known as a CIK (Crypto Ignition Key), and although most instances of it in film and television are fictitious, the premise is anything but.

Most people understand that there are ways of producing secure access keys that allow two or more people to communicate, or take a particular action with both parties' permission. However, very few people know how these keys are produced.

This is even true in industry, where design engineers will often attempt to use other forms of data storage devices to create similar security 'keys', when in fact only dedicated industrial portable memory products, like those Nexus supplies, can really do the job.

How the CIK works in the military

Security in military projects has always been paramount and therefore the concept of the CIK is both well understood and rapidly evolving. What makes a CIK like the Datakey range we supply so attractive to security conscious clients is that it really is very secure. In fact, we often don't know exactly what the products we supply are going to be used for, and because they're so secure, we're never going to know!

What we do know though is that the Datakey range of portable memory products is used extensively in the field of cryptographic network security. There are two market leading products in the UK which protect voice, data and video communication up to and including UK Top Secret, and Datakey tokens play a key role in both, ensuring that the communication flows remain encrypted and protected from potential eavesdroppers.

All of these devices using the memory token as a CIK, support PRIME, the UK's strategic standard for IP crypto. All network encryption devices with conformance to the PRIME framework are independently tested as part of the PRIME certification process.

As well as communication, memory tokens are used in security applications by both the military and the Government. Some of these are 'two key systems', in which one key is assigned seniority as a 'supervisor' key. Both keys are required if a certain action, ranging from opening a door to gaining access to armaments, is to be performed in the system.

This kind of operation often features a record keeping function on the key, which can be as complex as the software that runs it. Normally though, the minimum data it would record would be the location of the key and the activities it has been used to perform.

Balancing the need for security, strength & long life

Of course, in addition to data safety security, some designers have unique needs such as ruggedness, ingress protection or ease of operation. For instance, we have worked on military applications where the end user will be working in harsh conditions and therefore wearing gloves, which means ease of use has to be paramount.

At the heart of most designs is the need for longevity – the last thing any design engineer wants to be doing is redesigning something at great expense five years later because the technology is no longer good enough.

And it's this feature that sees a lot of Government and military bodies choosing Datakey – the blend of security and ruggedness, coupled with a lack of obsolescence makes them an ideal choice for those types of organisations.

We are committed along with ATEK (manufacturer of Datakey products) to ensuring that every product we sell can be re-ordered during the lifespan of the product the OEM builds it into, providing we can agree on a chip that will have the appropriate longevity itself. For instance, today we would recommend SPI (Serial Peripheral Interface Bus) over Microwire or I²C (Inter-Integrated Circuit).

The memory tokens used to secure communications are a great example of this kind of longevity. The current token used in the PRIME network encryption devices has been available since the 1990s and will be available for many years to come. There is no other data storage technology that you could buy in the early 1990s that is still available now.

Of course, the range of Datakey portable data carriers have improved in that time, developing larger memory capacities and new functionality, but a customer who bought a specific memory Key or Token nearly twenty years ago can place an order for a like for like replacement today.

So there you have it, data security isn't decreasing – if you choose the right provider, you can enjoy all the benefits that Hollywood tantalises us with, and much more.

www.nexusindustrialmemory.com