A GENISYS GROUP Publication

THE UK'S FASTEST GROWING CORPORATE TECHNOLOGY DIGITAL MAGAZINE
Packed with news, opinion, debate and reviews by expert analysts you can trust

CIOTODAYUK.COM

CIO TODAY UK

innovation for tomorrow, today

MARCH 2015 MONTHLY

Don't Be Next!

HOW TO STOP THE NEXT HACK ATTACK

ALSO IN THIS ISSUE

The Data Privacy Officer's Role

UK Virtualisation Viewpoint

Bringing Order To Incident Response

Bring Your Own Encryption –

Balancing security with practicality

BEING FREE TO CHOOSE THE MOST SUITABLE encryption for your business seems a good idea. But it will only work in a context of recognised standards across encryption systems and providers' security platforms. Dr. Hongwen Zhang, Chair Security Working Group, CloudEthernet Forum explains.

Since the start of the 21st century, security has emerged from scare-story status to become one of IT users' biggest issues – as survey after survey confirms. Along the way a number of uncomfortable lessons are still being learned.

The first lesson is that security technology must always be considered in a human context. No one still believes in a technological fix that will put an end to all security problems, because time and again we hear news of new types of cyber attack that bypass sophisticated and secure technology by targeting human nature – from alarming e-mails ostensibly from official sources, to friendly social invitations to share a funny download; from a harmless-looking USB stick 'accidentally' dropped by the office entrance, to the fake policeman demanding a few personal details to verify that you are not criminally liable.

And that explains the article's heading: a balance must be struck between achieving the desired level of protection against keeping all protection procedures quick and simple. Every minute spent making things secure is a minute lost to productivity – so the heading could equally have said "balancing security with efficiency".

The second lesson still being learned is never to fully trust to instinct in security matters. It is instinctive to obey instructions that appear to come from an authoritative source, or to respond in an open, friendly manner to a friendly approach – and those are just the sort of instincts that are exploited by IT scams. Instincts can open us to attack, and they can also evoke inappropriate caution.

In the first years of major cloud uptake there was the oft-repeated advice to business that the sensible course would be to use public cloud services to simplify mundane operations, but that critical or high priority data should not be trusted to a public cloud service but kept under control in a private cloud. Instinctively this made sense: you should not allow your secrets to float about in a cloud where you have no idea where they are stored or who is in charge of them.

The irony is that the cloud – being so obviously

vulnerable and inviting to attackers – is constantly being reinforced with the most sophisticated security measures: so data in the cloud is probably far better protected than any SME could afford to secure its own data internally. It is like air travel: because flying is instinctively scary, so much has been spent to make it safe that you are
less likely to die on a flight than you are driving the same journey in the "safety" of your own car. The biggest risk in air travel is in the journey to the airport, just as the biggest risk in cloud computing lies in the data's passage to the cloud – hence the importance of a secure line to a cloud service.

So let us look at encryption in the light of those two lessons. Instinctively it makes sense to keep full control of your own encryption and keys, rather than let them get into any stranger's hands – so how far do we trust that instinct, bearing in mind the need also to balance security against efficiency?

BYOK

Hot on the heels of BYOD – or "Bring Your Own Device" to the workplace – come the acronym for Bring Your Own Key (BYOK).

The idea of encryption is as old as the concept of written language: if a message might fall into enemy hands, then it is important to ensure that they will not be able to read it. We have recently been told that US forces used Native American communicators in WW2 because the chances of anyone in Japan understanding their language was near zero. More typically, encryption relies on some sort of "key" to unlock and make sense of the message it contains, and that transfers the problem of security to a new level: now the message is secure, the focus shifts to protecting the key.

In the case of access to cloud services: if we are encrypting data because we are worried about its security in an unknown cloud, why then should we trust the same cloud to hold the encryption keys?

Microsoft recently announced a new solution to this dilemma using HSMs (Hardware Security Modules) within their Windows Azure cloud – so that an enterprise customer can use its own internal HSM to produce a master key that is then transmitted to the HSM within the Windows Azure cloud. This provides secure encryption when in the cloud, but it also means that not even Microsoft itself can read it, because they do

not have the master key hidden in the enterprise HSM.

It is not so much that the enterprise cannot trust Microsoft to protect its data from attack, it is more to do with growing legal complexities. In the wake of Snowden revelations, it is becoming known that even the most well protected data might be at risk from a government or legal subpoena demanding to reveal its content. Under this BYOK system, however, Microsoft cannot be forced to reveal the enterprise's secrets because it cannot access them itself, and the responsibility lies only with the owner.

This is increasingly important because of other legal pressures that insist on restricting access to certain types of data. A government can, for example, forbid anyone from allowing data of national importance to leave the country – not a simple matter in a globally connected IP network. There are also increasing legal pressures on holders of personal data to guarantee levels of privacy.

Instinctively it feels a lot more secure to manage your own key and use BYOK instead of leaving it to the cloud provider. As long as that instinct is backed by a suitable and strict in-house HSM based security policy, these instincts can be trusted.

BYOE

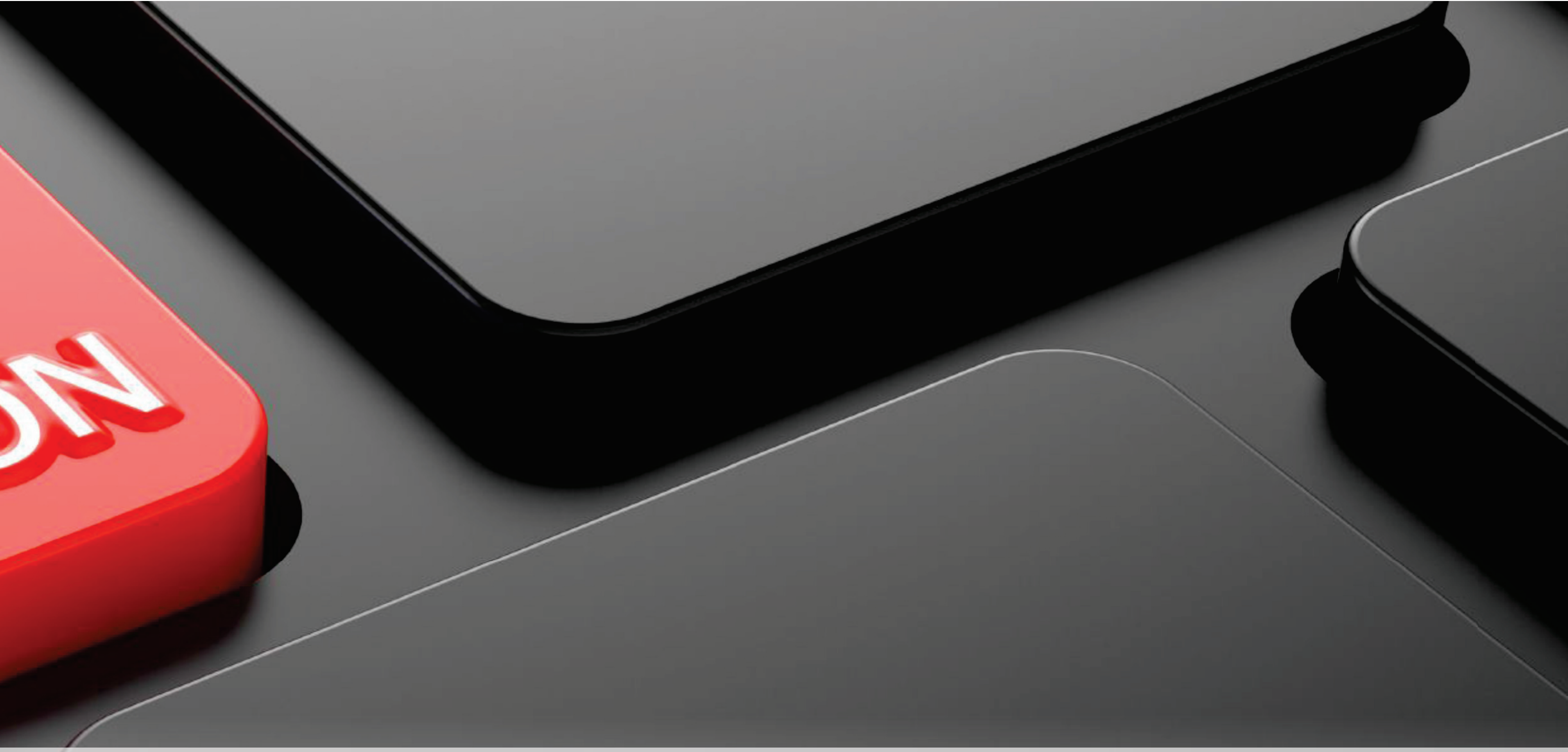
BYOK makes the best of the cloud provider's encryption offering, by giving the customer ultimate control over its key. But is the customer happy with the encryption provided?

Bearing in mind that balance between security and efficiency, you might prefer a higher level of encryption than that used by the cloud provider's security system, or you might find the encryption mechanism is adding latency or inconvenience and would rather opt for greater nimbleness at the cost of lighter encryption. In this case you could go a step further and employ your own encryption algorithms or processes. Welcome to the domain of BYOE (Bring Your Own Encryption).

Again, we must balance security against efficiency. Take the example of an enterprise using the cloud for deep mining its sensitive customer data. This requires so much computing power that only a cloud provider can do the job, and that means trusting private data to be processed in a cloud service. This could infringe regulations, unless the data is protected by suitable encryption. But how can the data be processed if the provider cannot read it?

Taking the WW2 example above: if a Japanese wireless operator was asked to edit the Native American message so a shortened version could be sent to HQ for cryptanalysis, any attempt to edit an unknown language would create gobbledygook, because translation is not a "homomorphic mapping".

Homomorphic encryption means that one can perform certain processes on the encrypted data, and the same processes will be performed on the source data without any need to de-crypt the encrypted data. This usually implies arithmetical processes: so the data mining software can do its mining on the encrypted data file while it remains encrypted, and the output data, when decrypted, will be the same output as if the data had been processed without any intervening encryption. It is like operating one of those automatic coffee vendors that grinds the beans, heats the water and adds milk and sugar according to which



button was pressed: you do not know what type of coffee bean is used, whether tap, filtered or spring water or whether the milk is whole cream, skimmed or soya. All you know is that what comes out will be a cappuccino with no sugar. In the data mining example: what comes out might be a neat spread-sheet summary of customers average buying habits based on millions of past transactions, without a single personal transaction detail being visible to the cloud's provider.

The problem with the cloud provider allowing the users to choose their own encryption, is that the provider's security platform has to be able to support the chosen encryption system. As an interim measure, the provider might offer a choice from a range of encryption offerings that have been tested for compatibility with the cloud offering, but that still requires one to trust another's choice of encryption algorithms. A full homomorphic offering might be vital for one operation, but a waste of money and effort for a whole lot of other processes.

THE CALL FOR STANDARDS

So what is needed for BOYE to become a practical solution is a global standard cloud security platform that any encryption offering can be registered for support by that platform. The customer chooses a cloud offering for its services and for its certified "XYZ standard" security platform, then the customer goes shopping for an "XYZ certified" encryption system that matches its particular balance between security and practicality.

Just as in the BYOD revolution, this decision need not be made at an enterprise level, or even by the IT department. BYOE, if sufficiently standardised, could become the responsibility of the department, team or individual user: just as you can bring your own device to the office, you could ultimately take personal responsibility for your own data security.

What if you prefer to use your very own implementation of your own encryption algorithms? All the more reason to want a standard interface! This approach is not so new for those of us who remember the Java J2EE Crypto library – as long as we complied with the published interfaces, anyone could use their own crypto functions. This "the network is the computer" ideology becomes all the more relevant in the cloud age. As the computer industry has learned over the past 40 years, commonly accepted standards and architecture (for example the Von Neumamm model or J2EE Crypto) play a key role in enabling progress. Creating such a standard is just one more aspect to the CloudEthernet Forum's (CEF's) mission to prevent the cloud from fragmenting into incompatible offerings and vendor lock-in by rival providers. BYOE could prove every bit as disruptive as BYOD – unless the industry can ensure that users choose their encryption from a set of globally sanctioned and standardised encryption systems or processes.

If business is to reap the full benefits promised by cloud services, it must have the foundation of such an open cloud environment. □