

Integrity for Compliance... and Security

Who's looking at my data?

To be successful, a business must make money. Increasingly this money is not just cash being transferred between organisations. This valuable information takes many forms, a business's IP, a bank's customer details, a retailer's credit card information. In the real world, we can see that cash is cash; we trust it because we can see it and feel it. Other items that we buy with our cash, we only buy when we are satisfied by the quality, look, feel, taste, etc.

We can restrict access to the things we hold valuable to our organization; we can encrypt our data and ensure all access on the network is to the correct users. We can even pass data across the hostile internet in trusted encrypted tunnels, but there is never any guarantee that the data we receive is the same when it was sent. In short, we could be being "sold a lemon".

For complete security we need something which follows the data. This "data-centric" approach is the only way in which we can truly trust a transaction of any kind performed on a network, by its users. Transactions can range from the simple: logging on, accessing a file, to the more complex: trading shares or buying a product from an online trader.

The network is tangible, we can see parts of it on a daily basis, wires and ports, printers and our own PCs and therefore we can touch our investment in it. This is one reason why such a large industry has grown up around networking and network devices. Another reason is addressing specific business needs with specific appliances.

Data-centric security suffers for being less tangible, but wherever there are security holes, there will be a criminal to exploit them in time. Access controls are taken for granted in most networks these days: I trust that the data I am accessing/creating can only be accessed by me, or those I choose to access it. However, this is often not the case. What about the administrator of the network?

Encryption is often seen as the holy grail for data-security, and whilst vital, it is nowhere near the complete picture. Much like SSL is vital for secure communications, it is rendered useless if the endpoints are not protected. Security is only ever as strong as its weakest link.

Combining access controls and encryption goes another step towards creating a strong defence against an unknown attack, but we are still left guessing about the original state of our data. Many compliance regulations these days specifically require the originator of data to be able to prove that it has not been tampered with, so what are the options?

The most widely understood solution that currently exists is digital signatures. This requires some form of PKI, at the very least a trusted key for each data holder. This gets expensive, and as anyone who has tried to administer a PKI will tell you, it leads to other headaches. What do you do when someone leaves a company? You can revoke certificates, but the revocation is never instant, and fraud only ever happens when there is the opportunity for it to happen.

Also, if data which has been digitally signed is changed, the integrity of all of the signed data is lost. You cannot trust any of the data it applies to and you don't know where the data has been changed. This makes any forensic processing of logs practically impossible.

The C-word

For compliance we need to address someone else's regulations, which have been written as a catch-all. The very mention of the word "Compliance" has many network administrators putting their head in their hands. Regulations such as SOX, J-SOX, HIPAA and PCI DSS, although

originating in the United States and Japan, are now being felt in Europe. PCI DSS applies to all retailers processing credit card details, but is easier to enforce in the United States with the backing of California Senate Bill 1386 which in simple terms says that if a breach of data occurs on a network, the breach must be made public knowledge.

As subsidiaries of American and Japanese companies have to comply with SOX and JSOX, plus other industry specific regulations, so do those that do business with them. The truth of the matter is that compliance is there for a reason: to ensure the security of the customers using our businesses.

In November 2007 a committee will sit in the European parliament in Brussels to discuss a new disclosure law, following the same lines as SB 1386. Suddenly these regulations will have a new set of teeth, the backing in law and the ability to apply large fines for allowing a breach to take place unnoticed.

Also in November this year, MiFID (Markets in Financial Instruments Directive) regulations will replace the current ISD to create a wider scope, tighter legislation and new pressure for finance houses to comply. The Directive calls for "more extensive transaction reporting requirements". It is not just retaining transaction logs for audit. It is also being able to prove that the data maintains its integrity from beginning to end, and whilst in long-term storage.

But compliance does not always mean security. Businesses can achieve all the requirements of a standard or directive and still be open to attack. Different industries obviously need different requirements for compliance, but what about different companies within the same industry?

Where security is a general business issue, compliance comes as a written standard which everyone must comply with. This can be seen as unfair or unattainable, but the rules are there for a reason. Written, measurable goals can be set for everyone to comply with. They are then audited on their compliance. This usually boils down to meeting technological goals, and if these are all set too high, no-one can reach them. Set them too low and a standard achieves nothing.

How do I protect my IP?

A more granular approach to data integrity is needed, in line with the data encryption and access controls that accompany it. Data encryption can now be done at high speeds, 150Mb/s +, something which digital signatures will never achieve for integrity, and these speeds need to be matched, if not exceeded.

The granularity needs to be as controllable and definable as the network access, down to individual users and the change of bits/bytes of information. When the integrity of data is in question, we need to ensure that more information is not lost, complete transactions can be reconstructed and the source of breaches discovered before they become financial losses.

It has long been known amongst the security community that data-centric security is as important as user, perimeter and network security. Once this becomes clearer to businesses it will need to be properly addressed before we are truly safe from information loss.

This article has been written by Rob Newby, Director of Product Management at Kinamik Data Integrity.

Kinamik will be showcasing its solution at booth C19.

www.kinamik.com

Copyrights Kinamik Data Integrity S.L - 2007