

# The CIA triad: Have you thought about Integrity?

A Whitepaper by Kinamik



© Kinamik Data Integrity, 2007

## Contents

Introduction.....	3
Availability .....	4
Confidentiality .....	5
Integrity.....	10
Conclusions.....	13

## Introduction

It seems a long time since we had to deliver memos by hand, share ideas on paper or contact people on the other side of the world solely via the telephone. That e-mail and the Internet, particularly the World Wide Web, have completely revolutionized the way we live, work and do business is not in dispute. But with the rapid change in communication methods, so there is a rapid change in security threats, and the measures with which to address them have so far been slow to catch up.

In days gone by, an internal memo containing private information would be handed to a trusted party, a secretary or administrator, who would deliver the memo to its endpoint, sealed in an envelope in cases of high confidentiality.

Ideas were shared in meetings, in closed rooms, all visitors known to each other or introduced via a trusted third party. As a result, the information disseminated in these meetings was held as a joint piece of work, the inherent value of the whole shared amongst the individuals involved and only available again through further collaboration.

If input from non-local parties was required, a telephone call was needed to gather information, for further integration with the project or meeting. Of course this went for our personal lives as well as our work lives. To arrange a meeting, a party or just to pass a message on, we needed to pick up a phone or write a letter.

## Availability

Take up of the internet was not as rapid as popularly imagined, although now it seems impossible to imagine a world without it. Use of email and the internet in the early 90s was limited to a few businesses, government and universities. The tools to make this simple did not exist until the late nineties, when the real explosion of internet based businesses occurred.

The 'Internet bubble', or 'dot com boom' was responsible for making many new millionaires across the globe, people became rich from simple ideas which used this new, free and easy method of information exchange.

The demand for availability of information quickly outstretched the networks' capabilities for carrying the traffic. A common problem for businesses in the early days of the internet, which continues today, was providing sufficient bandwidth for customers to access their e-commerce portals, web pages and mail servers.

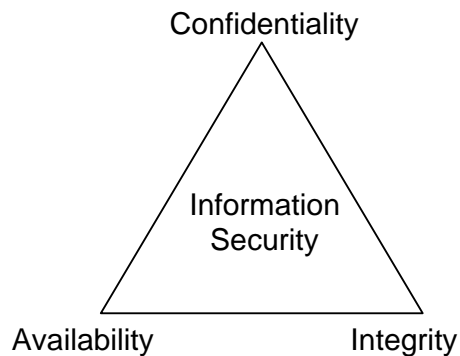
Interestingly, and maybe counter-intuitively, the first problem that information security has to address is just this: How to make the information available, not how to stop it being accessed.

In 1984, a small group of engineers took existing UNIX based servers and turned them into dedicated devices, which until then had run as services on host machines, which communicated with each other by telephone line connections. The company, based in San Francisco, named these devices for the services that they were solely dedicated to providing, and switches and routers were born. At the time, the fledgling Cisco could never have dreamed that they would be providing the switching infrastructure to most of the globe a decade later.

## Confidentiality

Of course, when information is made highly available, it brings its own inherent risks. By its very definition, the more available I make my documents, the more chance there is that they will be seen.

So here we have a sliding scale, the more available I make my information, the less confidential it becomes. I can't have one without the other suffering, at least to some degree. The CIA triad, pictured below, is a well known concept in Information Security. The closer one moves towards one apex, the further one is removed from the other two.



The idea here is to make the trade off a sensible one, based on the value and sensitivity of the information you are responsible for, and ultimately to end up in the middle of the CIA triad, with the best trade-off of each property for the value of the data you are protecting. There is little point in me encrypting and restricting access to a publicly available document, but what about my company payroll, the CEO's bonus details, or my clients bank details?

There have been many advances in encryption over thousands of years of its invention, from simple substitution ciphers to complex elliptic curves and Diffie Hellman key exchange. The advent of computing has merely made this process faster to implement, and to break. The story of encryption is long and diverse, and not the focus of this document. It is safe to assume for our purposes that at any one time encryption is at a reasonable level which is sufficient to keep information occluded. The reality of course is different, hackers will always be breaking encryption, and new advances will be made to stop them, and so the cycle will continue. But even with the strongest encryption we have to ask, is this enough?

Encryption is widely recognised (if not fully understood) because of the tangible change of information in the encryption process. What is not always appreciated is that without the correct access controls in place, encryption is only a physical control.

### **Physical and Logical controls**

Security is often split into physical and logical controls. Physical controls are usually obvious, man-traps at the entrance to buildings, security guards, high fences, security cameras, etc. The list is long and varied. Logical controls are less obvious, and arguably more important to get right as a result.

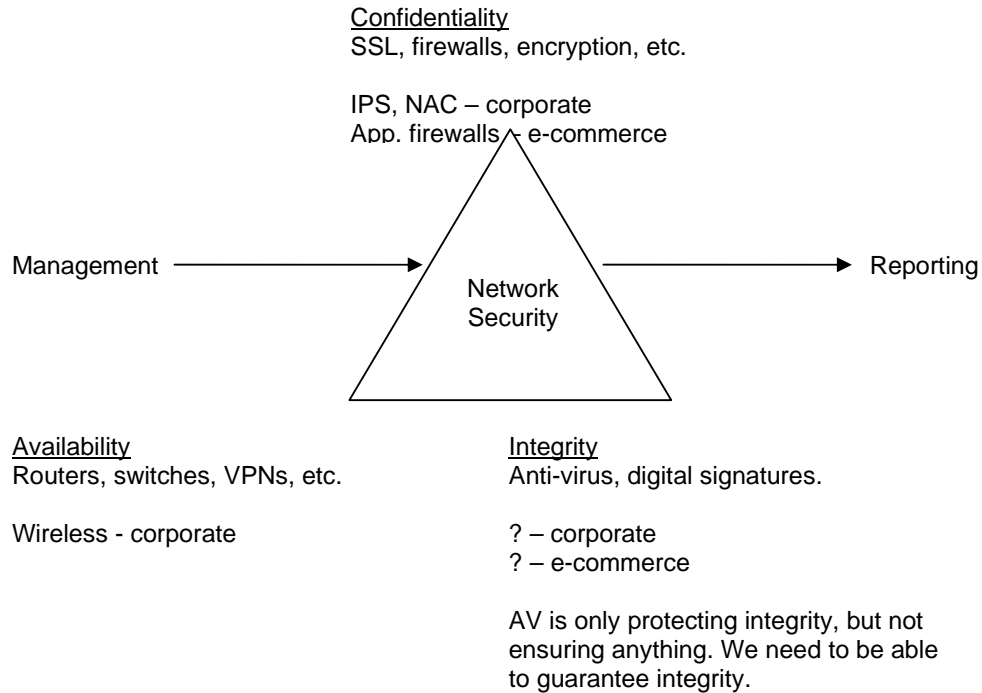
Access controls, authentication, authorisation, data and user classification, all fall under logical controls. They are all controls on the data or systems processing the data which make decisions on who has logical access to that data.

Encryption without access control is merely a physical control, it keeps everyone out and data is rendered unreadable. Encrypted merely prevents anyone benefiting from the theft of encrypted data.

Here we have an example of the availability of information being directly affected by its confidentiality, where before it was the other way around. Applying access controls makes the confidential data more available: people logging in correctly, and having the correct user attributes, can now access the data in clear text.

### **Network Security**

Network security concerns itself with logical controls, and has been the basis of the CIA triad being born. It can be seen quite simply when trying to classify any form of network device or security application, as below. Recently, network security has evolved to the point where to “add value”, firewalls increase availability, switches provide access controls (NAC), etc. This blurs the CIA boundaries a little, but it can still be seen where the original focus of these security applications occurred.

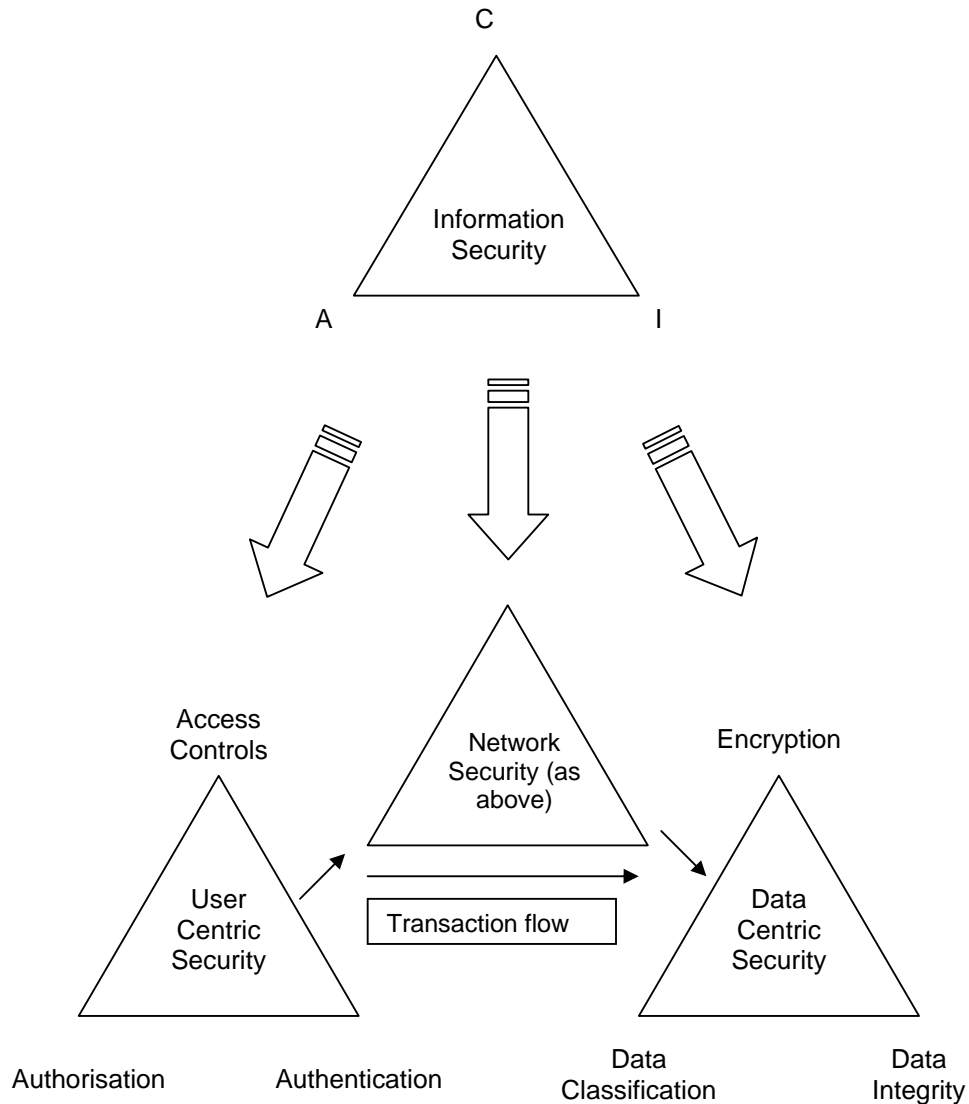


Network security does not address the problem as a whole however. There are many processes, policies and other safeguards that cannot be simplified in this way. Having a router, a firewall and anti-virus may be the basis of a network, and one which might keep you safe in the simplest of terms, in an internet café for example, but the moment valuable information becomes a part of your business – an inevitability rather than a choice – more is needed.

A better way to think of the network is as the mid point, or even the glue, between users and data.

It was recognised at around the same time that network devices were being introduced to address network security, that user security was needed to address authentication, authorisation and access control to corporate and e-commerce networks.

What has only become obvious since the proliferation of user and network security is the need for another layer at the data level.



### **Separation of duties and collaborative changes.**

Just as encryption needs access controls to provide us with security, integrity needs authentication, and availability requires proper authorisation. Although not immediately obvious, we can now see the link between these properties above, and how they can be drawn together to add real value to existing network security.

Even with a separation of duties, a collaborative change can still take place without integrity controls. Since perimeter security has been so effective at keeping hackers out of networks, attacks on data have become internalised. It is now estimated that 80-90% of network breaches happen inside the firewall. This is often by a privileged

user or even a network or security administrator. These are the people you are handing the keys to the trophy cabinet – do you trust them?

To prevent one single administrator from being able to commit these breaches, a security process called ‘separation of duties’ is often applied. A real world example is nuclear armament. The President of the United States of America cannot launch nuclear weapons without them being armed by his Chief of Staff. This is of course an over-simplified example, and perhaps over-dramatised, but you get the picture. One is useless without the other.

However, given enough of a financial incentive, blackmail, political pressure, etc. do you think it possible for one to persuade the other into an unwise, illegal, or even genocidal act? We hope not in this particular case, but there are many other cases like it in network security. Encrypted databases which need security administrators to decrypt and DBAs to retrieve information, sensitive files which need systems administrators to allow access rights, and security administrators to retrieve. Yet this information is still being breached. And of course, being administrators, they can cover their tracks. It is a simple task for an administrator to delete their logs in retrospect, and no-one will be any the wiser.

Unless there is a deterrent or something in place to stop this completely, this cannot be stopped. A one way process, applied to all log data, or even the critical data itself is required, so that any change is detected, recorded and reported on. Without data integrity, this does not exist.

## Integrity

As with many things seen in print, the web is often taken to be a source of information, a vast wealth of knowledge at our fingertips. You've believed everything you've read so far, right? Have you ever stopped to ask yourself why?

The more people who have access to a document or file, the less you can trust it's integrity. Something I release as being the truth, even digitally signed with my own certificate, can be changed, re-signed, and re-released, apparently as my own faithful document.

A recent CCTV case came to court in the UK where neighbours were in a dispute over boundaries of property. A simple dispute rapidly descended into an unresolvable argument, tempers became frayed as neither side was prepared to concede that their land belonged to the other. Eventually one side produced video evidence to a court of the other party apparently shouting abuse and physically assaulting the defendant. The video was used to prove the complainant's unreasonable behaviour and the case went in favour of the defendant.

The facts were somewhat different. The complainant was an elderly man who had lived on his land for over 30 years, the defendant from a family of travelers who had only recently set up a site near to this man's property. They had encroached on it, he had asked them to move back and they had refused. They stayed, erected a pillar outside their newly claimed ground and invited the man to come and have a look. Then they turned the video camera on. As the man approached the house, they taunted him and the defendant came outside and threatened the man with legal action if he touched his new 'property'. The complainant got angry, swore at the man and walked away. The traveler called him back and stood in front of him, blocking his path home. The old man pushed his way past and went back into the house.

Careful editing of the film made the court believe what they saw. The case was thrown out and the complainant now has to live with diminished land, security and trust in the law. This is because the digital information was just taken as correct without any check as to why.

## Digital Signatures

Much is made of the use of PKI and digital signatures for increasing security, and when implemented correctly this can be a great solution for a tough problem. PKI is not a simple integration however. It addresses more than one concern, authentication, integrity and encryption, which can be confusing, and therefore it can become extremely costly. Many PKI projects that start off with the simplest of intentions have to be abandoned when integration problems with existing systems become insurmountable – often because of a confusion of the function of each system.

Inside an organisation, PKI can work well to provide authentication to a wide range of systems, all controlled by a central certificate authority. Out on the internet however, this model breaks down. Unless someone receiving my digital signature already has a copy of my certificate, how are they to know that it is me who signed a document?

If the certificate doesn't match one they have previously accepted, how do they know I haven't updated my certificate or changed my CA? Here, a theoretically good solution suffers from all of the problems of security, confidentiality is compromised by integrity and availability.

So, if I am in an organisation and using my certificates for creating digital signatures, and one of my signatures reveals that a document has been changed between original signing and my receiving it, what next? Do I know where the document was tampered with? No, not unless I have the original, in which case, how do I know that hasn't been altered too. And so the problems continue.

The biggest problem with integrity is it is still rarely considered. People believe that electronically stored data is true, simply because it is electronic data. We are used to seeing the written word, and knowing that it hasn't been altered. The very fact that it is printed means it can't easily be tampered with. Making the transition into the electronic world, people forget that they are dealing with data that can very easily be changed.

A weakness in Amazon.com's programming some years ago meant that during check out a buyer could simply change price information in the address bar of their browser. Instead of buying a book for \$25, it could be yours for 1c. Amazon did not

notice this for some time because it was not widely reported, but when they did, the reaction was to encrypt the cookie which contained this information. No-one has gone to the trouble of decrypting this cookie so that they can change the information and still get the books for 1c. But it is possible. If I got possession of Amazon.com's private key, all the books in their catalogue could be mine for small change, and there would be little comeback for them.

A simple integrity check at either end of the transaction could have saved this issue from ever becoming known, the embarrassment it caused and the resulting (albeit temporary) loss in sales.

### **Security by obscurity**

What Amazon and a thousand other businesses like them are doing is ignoring integrity. As attacks and attackers are forced to become more sophisticated, this isn't just advisable, it is necessary. If it is possible, you can guarantee that one day someone will do it, no matter how unlikely or remote that chance is. The case with Amazon is something highly visible, but like the case with the administrator covering his tracks, much of the integrity threat is invisible after the event.

Apple make a big deal about how secure Mac computers are, but are they really more secure than Microsoft PCs, running on the same hardware, performing the same functions? This is lying with statistics, or security by obscurity. Macs are attacked less often, because they are less prevalent across the planet. Windows and Linux systems are everywhere, Windows because it was the first commercial operating system, Linux because it is free. So when someone wants to start a general attack across the internet, they craft an attack for Linux or Windows systems.

They will maybe get a return of 1% of systems having a vulnerability against their attack, but 1% of 500 million is far more than 1% of 500,000.

If you are not ensuring the integrity of your information, its not a question of if it will be attacked, but when, and how hard it will hit you financially.

## Conclusions

So we might ask the question, what of network security? Do we still need firewalls, IPS, etc?

In an ideal world, no. Every application and device introduced to our networks would be secure in itself, and network security would be a matter of providing the secure transport methods necessary to facilitate communication between user and data. Indeed the Jericho Forum (security without walls) has been set up to try and achieve this security nirvana. Perhaps in time this will be realised, but at present the state of the environment and the controls is not ready for this.

But, IT isn't just about the Users and the Data. The network houses applications, printers, telephones, new devices appear all the time running on IP, and are not always secure first time around. To address security in full, we need to address each of these points. And we need to address the C, I, and A of each of them. Traditionally system administrators have started with the areas which make the most sense, it is logical to make systems available, and then to make them confidential when problems arise. It has also been logical to then ensure the integrity.

	<b>Availability</b>	<b>Confidentiality</b>	<b>Integrity</b>
<b>User</b>	Authorisation	Role-based Access controls	Authentication
<b>Network</b>	Mandatory Access controls	Firewalls, SSL, IDS, IDP, etc.	Anti Virus, Change Control Management
<b>Data</b>	Discretionary Access Controls	Encryption	<b>Kinamik</b>

User and network security are now state of the art, most networks have the degree of protection they need to remain secure, but only in terms of users and networks. However, in terms of data, they are often lacking.

It can be seen even from this simple table that there are many more answers to network security than there are to user or data security. In fact there are many individual solutions available in many of these areas of network and user security. So far there are few answers to the data security problems, and those that exist address

confidentiality primarily, and often ignore integrity completely because it is so far something which is being kept occluded by the problems of data encryption and network integrity.

Many networks have not classified or encrypted data, relying on user access controls to apply this to some level, and integrity is often overlooked completely because, as demonstrated earlier in this document, electronic data is seen in the same terms as the written word. Security is heading now towards completing transactional safety from user, through the network, to the all important data, where the real value lies.

We are moving towards such good security of users, networks and data, that we are rapidly approaching a level where the only activity left which can cause business information breaches is in the integrity of the data. If you aren't dealing with this now, you soon will be.

**Kinamik** provides integrity to the data, which can be kept with the data or aside from it, depending on the requirement. Keeping integrity with the data ensures that the data can not be changed at any point in a transaction without it being recorded and logged. Keeping integrity information aside from the data allows later verification in case of forensics, policing or other verification needs.

© Kinamik Data Integrity, 2007

For further information about Kinamik Data Integrity, please contact

[info@kinamik.com](mailto:info@kinamik.com) or visit <http://www.kinamik.com>