

/vision

# Information security

>>i've got nothing to hide, but everything to protect

**Information systems play a crucial role in our modern society. Naturally, those systems need to be properly secured. But even more important is the question of what data we store in them and why. Privacy is best protected by having as little information as possible.**

## **Information security as the finishing touch**

More and more companies and public bodies use information systems for their operational management. From supermarkets to hospitals and from banks to the tax department, data about us are stored everywhere; purchasing behaviour, health problems, debts and income.

This is sensitive information that we would like to see secured properly. However, in the world of information systems there is a strange paradox. Although security is an inseparable part of any information system, it is often not incorporated into the design in an integrated manner. Security is only considered at the end. "The house is finished. Now all we need is a lock on the door." This separation between architecture and security has grown up over time. When securing data, we focus on the particular information architecture. But nobody asks why the architecture is the way it is.

## **Privacy is not having information**

Yet for the sake of privacy, it is important to pose the 'why question' at the very start of the project. The core question is: ought we really to be storing that data there? In the ideal case, we would have as little information as possible in order to safeguard privacy. Often, these kinds of questions are not considered in the design of a system. They are left to the implementation side. This results in partial technical solutions with protocols, passwords and physical security measures – all of them retrospective – rather than thinking properly about the concept beforehand.

## **Anonymous road pricing**

Unfortunately we are still seeing more failures than successes, but luckily there are also some good examples where the security and privacy aspects have been considered from the very earliest stages. An example is the Kilometer road pricing scheme, which attracted a great deal of attention, albeit much of it negative. In terms of security and privacy, that was undeserved. The essence of road pricing is recording how many miles a car has driven on a particular type of road.

In-car equipment calculates the total amount owed from the GPS coordinates and the various rates that apply. The computations are carried out in the car – information such as time and location do not leave the vehicle. All that goes to the authorities are a few anonymous details. The same principle applies in other systems too: privacy risks are most easily and best solved on the user side. In this way, the system builder ensures that sensitive information does not become available in the first place.

## **Function creep**

From a technical perspective, it can be attractive to gather as much information as possible and then combine it with as many functions as possible. Because you never know what you might need in the future. Minimalism is often lost on technical types. Their enthusiasm for technology instead makes them want more options and functions. Unfortunately, that also has risks associated with it, as we are now seeing with telephone and internet exchanges.

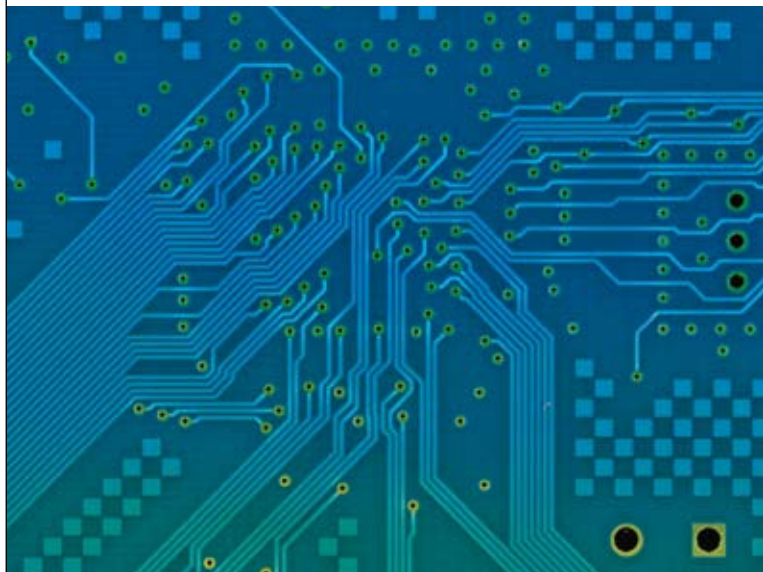


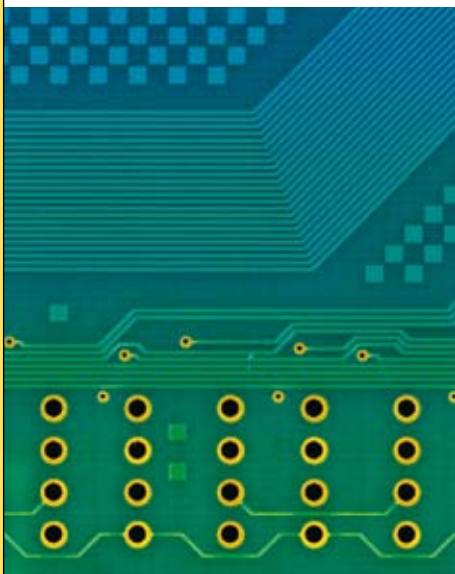
In the past, designers of new digital telecom exchanges built in storage functionality. This was useful for analysing the quality of the systems and networks. Data was kept for six weeks and then removed. Storage was not anonymised, because it was only meant for in-house technical analysis. However, the authorities thought the information stored would be useful for detection purposes: “We can use it to locate and track down criminals.” This is how function creep happens: built-in functions are later used or abused for other ends.



## >>which information to store?

The Netherlands now top the world rankings for phone tapping. Moreover, European legislation requires telecom providers to store all data for all users for 6 months. It is fair to ask whether this legal provision would have been introduced had the technical possibilities not been available. But thanks to the extensive functionality of modern telephone exchanges, this infringement of our privacy is now possible.





### **What is information security?**

In short, if the information is there, there is a strong temptation to use it. So a sensible designer ensures that a system requires as little information as possible. And of course that information needs to be properly secured in terms of availability, integrity and confidentiality. It is all about the total system that the information has to pass through: both the storage and transport of data.

### **Availability**

The road pricing scheme would have involved every car making a permanent record of its route. That meant that the GPS signal had to be available everywhere and at all times. The in-car boxes would also have had to be operational at all times. Communication with the back office was less critical. If the connection is lost, the box stores its data so that it can try it again later. Solving these issues around availability requires keeping a good overview of the situation. How do all the subsystems work together? What happens if one system fails? How does the system restore itself? That is system engineering.

### **Integrity**

Integrity is about the accuracy of data. Are the figures I am reading out correct, are they up-to-date, complete, not manipulated and from the stated source? Important questions for any information system, and certainly for systems that provide support for important decisions. Aircraft and ships need to be able to have complete faith in measurement data. Saving measurements in a “data log” allows us to demonstrate manipulation if there has been any and make a judgement on integrity. This allows the user to see – and prove – what has happened. In this case, data storage serves to provide proof, but it also enables us to analyse what went wrong if there are problems. An aircraft black box, yields indispensable information. In its operation, this type of system resembles financial systems. A bank wants to be able to trace every transaction from payee to recipient. Banking systems are by definition not built with a view to privacy. On the contrary, their security works by following and analysing payments. What is a customer paying for with his or her credit card, how much are they paying and what kinds of shops or companies are they paying the money to? If there is anything unusual, the bank spots it at once. This is how banks combat fraud. They are unlikely to abuse their data – a bank depends on its customers’ trust.

## **>>open and complete communication with user**

### **Confidentiality**

Confidentiality means only making information accessible to authorised persons and systems. So above all, confidentiality is about organisation. Who has access to sensitive information and how do we prevent unauthorised individuals from gaining access to it?

### **Security technology**

A wide range of cryptographic techniques exists to protect the integrity and confidentiality of signals or communication. These techniques encrypt the information, so that no one can access it en route. The recipient has a key to unlock the information. He can also see if anyone has been tampering with the data on the way. Digital keys can come in the form of a Public Key Infrastructure (PKI) certificate, this is a worldwide technology that provides people and machines with digital passports (PKI certificates) and their own keys. PKI certificates are issued by specialist firms like VeriSign. They are the trusted third party in this process of encryption, a kind of ‘key master’ of the internet. It should be stressed that a digital passport does not offer absolute security; just like an ordinary passport, it can be forged.

**Residual risks**

However good your security is, there will always be residual risks. There is no such thing as a system that is 100% safe. So the residual risks must be dealt with at the organisational level as soon as they are encountered. For example, when residual risks occur, who is responsible and is the organisation capable of deciding on action and communication? This means that alongside technology, plans also need to be made in terms of prepared scenarios and processes to deploy additional technology

**Communication**

The hacking of public transport chip cards has received a lot of attention in the Dutch and English media. Perhaps this is because journalists do not know exactly what is going on. However, it does mean that the general public is getting a distorted picture of new technology. This problem also affected the Netherlands road pricing scheme. In technical terms, the road pricing scheme was well constructed, but there were problems in communication with the public. Citizens were being confronted with new and unfamiliar, and above all compulsory, technology. Unfamiliarity breeds suspicion and we find technology scary. Particularly if we think our privacy is at stake.

On the other hand, we constantly phone and surf the web without giving a second thought to privacy. But as soon as the government makes something compulsory, we get edgy. Privacy and information security are sensitive issues, which means that communication by government and companies needs to be accurate and persuasive precisely in those areas. And the timing has to be right: choose your moment to communicate, deliver a consistent story and have clear answers ready to all questions. And be honest about the residual risks. "In view of the state of the technology and the organisation, we can now do this – but no more than this."

**Trust and reputation**

You can destroy a good project with poor communication. Inadequate communication damaged confidence in the road pricing scheme. The communication that there was came too late and was reactive, and it was in response to negative questions. If you lose the public's trust, you will not win it back with a brilliant technical solution. Trust is a product of communication, not just with citizens but also with companies and among companies, in other words with all stakeholders.

