On the Practical Impossibility of Embedded ICT Security

When someone talks about ICT Security our mind goes immediately to firewall or cryptography, if talking with ICT personnel, or to anti-virus, if talking to normal ICT final users. But it in principle it should not be like this. Actually by talking about ICT Security we should just be led to consider how well our ICT system is behaving, which accidents happened or have been prevented, or which security features are present or missing. Why do we always think about assessing or buying a new security device and not only about the intrinsic security of our ICT products?
Indeed today we are used to consider ICT Security as an add-on to ICT products and solutions. When we buy a ICT product we usually have to evaluate security as a separate issue, with a separate budget and with separate personnel to manage it. It would be very nice indeed if we would not have to worry about security and spend money because of it. But as of today, this looks like an utopian dream.

Insecure ICT

Obviously the need for add-on ICT Security products is due to the fact that ICT products are insecure. The lack of security of current software and in some cases also hardware ICT products goes back to the origin of ICT and its fast-paced development in the last 20 years. For example, we all know how the Internet protocols have been designed in the '60 and we all know that these protocols have not been written for what they are used today. So what do we do? Of course we use them and try to patch them up adding some extra security feature which hopefully will help in fixing the problems.

We are where we are also due to the need to release new products within the time-line fixed by the management and trying at the same time to get out the maximum number of features at a lower price in less time. Obviously in this situation security features are the first to be cut out.

But more than looking at the past, let us try to consider the current situation and what could happen in the next future. As we said, we all know that ICT products are insecure, and that they are like that both because they adopt standards, protocols etc. that have not been designed with security in mind, and also because they are inherently insecure due to bugs and mistakes both in design and implementation.

The Dual Market

It should be obvious that in the situation where security has not been considered enough in the development of ICT products, someone thought about creating ICT Security products which would provide those missing features. At first sight this seems a very good idea, but actually in the long run it is not. Indeed the situation today is that we have two markets which rely on each other to prosper.

From the ICT industry point of view this is most convenient. Those who develop and manufacture ICT products do not need to care too much about security and have mostly features, time-to-market and prices in mind. They rely on someone else to fix the security issues and make the products usable. So they depend on the existence of the ICT Security market to be able to sell their products.

On the other side, those who produce security products depend on the the weaknesses of ICT products to offer solutions which fix these problems. If ICT products would not have bugs, weaknesses and missing security features, their market will almost disappear: just think about the anti-virus market and what it would mean for the ICT Security industry if viruses would not be there in the next release of software. So the ICT Security industry relies on the fact that most products on the market are very weak from the point of view of security.

Who is loosing in this kind of game is the final user. He gets a product that is, to say the least, weak from the point of view of security, in some cases it is also missing security features and, unfortunately too often, has security bugs. To be able to use it, the final user is forced to buy some other product which supposedly fixes the problems of the first. Actually, you can imagine this chain to continue, that is that he will need a third product to fix the problems of the second and so on. In any case the customer is in a loose-loose situation, he has to buy two products instead of one and, even more worrying, he knows that the first has problems, even big problems, and that the second is only a palliative, just a way to run around the problems without really eliminating them.

Add to this the remarkable feature of the ICT market for which producers are not responsible of their products, and the loosing situation of the customer is even worse. He buys something which has problems, to fix them, or better cover them up, he has to buy another product from someone else which offers some protection from the weaknesses of the first product. Besides having to buy, manage and maintain two products instead of one, if something anyway happens neither the first nor the second producer will obviously be responsible for what happened. Indeed the user bought the first product knowing it had problems and tried to fix them buying a second different product. Definitively he is in a no-win situation. Actually, all of us are in a no-win situation!

ICT Security is getting harder

But the current situation of the ICT and ICT Security markets has not been imposed on us by bad market practices, but it is almost an unavoidable result of what has happened and the intrinsic problems of ICT. But why it is so hard to get ICT Security right?

Security problems in ICT can be divided in two overall classes:

1. problems, bugs or mistakes in the design or implementation of ICT products
2. incorrect usage of ICT products by humans.

These two classes obviously do overlap and are not at all distinct, still they are useful to let us understand the kind of problems we are facing. The first class contains mostly problems of technical nature within ICT. The second class includes problems which have mostly to do with how we humans use this new technology.

This second class is often overlooked, even if recently is getting more attention due to the phenomenon of *phishing*. Indeed we should always remember that humans and computers adopt different logics, and it is not at all easy to design an interface which would allow us humans to interact with computers in a way that does not lead us in error or confusion.

Indeed most ICT users do not have clear ideas of what can be the consequences of some usages of the technology, and ICT itself today is of little help to make these consequences clear to the user or limited in their effects. We can just make a simple example. Let us consider the use of biometrics as an authentication method. At first sight it looks like a very good idea, since it looks like as if nobody would be able to impersonate me if the authentication method used is my fingerprint. But what about a serious criminal who will not hesitate to cut off my finger so to be able to have access to the ICT system? Or, on the other side, what about the possibility that my biometric credentials are stolen or leaked from the system and that someone else could use them? We can always change a username and password, but we cannot change our fingerprint, or at least we cannot do it so easily and without pain.

The crucial point of this example is that to most users, us included, most often it is not clear what could be the consequences of the usage of ICT. So we could make an incorrect usage which can lead to security problems for the user, which can go from having the PC hard-drive deleted, to a serious loss of money from the home banking or the stealing of the digital identity.

The human interface is not an easy problem, actually it is known to be a very hard problem and we can just try on one side to improve the ICT interfaces and on the other to educate the users and to make them understand better what actually is a computer.

Just this class of problems makes it necessary to have security as an independent product or service. Indeed when we consider ICT Security we should not only consider the first class of problems we mentioned, but also this second. And when humans enter into the equation, there is never a solution which is valid for everyone. Actually even in controlled and limited environments it is difficult to find a security solution which fits everybody. Let us again consider biometrics to illustrate this point.

The identification of users made by biometrics is never exact. Biometrics always give us the probability that the sample just measured matches what has been previously memorized. If we require very precise matches, like you would do in a military situation, it will often happen that users will not be identified due for example to local conditions: temperature, humidity, human health status etc. So there will be many false negatives, that is users who should have been authenticated but who did not. On the other side, if we require less precise matches, it will happen that users who should have not been authenticated actually were authenticated since they had been mistaken for another user. These are false positives, and it depends only on the situation if they are worse than the false negative, as they could be in a military situation but as they could not be in another commercial application. Of course what happens depends also on who are the users who use the biometric system, how physically homogeneous is the group, how trained to use it they are and so on.

So adoption of biometrics cannot be embedded into a product but requires local evaluation, user intervention etc. Analogously most security issues related to human interactions with ICT cannot be solved alone by the technology, so they cannot be embedded in the ICT products and they require external solutions.

Getting better security

This means that we need to have a ICT Security market which provides us with solutions to security problems. But the point is if we do also need to have a ICT Security market for products which solve problems of other ICT products. This is the situation today and at first sight it would seem that if ICT producers would do things right we would not need this kind of ICT Security products. Well, actually the situation is more complicated than what it appears at first sight.

First of all, software and hardware products are getting every day more complicated, larger and more complex. Already many years ago it was clear that the ICT industry was, is and will be dealing with probably the most complex product that human has ever imagined and dealt with. So complex that actually humans cannot be really sure of what they do with it: even if computer science in theory is an exact science, in practice it is impossible to write a complex software or design a complex hardware been sure of all possible relations between inputs and outputs, and without making any even little mistake or just a simple misjudgement on all possible outcomes. Large and complex hardware and software products are just intractable by themselves. So they will have bugs, we cannot avoid it.

On the other side, security is hard, it is so hard that we need people trained and specialized exclusively in security. The same people cannot be at the same time software designers, programmers and security experts. But this does not mean that we must have different products since we have different people specialized in different aspects of ICT. Actually a good team would mix all the professions and get the best out of each one of them. It is easy to say, but very difficult to do if the different professions do not really understand each other at the technical level. Typically a feature required by the designer would be already difficult to implement by the programmer, but if you include also the security specialist you'll get an impossibility. So at minimum you have to decide either to forget about the feature or to forget about security.

It will take a long, very long time before ICT will evolve so much so to be able to see a real merging between all these different issues and be able to produce ICT software and hardware with security built-in by default. We are so far off it that we doubt to see this in our lifetime.

Still it doesn't seem right to have ICT products which fix the security problems of other ICT products. Everybody understand this and there is already a clear business request for a solution. Companies do not want to have to deal independently with ICT products and their associated ICT Security products. Companies have business needs which should be fulfilled by ICT solutions. All the intricacies of how this is done are at the end not so important for the goal to be reached. In other words, security should be an issue solved by those who provide the solution and not independently by the company itself.

This is also supported by the slow but continuous movement of the ICT market towards a commodity market where at the end all technological issues are solved within the ICT industry and only the service is offered to the customer.

So if we cannot conceivably expect to have security embedded by default into all ICT products, we can work towards transforming the ICT market in a market of services and product bundles, where the final customer will be offered a solution which includes all the aspects: both the features and the security.

This is not so much different from other markets: as usual a good comparison is with the automotive market. Cars include many security devices, from belts to air-bags, which are designed and produced by specialized companies. But when we buy a car we are not requested to add to it the belts or the air-bags, the car comes with them already installed and tested.

What we can hope and we can expect to happen in the next future, is a transformation of the ICT market in this direction, that is towards a market of ICT solutions which bundle together all relevant technologies and instruments, included all necessary security features, to offer to the final customer, being both a person or a company, just a single *secure* product.

Andrea Pasquinucci
PhD CISA CISSP
http://www.ucci.it/