A proposed model for explaining and educating Information and Computer Security principles

Hendrik Visagè
Department of Computer Science
University of Pretoria
Email: hvisage@envisage.co.za
hvisage@gmail.com

Martin Olivier
Department of Computer Science
University of Pretoria
Email: molivier@cs.up.ac.za
martin@mo.co.za

***Abstract*—Most of the current Information and Computer Security (ICS) literature and research, appears to be following a traditional model of first addressing the technological and technical issues, and assuming that these issues will be augmented by humans. This is evident in the proliferation of security devices and software in our daily lives. Though we still have ICS problems. However, authors like Von Solms come back to the question, though in different degrees, of whether the involvement of humans is sufficiently addressed.**

The problem is that the elements of ICS are not correctly addressed in the right order to make ICS work properly.

This paper presents a model that gives an alternative perspective on the different elements of ICS. This model was developed while the author were doing ICS-related work, and it borrows insights from Maslow's hierarchy of human needs and desires, where there are certain needs that have to be satisfied before the desires can be achieved. Using this idea that the bottom layers have to be satisfied or addressed before the upper layers should be considered, a layered pyramid has been developed as a model to be used in ICS.

It is suggested that this model is a useful tool to help managers, computer professionals and users, get a better perspective on and understanding of ICS-related issues.

I. Introduction

Our world has become a computerized and connected place where the Internet is accessed from various devices while money is withdrawn using a computerized PIN-enabled card utilizing different communication methods. Users are doing all these while they have little understanding of the technology or technological challenges involved in providing them with the services they require. In addition, in consumerists lifestyles, Information and Computer Security (ICS) related breaches are reactively addressed with a product or feature. Even if this does not solve any future problems, it gives the users a false sense of security.

The problem is that there are several complex management and policy models relating to ICS, and the models reviewed to date do not have a proper human focus nor do they place the human and technological issues in the right perspective with regard to each other.

Multilayered security-in-depth, evaluate the different issues and gives some compliance rating for each aspect of the security evaluated. Although this should not be used as a set of check-boxes, the tendency is that for it become a product-installation and feature-enabling exercise. Thus even when management feels safe, they are not.

Despite authors like Schneier[1] or Von Solms [2] alluding to the human aspects of ICS, our initial literature study, show that recent ICS research and development has predominantly focused on the technical elements and then appears to implicitly assume that these elements will be augmented by the users of the systems. Although there is nothing *per se* wrong with developing and researching technical ICS issues, it is part of this paper's aim to show that the human and environmental issues needs to be properly considered for ICS solutions to be successful.

This paper proposes an ICS model that requires a certain threshold of security compliance on the lower layers before the upper layers can be considered to be secure. This threshold idea (borrowed from Maslow's hierarchy of human needs and desires) is different from security-in-depth, which assesses and reports separately on each element. The model does not prescribe the levels or details for each layer, but states that the relationship between the layers should be considered and evaluated in order to provide secure information and computer systems.

Thus the model that we propose, will help people to anticipate ICS problems and put the elements of ICS (broadly: people, environment, computers, networks and science) into their rightful place and in the correct perspective. This proposed model has been successfully used by the authors to informally educate colleagues with regard to their role and their equipment's roles in ICS, and it is suggested that it will be a useful tool in educating personnel and guiding managers in making more effective ICS-related decisions.

II. Background

The HAISA 2010 call for papers[1] commences as follows:

> It is commonly acknowledged that security requirements cannot be addressed by technical means alone, and that a significant aspect of protection comes down to the attitudes, awareness, behaviour and capabilities of the people involved. Indeed, peo-

[1] http://www.haisa.org/default.asp?Page=cfp

ple can potentially represent a key asset in achieving security,

The authors are of the opinion that the technical solutions should relate to human and environmental aspects, especially as the phishing attacks lately experienced are targeting human nature and bypassing various computer security systems. Research into ICS models for management and policies, revealed that O'Brien [3] was of the opinion that human vulnerabilities underlie the different approaches to network security and that this highlighted the need for physical security features as well. He quoted Smith ([3]) as saying that corporate, government and military bodies in America were practising computer security half-heartedly. O'Brien also pointed out that "*human vulnerabilities cannot be solved with technological solutions alone*", and that the insider problem should be addressed with human solutions.

Eloff and Eloff [5] [6] are asking for new paradigms in ICS while Grobler[7] presented a new information security architecture (NISA) which was the first model that the authors found that showed an approach that partially involved personnel. This NISA focuses on the enterprise, butdoes not address the normal computer user who does not work in an enterprise. Though it does capture the necessary details for managing security policies, it is in our opinion too complex to make it a tool for educating the general computer user in ICS.

When studying the programmes for security-related conference programs like iNetSEC 2010, AIMS 2010, 24th IFIP International Information Security Conference and the 11th Joint IFIP TC6 and TC11 Conference on Communications and Multimedia Security, the author could identify just one relating to humans: *Predicting and Preventing Insider Threat in Relational Database Systems*,by Yasseen and Panda in WISTP 2010[2]. These conferences had a predominantly technical focus.

The keynote speeches by Von Solms, titled "Is the Information Security king naked?", and Jones, titled "Why isn't information security working?" at the HAISA 2010 (Human Aspects of Information Security and Assurance) symposium which was co-hosted with the South African Information Security Multi-Conference (SAISMC) ask the questions that the authors would like to address.

The problem that the authors identified in all of this was that ICS is a human versus human conflict. In other words, in ICS our adversaries are not the computers and programs that are used as tools, but the persons behind the tools. Like any battle, this conflict is fought by people who need to understand their weapons and, even more important – their roles in the battle. In ICS, the users are the troops and the weapons are the computing devices, and the users need to understand their roles and their computing devices.

III. History of the model

As Von Solms[8] pointed out humans are the weakest link in ICS, and we therefore need to provide some history to the actual model presented here.

[2]http://wistp.org/program

The model has its roots in the authors' experiences with the over-emphasis of some security solutions presented by cryptography and firewall vendors in the mid to late 1990s. The authors identified the need for a security picture to educate decision-makers and shapers with whom the author came into contact. The problem was that they needed to find the right perspective for the various security needs and products available and not to be overwhelmed with the marketing by vendors and reports from auditors.

During attempts to develop such aperspective, several other ideas – like the onion rings for operating system privileges regarding hardware access – were used unsucessfully. Maslow's hierarchy of needs, in the form of a pyramid, then provided a solution to the issue, namely that the needs with regard to security had to be identified first, followed by the wants, which would build on the foundation provided by the needs.

It is not possible to attach a formal research methodology to this model, as it evolved with experience, observation and discussions while the authors were actually working in the ICS and system/network administration fields. The ordering of the layers in particular came from observing how humans and computers interact between themselves and with each other.

IV. Proposed Model

Figure 1 shows the model that the authors developed, and although it does not include all the detail that ICS researchers might want, its simplicity conveys the message to others who are not yet security conscious and makes it easy for them to remember.

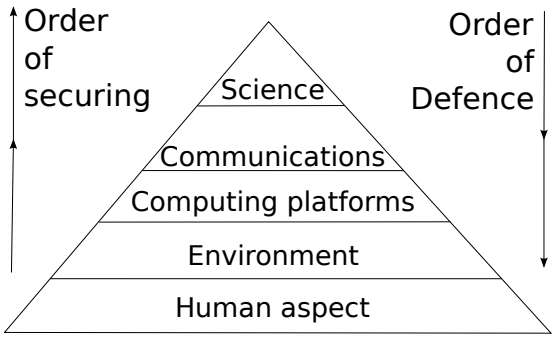

Fig. 1. Model for ICS

The ordering of the layers from the bottom up, follows the order of a user's interaction with computers. Firstly, the human connects with a computing device via the physical environment. The computing device will then connect to other resources using some form of electronic communication. All these interactions are governed by applicable protocols and policies.

As was mentioned in the introduction, the model requires a certain threshold of security compliance on the lower layers before the upper layers can be considered to be secure.

The other aspect of this model, is that if an upper layer fails to prevent an incident, the layers below it should be utilized and be responsible for detecting, preventing or reacting to the

incident. The host operating system therefore should not rely on the security of the network, but should rather handle its own security sufficiently to be able to handle failures from the network security devices. The network security in this regard should augment, and not be, the primary security for the host operating system.

The following subsections will explain the model's different layers from the bottom up.

A. Human aspects

Users of information and computer systems need to be educated on their roles in ICS. They are the people who have to endure the pain when they loose their money, data and privacy in an ICS incident but they do not understand the impact of their actions. Schneier empathetically points out that humans have difficulty in evaluating the risks relating to computers [1].

This is a wide field to consider and because it is people who are addressed at this level it is not as easy to control as a Turing machine. The way to try and control personnel is with policies and procedures, but the politics and culture involved in an organization and society make the matter more complex. However, this layer does not stop at the enterprise or government agencies as we have people at home using computers, cell phones and bank cards.

Anderson [9] identified failures in retail banking related to ATM cards and PINs. Most of the problems identified, involved fraud by people who were not knowledgeable cryptanalysts or knowledgeable computer hackers. They were mostly ordinary people who saw gaps in the systems and exploited those, even though the card and PIN security were not compromised. This is typical of the human aspects of security, as people do not follow the prescribed procedures or inadvertently change them, for various reasons.

ICS involves more than enterprises or the goverment, however, as it extends to the home user whose computer has been infected with a botnet virus through his[3] DSL line and to the celebrity whose cellphone was stolen and contact details were published[10]. It also includes the phishing attack on a normal user's banking details.

From personal experience, the authors have seen the demise of the contacts book, which has been replaced by the contact list on a cell phone. Yet people are now exposed to the risk of losing their cell phones without the contacts having been backed up, as they neither understand nor appreciate the effects of the unsecured contacts list on the cell phone. Experience has shown that these choices are mostly based on convenience[4], and not on security.

However, even when humans – and especially the insiders in a company – are known to be the weakest link in ICS[8], they are also the major defence when things go wrong for any organization, as they (if empowered accordingly) can act swiftly to curtail the effects of a security breach. This is what could be called the underestimated "Human Firewall"!

[3]The use of one gender refers to the opposite gender too

[4]The authors would be interested in a survey in this regard, though

B. Environmental aspects

Going up one layer, we get to the environmental aspects. Here we consider primarily the physical access to the computing devices. We also have to keep in mind concepts like business continuity and other types of data access like print outs. This could become a grey area for drawing a definite line between the environmental and human layers, especially with regard to policy and procedures relating to the environment.

There is a saying "possession is nine tenths of the law", meaning that if you are in physical possession and control of something, you have a better chance of keeping it. The authors' equivalent saying in computer terms is that *control of the console means control of the machine*, which means that to secure any computing device, you need to start with the physical environment to prevent unauthorised physical access. This does not end with servers, but extends to desktops, laptops and smartphones to name just the obvious. This is an important concept in security and also forensics, because the moment you have physical control over a computing device, you are able to load or extract data (or program codes) from the device. This is why you should protect the device from unauthorized physical access.

The environment is controlled by humans, however – be it the policies and procedures implemented by an organization, or the cell phone user securing her cell phone in her vehicle. In other words: without a secured human aspect, the environment can not be deemed to be secure, as no matter what physical access controls are implemented, they are all ultimately controlled by one or more humans.

It should also be acknowledged that if something goes wrong in their environment, it will be humans who react to that incident. This makes the human layer the safety net for incidents and problems occuring in the mostly inanimate environment.

C. Computing platforms

Having considered the human and environmental aspects together with their security dependency, we move up to the computing platforms. At this layer we group the host operating systems, applications and other devices providing data or processing services for an entity or person. It is perhaps too wide or too narrow a definition, but for the sake of simplicity in applying this model, we will abstain from adding more detail[5]. Here we also do not distinguish between applications and the operating system on the device, as from a user's perspective, they are seen as a single entity, together with the hardware.[6]

On this layer, the access controls of the applications and operating systems must work together to prevent unauthorized access under normal working conditions. Thus this would

[5]Noting also that even though we are aware of possible grey areas in our definitions, we could not consider the grey areas in this paper due to lack of time and space

[6]With the advent of Trusted Computing Base (TCB) systems, another grey area is the placement of the hardware in this model. For the sake of simplicity we chose to include it in this layer.

exclude unauthorized physical access, as was mentioned in the environmental layer.

There are many ways to implement and design the application and operating system security and abundant research has been done on this topic. However, we have to point out the obvious, namely that the applications and operating systems have to work together on this layer. In other words it does not help to have a tight operating system setup when the application does not protect its data. The reverse also holds true: that a well-designed application has no security when running on an operating system that allows any logged-in user to read or modify every file.

Getting back to the interdependency of the layers–: we all know that computers are physical entities and we issue commands to computers using physical means like our hands or, lately, speech. Computers themselves need physical hardware and energy to operate. The output from every computing device is observed by humans through physical means, typically our sight or hearing. This links the computing platforms primarily to their physical environment, and secondarily to their operators[7] – who are humans.

This brings us back to the physical control of the console mentioned in the previous layer. Here it should be obvious from forensics that no computing platform has any defence against the physical removal by and access of the datastore through another mechanism – even encryption and tamper-proof methods just delay the attacker with enough time and resources at her disposal. We will state that this proves the link between and dependency of the computing platform on a secure environment and, ultimately, a trusted human layer.

When something goes wrong in this layer, the platform needs to report the failures or incidents, and though it might not be so obvious initially, these incidents are still reported through the environmental layer to the human operators. To explain it in the context of our model: a security incident in the computing layer's application is reported through the physical environment, where a printer or screen provides the information to a human. This supports our case that the computing platform relies on the environmental layer and, ultimately, the human layer as reactive response and safety net for ICS incidents.

D. Communications

We have showed the links between the human, environmental and computing layers of our model and consider the communications layer in this section. ICS usually refers to this as the network security. Though all communications occur through some sort of network, we will broaden this layer to more than just the normally understood LAN, WAN, VPN and Internet traffic to also include communications between devices using other forms like USB, RFID or PIN chip devices. Again there are grey areas in deciding where the actual distinction between devices and communications can be drawn: is a router/switch a device or a network? We could make a case for both, and will leave this for another discussion

We are not going to rehash firewall-based network security other than to state that a secure firewalled network cannot guarantee a secure computing platform. In other words, when an application or host needs to be accessed through a firewall, the firewall can not always provide protection against an insecure application, or against a user who disclosed his login details. In this case the insecure application or host acts like a cyber-insider passing data through the firewall.

Homer and Ou [11] have confirmed this insecurity in the experiments where the vulnerable computers and incompetent users were highlighted as security problems for the network. O'Brien [3] also concluded that humans are the biggest concerns for networked security. To reaffirm this point: When an internal host is compromised through its externally accessible services or human incompetence, the firewall protection is negated for the rest of the internal hosts "protected" by this firewall.

Furthermore, a firewall makes the (implicit) assumption that all the untrusted connectivity can not bypass the firewall. To ensure this, we have to move down a layer to the environment, where the networking infrastructure needs to be physically protected from outsiders making unauthorized connections. Moving another layer down: the humans need to be vigilant in not allowing strangers unrestricted access to internal network infrastructure. This does not stop with LANs, but should be extended to any communication links, whether that be USB or other mechanisms where two or more computing platforms communicate.

On the defensive side, any problematic communication incidents that a computing platform experienced or noticed should be reported as we have mentioned before for the computing layer. Moving a layer down, the environmental aspects should provide indications of unauthorized access, typically through tamper-proof or alarm mechanisms. On the bottom layer, the human element is needed to react to strange communication messages, or the abnormal behaviour of computing devices. Furthermore it is the human who should be alert enough to notice and report environmental changes like spliced cables.

Internal versus external communications: At this point we need to mention that there is a case for the difference between controlled internal and uncontrollable external networks like the Internet. Most of the firewall-based security is about preventing unrestricted access from an uncontrolled network to a controlled network. Our focus and contention in this section, concern the controllable internal network.

Once the communications leave the boundaries of the controllable networks, we have a different set of problems, and that is part of what we will be looking at in section IV-E. When we want or need to add more detail in this model, this would be one of the considerations to split these two into separate layers. However, in order to convey the message and for the sake of simplicity, we will keep this as a single layer at this stage.

[7]Here we define an operator as any type of user, programmer or other person interacting with the computing device

E. Scientific elements

We now conclude the description of this model by considering the top layer. We group various mathematical models, algorithms and protocols together here. Research about management and policies relating to ICS should also be included in this layer.

The appropriate use of cryptography helps us to protect sensitive communications via untrusted media. If used correctly, it will also help to protect stored data in computing platforms. Models used in the right manner would help to enhance the trust that clients place in organization, while protecting the privacy that people expect from service providers.

For the purposes of this paper we will consider the problem relating to sensitive inter-branch communications through VPNs traversing unsecured or uncontrolled networks (refer to IV-D). Here we have already secured the lower layers, in other words we have a controlled network, secured computing platforms and environment and the humans are acting according to the policies. However, at this point we need to transact with another branch, using a third-party communication provider (like an ISP). We need to protect these sensitive communications, but as the bottom layers are not in control of the data while it traverses these untrusted networks, we are now justified in using cryptography to secure the communications. If implemented correctly, cryptography will now be able to provide the added security we can not otherwise obtain from the lower layers. This we do by implementing a VPN (virtual private network) using some form of encrypted channel that will encrypt the traffic from one network and send it to the other side where it will be decrypted and sent to the remote network.

Yet again, however, we have the problem that the networks (specifically the internal communication layer mentioned in section IV-D) on both side need to be secured. If a network packet is be injected on one side, destined for the other side, it would be encrypted and sent, without question, through the encryption channel. This then means that even though the encrypted channel is protecting the data that traverses the untrusted network, it still cannot be trusted, as the network on the other side may have been compromised.

Though the mathematics and foundations of cryptography have been peer reviewed and found to be based on solid foundations, we still have a human element involved in the implementations and human errors have been shown to weaken the cryptographic security. Examples are the infamous SSL random number generation bugs (one being the Debian automated security source code fixing, and another being the Netscape HTTPS bug). So even here we just can not assume that cryptography will make something magically secure, and we have to consider the case when something does go wrong. An example of this is a simple encryption key that has been leaked, and we now have encrypted channels entering from untrusted (though duly authenticated and encrypted) sources. For this we still need protection from the communications layer and computing platforms to detect and report suspicious activity.

There is still much more to write about this layer and its interaction with the other layers. However, for this paper we have limited ourselves to just the one case to show the model's main basis and ideas relating to this layer, instead of delving into all the details and grey areas.

V. Value of the model

It may sound obvious, but the mindset we want the ICS community to consider – on the basis of our model – is that if you cannot sufficiently trust or gauge the security of the layers below, a higher layer cannot be considered to be secure. These layers do not stand alone, they are connected like a chain, and a weak link in one layer has a compromising effect on the rest of the layers.

Another point in favour of this model, is that it is a model that the private users can remember and understand. It does not add complex details that ordinary people do not need to care about...too much. Even so, it is also applicable to the corporate ICS, and its non-ICS -focused personnel and managers can be educated to get a clearer understanding of ICS and the related components.

VI. Future work

The intent of the authors is to formalize this model, as there are still grey areas that need to be addressed or classified. Where should certain aspects like policies and procedures be classified, for example, and do they need to be on a separate layer or not? These will be considered as we compare our model with other models and policies like COBIT and NISA.

Looking at the inaugural conference on Humans in Security [8] programme, we noticed the term "holistic security", and that this conference had several industry and auditing presenters as well as academic representation. This means that a paradigm shift could be occuring in ICS, and that that work should be compared to or integrated with our model.

Lastly, we are still open for advice on naming the layers, especially the top layer as we progressed from "cryptography" to "mathematical aspects" and also considered "formal aspects". We also only touched on a simple case in the top layer, while we acknowledge the fact that it would need more investigation and research. One of the surveys we still want to conduct is to ascertain the current amount of research being conducted on each layer.

VII. Conclusion

In this paper we have proposed a model and shown the interdependency between the security of the upper layers and on that of the lower layers. The model is layered from the bottom upwards with the human aspect on the lowest layer, followed by environment, computing platforms, communications and on the top the scientific models and algorithms. We explained these layers to show the dependency on a secured layer below, while failures on the upper levels should be caught by the lower layers. We acknowledged that there are still

[8] http://www.humansinsecurity.org

unanswered questions and that the top layer needs a more thorough explanation with regard to other aspects involved.

REFERENCES

[1] B. Schneier, *Secrets & lies: digital security in a networked world*. John Wiley & Sons, Inc. New York, NY, USA, 2000.

[2] B. von Solms, "Information security-The third wave," *Computers & Security*, vol. 19, no. 7, pp. 615–620, 2000.

[3] D. O'Brien and A. W. C. C. B. PA, "The Human Dimension of Network Security," 2004.

[4] G. Smith, "An Electronic Pearl Harbor? Not Likely," *Issues in Science and Technology*, vol. 15, no. 1, pp. 68–73, 1998.

[5] J. Eloff and M. Eloff, "Information security management: a new paradigm," in *Proceedings of the 2003 annual research conference of the South African institute of computer scientists and information technologists on Enablement through technology*. South African Institute for Computer Scientists and Information Technologists, 2003, p. 136.

[6] ——, "Information security architecture," *Computer Fraud & Security*, vol. 2005, no. 11, pp. 10–16, 2005.

[7] T. Grobler and B. Louwrens, "New Information Security Architecture," in *ISSA 2005 New Knowledge Today Conference*. Information Security South Africa, 2005.

[8] B. von Solms, "Is the Information Security King Naked?" in *Information Security and Privacy*. Springer, 2009, pp. 1–7.

[9] R. Anderson, "Why cryptosystems fail," in *Proceedings of the 1st ACM Conference on Computer and Communications Security*. ACM, 1993, pp. 215–227.

[10] B. Krebs. (2005, April 15th) Paris Hilton Hack Started With Old-Fashioned Con. Yes. [Online]. Available: http://www.washingtonpost.com/wp-dyn/content/article/2005/05/19/AR2005051900711.html

[11] J. Homer and X. Ou, "SAT-solving approaches to context-aware enterprise network security management," *IEEE Journal on Selected Areas in Communications*, vol. 27, no. 3, p. 315, 2009.