Association for Information Systems
AIS Electronic Library (AISeL)

CONF-IRM 2012 Proceedings

International Conference on Information Resources Management (CONF-IRM)

5-2012

A Discussion on Life Systems Security and the Systems Approach

Andrew M. Colarik
The University of Auckland, acolarik@hotmail.com

Lech J. Janczewski
The University of Auckland, lech@auckland.ac.nz

A Discussion on Life Systems Security and the Systems Approach

Andrew M. Colarik
a.colarik@auckland.ac.nz
The University of Auckland

Lech J. Janczewski
lech@auckland.ac.nz
The University of Auckland

Abstract
The relationship between information technology and information security historically has been quite reactive. New innovations in information technology have often been accompanied by new security threats that create challenges to its reliability and overall integrity. In this paper, a historical perspective that outlines the evolution in the development of the security function is used as a starting base. Changes in the way security issues are viewed and how this view affects the design and development of secure systems are then postulated. It is proposed that these changes should be incorporated into the security functions of any waterfall development model, and especially during the initial and terminating stages.

Keywords
Information, system, security, paradigm, waterfall model, life, survival, border.

1. Introduction
The relationship between information technology and information security historically has been quite reactive. New innovations in information technology have often been accompanied by new security threats that create challenges to its reliability and overall integrity. These in turn have triggered the development of new security countermeasures. As a result, new methodologies were developed to improve the resiliency of information technology against potential abuses, and consider security measures in every stage in the development of information systems. While there are several security life cycle methodologies that exist such as Whitman (2012) or Janczewski (1994), these in the opinion of the authors require modification.

In this paper, we postulate substantial changes in the way that security issues should be considered and how they may be handled across the digital world. We suggest that in principle the systems approach to security while still valid and substantive requires updating to reduce the reactive component to security and instead foster a more holistic and proactive perspective to the security relationship. The authors of this paper believe that the systems approach component of the information security life cycle requires revisions, and in particular at the start and end of the cycle.

The format of this paper is the following: In order to understand the direction of change in the field of information security, we will examine how security issues have been addressed from the dawn of electronic computing up to the beginning of the 21st Century. This is necessary to have a

foundation for an analysis of the changes in the attitude towards handling security issues (Chapter 2). This will be followed by a proposed model that will illustrate the change in perspective required to revise the information security life cycle (Chapter 3). From here we shall define the required changes to the systems approach towards the development of information security subsystems (Chapter 4). The paper terminates with our conclusions (Chapter 5).

2. Information Systems versus Information Security: A need for a new paradigm

A postulate for introducing a new paradigm to the methodology in the development information systems security defences must be based on an evaluation of its development over time. This chapter reviews these defences from the early 1940s. The given dates should not be treated as clear boundaries: they rather indicate periods in particular that defences were predominant.

1940s-1960s

The tools for helping people to perform mathematical operations (i.e. mostly accounting) have been known for a millennia. The first "computers" were purely mechanical devices. During the 19th and early 20th centuries there were numerous efforts to replace some mechanical parts with electrical circuits. Several machines were developed, such as ZUSE (Lee, 1994), or the Mark 1 (Harward Mark, 2011) using electromagnetic switches. Built in 1943 at Bletchley Park in the UK, the Colossus machine is considered the first fully electronic computer (Copeland, 2006), and this was followed in 1946 by ENIAC at the University of Pennsylvania's Moore School of Electrical Engineering (Weik, 1961). Therefore, our analysis of security issues will start with an analysis of the security issues related with these projects, with a special emphasis on the Colossus project.

Both of these machines (i.e. Colossus and ENIAC) were built for military purposes and security issues were setup from the military point of view. There are a lot of publications about these two projects and many were written by people directly involved with these projects such as Ms C. Caughey's (1996) book.

One of the authors of this paper had a rare opportunity to know her personally, and from these readings and conversations one obvious conclusion emerges: the security of these operations was based on an extensive vetting of all project personnel candidates. That set the foundations for an efficient motivational system for those connected with the projects and also facilitated the development of sound physical security. The outcome of this approach could be seen in the case of the Colossus operators at Bletchley Park. Several thousands of young men and women were working there. Despite this number, the Germans never learned about the facility. Even many years after the II World War the participants were concerned about security. When writing in late 1990s about her job at Bletchley Park Ms Caughey applied for permission to publish her memoires from UK Government Communications Headquarters. Their (positive) answer is enclosed in the book.

1960s-1970s

In the 1960s and 1970s, the majority of computers were developed in academic institutions or research laboratories. The emphasis was no longer on security of computing but rather on the design and construction of hardware and software. The attitude towards security had turned 180^{o}

degrees. The researchers were happy to publish the results of their work; physical security was governed by limiting disturbances to the researcher works and the computers itself. This attitude was reflected by both computer manufacturers and users. During these times, numerous centralized computer centres were being built. The design of these centres emphasized the owners' pride in using "super-duper" modern computer technology.

Usually, the main computer room was located on the ground floor with a big glass wall allowing people from outside to have a look at the modern technology and its operation "technology rituals". There were altars (i.e. system consoles), priests (i.e. computer operators) dressed in special cassocks (i.e. white overalls and shoes) performing religious duties (i.e. changing disc packs and managing consoles). Examples of such computer centres from the opposite sides of the Globe are represented in Fig 1 and Fig 2. In both photos you may notice big glass walls (now well covered) allowing a glimpse inside the computer rooms.

During the early 1970s the importance of the computer installations grew. The machines started playing a decisive role in the organizations' management processes. The public learned about it and realized that damaging the computer centre could damage the functioning of an organization. Many physical attacks against computer facilities happened around the world.

In 1969 students rebelled at the University of McGill in Montreal by destroying the library of their computer centre. In those days, the data and programs were stored on punched cards and subject to the physical security threats. The students simply obtained them and threw them to the winds. Whole blocks of the streets around the campus were littered with punched cards. Threats to do the same at the University of Toronto forced the Toronto University President to quickly accommodate the students' requests (Janczewski, 2011).

In 1982, Neil Roberts, a 22 year old anarchist punk rocker, detonated a bomb he was carrying at the doors of the police computer centre in Wanganui, New Zealand (Janczewski & Colarik, 2005). The damages were restricted to the reception area. Despite his attempt, the operation centre was undamaged and uninterrupted as a direct result of the designers' security.

Fig 1: Former Computer Centre of ZETO-ZOWAR, Warsaw, Poland (Photo: L. Janczewski)

Fig 2: Computer Centre of the University of Auckland, Auckland, New Zealand (Photo: L. Janczewski)

These types of attacks forced the architects to conceal computer installations well inside a building's structures and keep them isolated from potential physical threats.
Another major component to this era's security issues was the software that ran on these systems. The main security concern there was placed on unauthorized access and copying of computer software. Preventing that was often poorly addressed. In the early 1969s the Eastern Europe Communist Block decided to setup their family of computers known as RIAD. The operating systems run on these machines were illegally obtained IBM 360 and Digital PDP series software (Judy and Clough, 1989).

1970s-1990s

The transfer of information between computers or remote terminals and computers started long time before the development of the Internet. Connections were based in those days (late 1960s and early 1970s) on dedicated telecommunication lines (Bernatowicz, 1978). These systems were mostly used for a national government's and military purposes or financial transactions between major banks. USA's ARPA Net (Leiner, 2011) is a primary example of a military installation. During the second half of the 1970s, systems such as the Computing Centre of the Polish Ministry of Machine Industry were receiving data from around 50 terminals spread over the whole country.
During this time the banking sector began using the electronic transfer of data on a wider scale. In 1973, the Society for Worldwide Interbank Financial Telecommunications (SWIFT) was born. From a centre in Brussels, a handful of people with an ambitious idea were supported by 239 banks in 15 countries. SWIFT created a shared worldwide data processing and communications infrastructure through a series of communication links and a common language for international

financial transactions. Since then the SWIFT network has grown tremendously. For example on the 25th of January in 2008 alone, it exchanged 16,550,075 messages (SWIFT, 2011).
Such growth was noticed by individuals seeking to illegally profit from it. The phenomenon of hacking was born. Initially, hacking activities were concentrated on two primary domains: the introduction of unauthorized code to batch processing and obtaining information about banking secret codes. Banking secret codes were used as a sort of encrypted hash function added to the transmitted banking transaction. One of the first publications about attacks on banking systems was written by Bill Landreth (1986) in 1986 .
Unauthorized code technique attack popular these days were so called "salami attacks". Name comes from salami sausage served in thin slices. Salami attack is a series of many minor actions, often performed by clandestine means, that together result in a larger action that would be difficult or illegal to perform at once. An example of salami attack, also known as penny shaving, is the fraudulent practice of stealing money repeatedly in extremely small fractional amounts usually by taking advantage of the rounding that occurs to the nearest cent or other monetary unit in computerized financial transactions. It would be done by always rounding down and the putting the rounded fractions of a cent into another account. The idea is to make the change small enough that any single transaction will go undetected. Thomas Whiteside's (1978) book, Computer Capers: Tales of Electronic Thievery, Embezzlement & Fraud, documents how a programmer at a mail-order company diverted money from rounded-down sales commissions into a phony account for three years before he was caught.
In consideration of the above, we may say that until the early 1980s, the interest in the field of information security was concentrated on three primary aspects:

- Physical security of the data centres (dominating aspect),
- Personnel security (human relation security problems),
- Reliability of software and hardware

Computer security was emerging with a focus on these three aspects and was studied separately in a reactive manner. The emphasis was on how to best protect a given system against these recognized threats. To illustrate this fact one of the authors of this paper recalls an IBM sponsored security conference, which was held near Bruxelles, Belgium, in late 1970s. At the conference, practically only the first of the two above bullet points were discussed.
Initially, the development of the Internet and the first of its applications did not change much of the above situation. The prevalent means of exchanging data was through so called "discussion lists". Nevertheless, even the early Internet allowed the transmission of software and that formed a support structure for spreading viruses. The notion of computer viruses was well known before that period of time but the first viruses operating "in the wild" appeared in the early 1980s. Some of them become known well around the world: "LSD" and "Brain" viruses. LSD reportedly was created at the University of Victoria, Wellington, New Zealand. The LSD virus made the computer crash and shows a text on the screen: "Want to fly high? Take LSD". The Brain, created in 1986 by the Farooq Alvi Brothers in Lahore, Pakistan, was reportedly developed to deter piracy of the software they had written (Virus: Boot Brain, 2011).
The majority of early viruses were of the boot sector type (i.e. the main body of the virus was hidden in the booth sector of a floppy disc). Hence, the infection happened through the exchange of floppy disks. But getting viruses via the Internet was also possible. Neutralizing viruses was a relatively easy task. It required cleaning the booth sector of a diskette to be plugged into a PC or

through the inspection of the boot sector of the hard drive. Virus scanners were yet to be developed.

1990s-2000s

All the above had started changing rapidly with the mass implementation of home-based Personal Computers (PC). The first successfully mass marketed PC was the Commodore PET introduced in January 1977 (Bagnall, 2006). It was followed by Apple's and IBM's PC machines. What started as a few thousand people having access to computer technology surged to millions in a few short years. Gartner Press Release (2008) says that more than 1 Billion PCs are in use worldwide in 2011 and is heading towards 2 Billion Units by 2014.

This expansion of personal computing power laid the foundations for the user base that would later access the World Wide Web. At the beginning of the Internet, the technical constraints on the exchange of information between individual systems were fairly limited. The typical transmission speed was 2400 bauds and transmitting pictures and videos was almost impossible.

Fred Cohen, who published one of the first academic papers on computer viruses in 1984, started to develop strategies for the development of antivirus software in 1988, and these foundations were incorporated by antivirus software developers (Cohen, 1987). During this same period, a mailing list named VIRUS-L was initiated on the BITNET/EARN network where new viruses and the possibilities of detecting and eliminating them were discussed. Some members of this mailing list such as John McAfee or Eugene Kaspersky later founded software companies that developed and sold commercial antivirus software.

The mass introduction of PC's combined with the emergence of computer viruses gave birth to a change of paradigm in secure computer processing. As a result, the security community started pointing out (Forcht, 1994) that information security needed to be treated in a more systematic way encompassing not only the exploitation of electronic resources but also physical and organizational issues.

With the introduction of The World Wide Web (WWW) by Sir Tim Berners-Lee (1990), the security concept changed again towards information security issues. With a web browser, one can view web pages that may contain text, images, videos, and other multimedia and navigate between them by using hyperlinks. This dramatically increased the technical capabilities of exchanging information between networked machines and as a consequence increased the possibility of the unauthorized access to them.

These technology developments were used effectively by computer hackers who enjoy almost free run through computer installation. The best example of such activities were described by Cliff Stoll (1989) in his famous book Cuckoo's Egg.

That lead to the introduction of many of the tools used by contemporary security specialists to set up digital defences. Various hardware and software packages were developed such as firewalls, intrusion detection, virus scanners, etc. and the like.

2000s -

All of these developments did not significantly change the way information security issues were treated as an add-on to an existing solution and also as a reaction to an existing threat. A system approach to the information security issues started to emerge and the "Secure Systems Development Life Cycle" (SecSDLC) procedures were born (Whitman and Mattord, 2012). Contrary to the previous attitude characterized by treating the security function as an (necessary but) add-on to any data processing activities, SecSDLAC postulates that security issues should

be an indispensable part at every stage of data processing operations (from design to implementation) , irrespective of their format (physical or electronic) encompassing all hardware, software, people and organizational matters.
SecSDLC eliminated the piecemeal approach to establishing information security facilities but clearly have reactive characteristics (i.e. reaction to existing threats). These (and many variants of these) models are currently not working very well in the real world. According to Mikko Hypponen (Grynkiewicz, 2010), F-Secure's R &D director, we are losing the battle with cyber crooks.
At the time of writing this text, the cloud computing approach to information technology is becoming a very hot issue. An interesting aspect of the whole concept of the *cloud* is the fact that the promotion of the technical facilities and existing implementations were introduced without a real evaluation of the security issues related to handing data in *clouds*.
One of the authors of this paper recently attended a nation-wide conference on information technology applications. A lot of presentations and exhibitions were devoted to the cloud computing concepts. However, none of the cloud concept supporting presenters was able to answer a simple question as to how to protect data held overseas from legal abuses introduced by law enforcement agencies of that country. Only recently has a serious discussion on cloud security issues have emerged (Ahmed and Janczewski, 2011).
In summary, the developments in the information security field are presented in the form of a diagram depicted in Fig 3. In the last 50 years, information technology has demonstrated astounding success. Consider that our societies have built a system from nothing that is more complex than anything before which has permanently and drastically changed the way we live. Humanity depends on these system and they should work reliably, being immune to disturbances, whether accidental or intentional. It is the information security discipline that handles these problems but so far has almost purely applied a reactive approach.

3. A Shift in Paradigm

Traditionally, security emerged from a self-protective position from external threats that may bring damage to the wellbeing of a subject or object. Over time, the security domain grew to encompass the protection of groups of various sizes such as the family unit, communities, states and nations as well as organizations that cross personal, professional and national borders. This was illustrated in the previous section. Thus, the domains to be protected encompass a multitude of potential boundaries. These borders are negotiated instruments that assign the rights of subjects to a given set of objects. In essence, the construction of a border is an acknowledgement of this agreement. The security goal of establishing a border in principle has been to mitigate risk through a series of protective barriers and supporting processes that create a more stable and predictable zone from potential threats.
By definition, security threats come from "outside" the individual, group, or organization in question. This is true even when the attacker resides within as he/she/it is acting "outside" the normal security processes of the system. An insider, by definition, has rights to access a given object/subject and can be considered immune with regards to external security measures because they are considered one of "us". It all seems to come down to "us versus them", and if you attack "us" from "outside" or by whatever means from "inside", you become one of "them". It is this condition that a protection mechanism is needed for defending "us" from "them" and more loosely "us" from "us". It is from this aspect that the authors would propose a new way of

considering security. What we propose conceptually is a shift in thinking that considers a protective barrier approach to security while considering the insider threat in a different manner. It is understood that security analysis starts with defining the system's boundary to be protected and then proceeds to an analysis of possible attacks. This is an extension of what many people do on a personal level for the preservation of their own lives, and we suggest that such an approach should be re-examined in a new context. What we are suggesting is a security context that emulates life systems and the basic protection process that flows from its self-preservation.

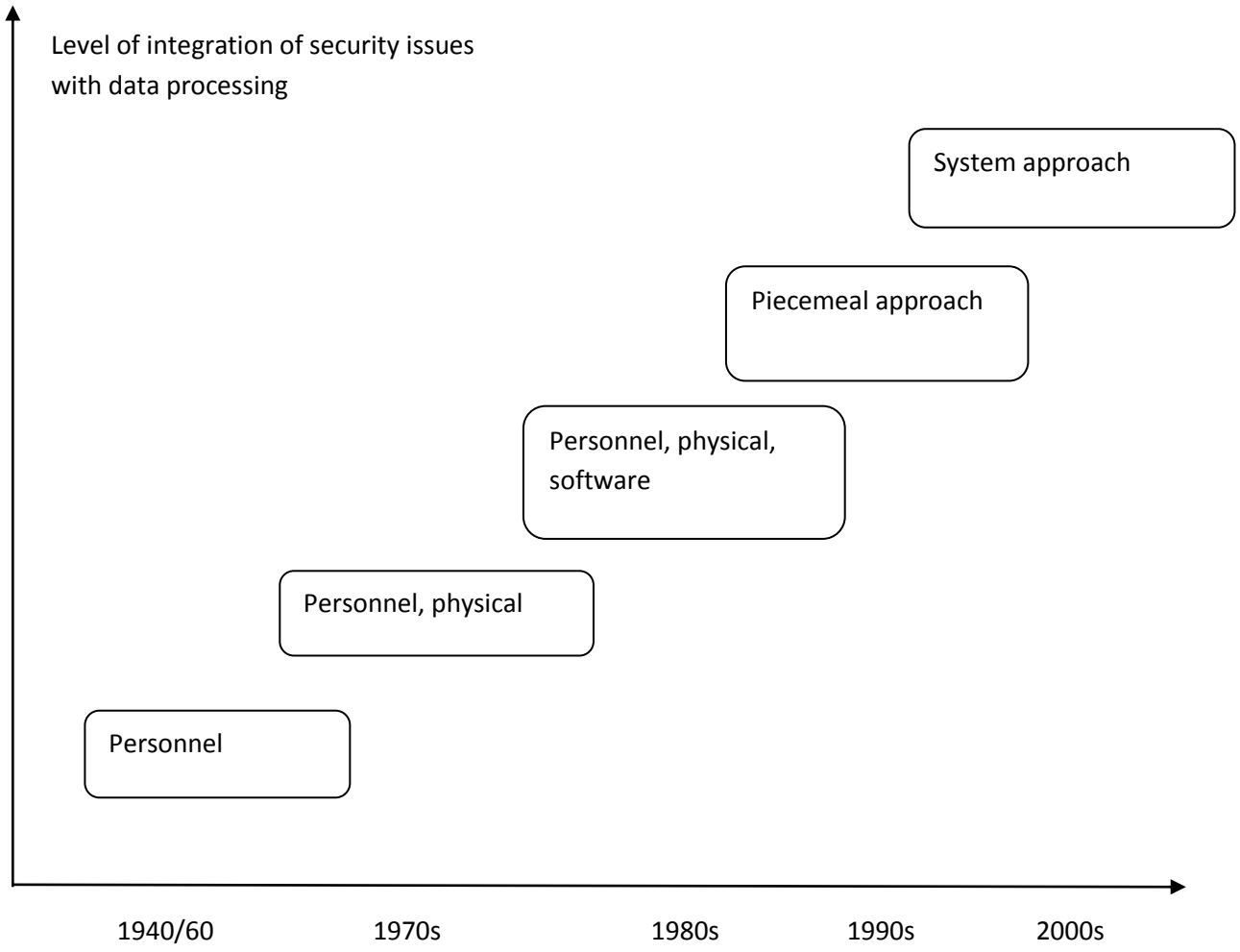

Fig 3: Developments in information security field

Living systems interact with their environment to be of utility and often use this interaction to learn, grow and adapt. In a general sense, a living system can be viewed as having a core structure that interfaces and/or interacts with its environment through its boundary constraint (see figure 4) in the same way that the human body is self-contained by its external shell and uses a boundary to balance personal space and interaction with its environment.

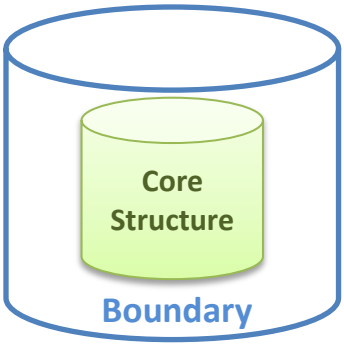

Fig 4: Boundary Constraint

This interface between a living system's core and its environment is often considered an extension of its total system and plays a critical role in its survival regardless of its substantive form. It is through this boundary constraint that a living system's use and value is actualised in a balancing act between interacting with an environment and being interacted with by an environment. It is from this interaction that a system actualises its value and/or is impacted by its environment, and reassesses its strategies, tactics and approaches to sustain itself. It is also a foundation for its self-adaptation and on-going consideration in changing its structural composition to better survive and prosper within its environment.

When the environment changes slowly, a system generally adapts to it over time. When the environment changes faster than it can adapt, three basic choices occur:

- The first of these is to attempt to exclude itself from the impacting environment through means such as isolationism, barriers, and the like.
- The second is an attempt at transplanting itself to a new environment where its structure can be sustained with little or no change.
- The third is to undergo an internal structural change in order to adapt to the impacting environment.

It is our assertion that a system will progress through these three stages as it becomes apparent that the change in environment warrants adjustment. It is the capacity of interaction and adaptation between a system and its environment that also drives this choice and how quickly the choice is made. A simple example of the above would be a person who has established a personal space condition with others in a time of plague. Proximity to the person is negotiated (i.e. aggressively or passively), the threat level assessed (i.e. risk versus return), and one consequence may be being infected by someone allowed within the person border (i.e. insider threat). If the threat of infection is high, a person may isolate themselves in their house, vacate the environment in search of a one with less risk or undergo structural changes by allowing their immune system to be challenged and therefore adapt internally to an external threat.

When we apply this approach to systems development and the application of security, we suggest that the first choice of exclusion (i.e. isolationism, barriers, etc.) resides in the domain of access controls rights as the prevailing paradigm governing such responses. We would offer that the second choice of transplantation (i.e. moving to a new environment) falls within the domain of innovative technology transfer as the prevailing paradigm governing such responses. In the third choice of structural change (i.e. internal adaptation in response to external environment),

we would offer that the domain of reverse engineering is the prevailing paradigm governing such responses. It is in the last two prevailing domains that we feel warrants additional security consideration in existing methodologies and will be elaborated on further in section 4.
What occurs at the micro level can often be aggregated to the macro and our shift in understanding is no different. When living systems decide to collaborate and interact on a collective level for mutual benefit, the individual systems are brought into closer association with other individual systems to form a larger system with its own collective boundary constraint (see figure 5).

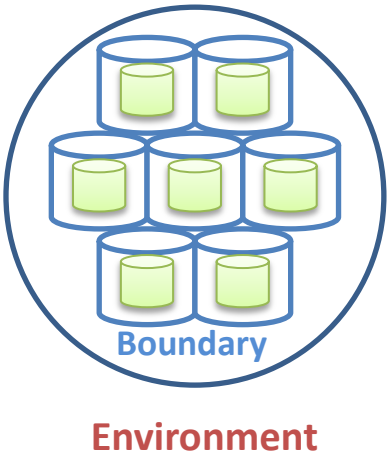

Fig 5: Collective Boundary Constraint

As a result of this collective association, the boundaries between individual systems, the collective internal environment and the external environment need to be considered in enacting security in all of its fundamental processes (i.e. interactions, collaborations, agency, etc.). In this consideration, we propose a model that suggests that the individual systems of the collective association negotiate and maintain their own boundaries between their individual interactions with their environments (i.e. internal and external) while accepting additional influences from the collective on negotiating those boundaries.
What the authors assert from this discussion is that security takes place in the boundary between a live system and its environment as a result of balancing interaction and self-preservation. We reaffirm that the goal of security is to optimize the balancing mechanism(s) between a system and its environment to ensure sustainability and survivability. For purposes of this paper, it is the form of this security; its structure and fundamental processes; its intent and consequences that we believe shape the longevity of a system. This concept applies whether it be an individual or a collective organisation, and as such leads us to reassess the methodologies in place today. In summary, the pivotal changes to the existing methodology of setting up the security functions of a system are related to the need to well define the boundaries of the protected system and modify these boundaries in the function of a changing environment.

4. Changes to the methodology of security system development

In the previous sections, we offered the reactive advancement of security with respects to information systems development; presented an alternative view point by which system borders are negotiated and applied become a border constraint; and how these may become the

foundation for re-examining how security is assimilated into the System Development Life Cycle (SDLC) in a more proactive, holistic manner. The authors re-affirm that the foundations for a methodology in developing security capabilities should be based on a systems approach like those of the classical waterfall SDLC depicted in Fig 6. There are many variations on the waterfall model in use today but their essence is often captured in the phases of investigation, analysis, logical design, physical design, implementation, and maintenance, and these form the basis for the systems approach to development.

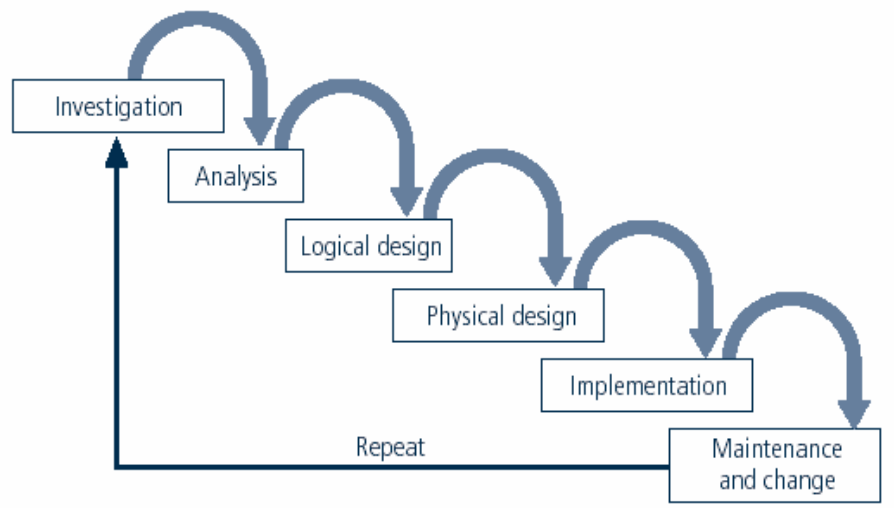

Fig 6: System Development Life Cycle (Whitman and Mattord, 2012).

The Security SDLS (SecSDLC) is a variant of SDLC that identifies specific threats and creates controls to counter them within this model. The main problem we would argue is that such an approach is static and needs to be more dynamic to address the wider range of system threats encountered throughout interaction activities. In addition, the waterfall model does not clarify the establishment of the system's boundaries, and as presented in previous sections this could become very problematic. Also, the rights of access are related to the system's data with no discussion on the rights to change the characteristics of an object (i.e. the controller of the object). These combined make the necessity to reconsider the existing methodology in developing secure systems.

In the first stage of the SecSDLC model, investigation typically considers the identification process, outcomes, goals, and constraints of the project; begins with the Enterprise Information Security Policy (EISP); and organizational feasibility analysis is performed. In the second stage, analysis typically considers studying documents from the investigation phase; an analysis of existing security policies or programs, along with documented current threats and associated controls is performed; an analysis of relevant legal issues that could impact the design of the security solution is conducted; and the risk management task begins. It is within these two stages that we propose several other additional functions.

What we believe is needed is a definition of the agents authorized to access these components (i.e. who is allowed to do what). Within a typical application, there are various functions to be performed by typical users (i.e. persons or subjects) authorized to perform non-change activities in order to utilize the system. These come with rights that may be limited use rights to system resources, operator usage (i.e. allowed to modify the system) or owner standing (i.e. full rights).

These agents and their rights to components need to be determined during the very initial stages of system development. Current models determine such categories as users, owners, operators, etc. but their rights are usually not well defined and are related mostly to process data rather than the capabilities of a system.

Another needed change is in defining the methods for communicating with the systems components. When designers develop a system, they usually do not concern themselves with other access methods such as access remotely through an application. Instead, they focus on the primary communication channels needed for components to interoperate and/or to provide users with access to applications. An example of this is web access rights channels which exist predominantly for gaining access to applications. Users must first be vetted through the authentication process before gaining access to a remote terminal or application. This is generally a development aspect that is performed late in the process.

Building on the agents and communication channels' definitions, we suggest the need to create a definition of potential methods of access to secure components. These need to be clearly specified in both the investigation and analysis stages as well as in the post analysis of potential covert channels (Amoroso, 1994) that must be expanded on after the system is developed (i.e. maintenance stage). From our own development practice, we have noticed that covert channel analysis is performed only on rare occasions. Understanding and identifying these methods is critical to preventing future attacks when a system must negotiate boundaries with other systems or operate in new environments.

The last area we offer for consideration addresses the inherent resistance to system changes and expansion. The system maintenance stage is usually one of the most neglected parts of the Secure SDLC. We believe that at this final stage would be the place to practically implement the outlined above procedures without compromising the security of the system. For the most part, every system is in a constant state of change (i.e. patches, revisions, updates, versions, etc.). New users and functions are regularly added or changed and the foundational technologies the system operates on are also changing. To some extent, these changes take place during the maintenance stage of the life cycle. However, in our opinion, the solution to the resistance to modifying a system needs to be addressed very early in its system design and implementation. In other words, our assertion is that through the comprehensive inclusion of the above added definitions a system will greatly improve in its capacity to go from being relatively static to being a much more dynamic structure throughout its life cycle. We offer that these proposals will in fact greatly extend the total life of most systems.

In summary, there is a need to comprehensively identify those agents authorized to access system components, define the communication channels to and between system components, and define the methods of access between the two. All of the above would allow designers to determine the best, most comprehensive manner in setting up the system boundaries of the components needing to be secured in a more holistic manner by following the concepts outlined in the section 3. This is especially true in the case that a system must make a transition from an independent operation to one that is more collective (i.e. as illustrated from Fig 4 to Fig 5). We believe that adding these components into the system design process would eliminate a significant weakness of the existing methodology.

5. Conclusions

Presented in this paper, we have shown how the attitude towards the security function has changed over many decades. The progression in change initially began with personnel and evolved to include the physical and software aspects in a piecemeal approach. The systems approach of the SDLC came to dominate as the level of integration required between data processing and security issues reached critical mass. As such, the approach through variants of the waterfall model became the methodology of choice in identifying the security issues needing to be addressed in the system development process. We re-affirm the value of this approach and the need for it to remain a progressive instrument in securing systems.

Throughout this paper, we have asserted that the existing methodologies are for the most part static in nature and do not address the core issues of a changing and highly interactive environment (i.e. changeable users and their characteristics, communication methods, and technologies). The authors of this paper advocate the conversion of the existing methodologies from those that are reactive to ones that are proactive in their approach to security in order to address these core weaknesses. More specifically, we believe a proactive approach would be better expressed by addressing the issues mentioned above in every stage of the SecSDLC, and especially in the preliminary and maintenance stages. We believe that a critical component in the methodology of a system's analysis should be a rigorous definition and examination of its border constraints (i.e. borders defined within the Trusted Computing Base concept).

Future works within this research will be concentrated on the development of usable techniques addressing the issues mentioned above and will include further refinements in securing a system's ICT aspects. In particular, the issue of handling changes to the environment in which the system must operate will be focused upon. The authors of this paper believe this aspect will become a dominant emerging issue at all levels of the development process.

References:

Ahmed, R., and Janczewski, L., (2011). *Governance Life Cycle Framework for Managing Security in Public Cloud: From User Perspective*, 2011 IEEE International Conference on Cloud Computing (CLOUD), pp.372-379, 4-9 July

Amoroso, E., (1994), *Fundamentals of Computer Security Technology*, Prentice Hall,1994

Bagnall, B., (2006), *On The Edge - The Spectacular Rise and Fall of Commodore*, Variant Press, Winnipeg

Bernatowicz, K. (1978), *It is not enough to have IBM* (in Polish: "Nie wystarczy miec IBMa), Informatyka, No 12

Berners-Lee, T., (1990), *Information Management: A Proposal*, CERN, May

Caughey, C., (1996), *World Wanderer*, Keasang Enterprises, Auckland

Cohen, F., (1987), *Computer Viruses: Theory and Experiments*, Computers and Security, No 6

Copeland, B.J., (2006), *Colossus, The Secrets of Bletchley Park's Codebreaking Computers*, Oxford University Press

Forcht, K., (1994), Computer Security Management, Boyd and Fraser

Gartner Press Releases, (2008), 23 June, http://www.gartner.com/it/page.jsp?id=703807, reviewed in September 2011

Grynkiewicz, T., (2010), *Where cybermafia is marching in, servers are burning* (in Polish: Gdzie wkracza cybermafia, tam płoną serwery", Gazeta Wyborcza, 8 Nov

Harvard Mark I (2011), (http://en.wikipedia.org/wiki/Harvard_Mark_I, reviewed in September 2011

Janczewski, L. (1994), Planning Efficient and Effective Data Security System, *Proceedings of the 1994 International Conference of the Information Resources Management Association*, San Antonio, TX, USA, 6p

Janczewski, L. and Colarik, A., (2005) *Managerial Guide for Handling Cyber-Terrorism and Information Warfare*, Idea Group Inc

Janczewski, L. (2011) personal information

Judy, R., and Clough, R., (1989), *Soviet Computers in the 1980s: A Review of the Hardware*, Advance in Computers, Vol. 29, Academic Press

Lee, J. A. N. (1994), *Konrad Zuse, Virginia Tech/Norfolk State University*, September, reviewed in August 12011, (http://ei.cs.vt.edu/~history/Zuse.html)

Landreth, B., (1985), *Out of the Inner Circle*, Microsoft

Leiner, b. et all, (2011*), A Brief History of the Internet*, Internet Society, http://www.isoc.org/internet/history/brief.shtml, reviewed in August 2011

Stoll, C, (1989), *Cuckoo's Egg*, Pocket Books, New York

SWIFT History, (2011), http://www.swift.com/about_swift/company_information/swift_history, reviewed in September 2011

Whiteside, T., (1978), *Computer Capers: Tales of Electronic Thievery, Embezzlement & Fraud* , Thomas Y. Crowell Company (NY)

Whitman, E.E. and Mattord, H, (2012), *Principles of Information Security*, Course Technology, Boston

Weik, M.,H., (1961), *The ENIAC Story, Ordnance Ballistic Research Laboratories*, Aberdeen Proving Ground, http://ftp.arl.mil/~mike/comphist/eniac-story.html, reviewed in September 2011

Virus: Boot/Brain, (2011), http://www.f-secure.com/v-descs/brain.shtml, reviewed in September 2011.