Discussion Topic: What is the Old Security Paradigm?

Steven J. Greenwald*

Independent Consultant
2521 NE 135^{th} Street
North Miami, Florida 33181-3581
USA

Abstract

If we are to have new computer security paradigms, then we need to have at least one clearly defined old security paradigm. The reasons for having an old paradigm are several. First, we can't know that any "new" paradigms that we create are truly new without something to compare against. Second, rigor requires that we define our terms clearly, and without a clearly defined old paradigm, any work toward rigor is going to be more difficult. Third, old paradigms are still at work, and sometimes present in "new" paradigm systems. Fourth, old paradigms can serve as useful pedagogical tools. Fifth, the preservation of knowledge and history is a worthwhile goal. Sixth, the mistakes made in the past can serve as a useful guide.

This paper is an attempt to ferret out the old computer security paradigm that existed (and still exists) prior to the current age. There is a startling lack of documentation regarding much of the early information processing security systems, and often information is fragmentary. This is literally "an attempt at a start" at defining the old computer security paradigm.

There seems to be a tacit status quo idea that we can have a new computer security paradigm without having a clearly defined old one. This paper constructively challenges that notion by introducing a new (informal) model of the old paradigm, termed "PIA" (Privacy, Integrity, and Availability). The thesis is that PIA is the old paradigm.

This topic created much valuable discussion at the workshop. Rather than completely rewrite the paper presented at the workshop to produce a better composite work based on the discussion, after much deliberation I decided to leave the workshop presentation paper completely untouched, with the exceptions of this paragraph, adding an epilog that incorporates some of the outstanding discussion that occurred at the workshop, and adding some bibliographical entries in that epilog. It is my hope that this will convey a peek at some of the flavor and spirit of the New Security Paradigms Workshop process to those readers not fortunate enough to attend, and to also serve as a valuable resource in itself thanks to the contributions of the workshop particpants and the roads they opened for me.

*Email: sjg6@gate.net, URL: http://www.gate.net/ sjg6

0 Introduction

In its common form, a paradigm is an example or a model. The usefulness of a paradigm is mainly for the purpose of comparison. For the purposes of this paper, a paradigm is essentially nothing more nor less than a model that is used as a basis of comparison, or used as a universe of discourse, depending upon the context.

A question that one of the NSPW referees brought up was "How old is 'old'?" Perhaps this can be better stated as, "What exactly is meant by 'old' in this paper?" I believe this question will be answered later, as an historical time line is presented. In addition, it is not my intention to imply that there is only one old computer security paradigm. There may be several (I believe this likely). However, the focus of this paper is on what is perhaps the predominant "old" paradigm. In addition, "old" does not rule out the fact that this paradigm is still in use in many places, or incorporated

into "new" paradigms. I wish to emphasize that this is a first attempt at starting a dialogue on what "everyone" seems to know intuitively, but no one has actually formalized (but there will be no formal methods in this paper; perhaps this is a task best left for the future, after a consensus has been reached in this area).

Why is formalization of the old paradigm(s) important? Well, if we are to have new computer security paradigms, then it behooves us to have clearly defined old computer security paradigms. The reasons are several.

1. How can we know that any "new" paradigm that we invent is truly new, unless we have older paradigms to compare against?
2. If we wish to be rigorous, we must have our terms clearly defined (to paraphrase old Socrates) and without a clearly defined old paradigm, our work toward rigor is going to be that much more difficult.
3. Old paradigms are still at work in existing systems and also as parts of new paradigm systems (as part or in whole of security policies).
4. Old paradigms can serve as useful pedagogical tools.
5. The preservation of knowledge and history is a worthwhile goal in and of itself requiring no further justification.
6. The mistakes (and successes) of the past can serve as useful guides for our work.

It is mainly the first through third reasons that prompted the writing of this paper. During the course of investigating "new" computer security paradigms, the author discovered that there doesn't seem to be a consensual, well-defined old paradigm. This begs the question: "Is there an old computer security paradigm?"[1] I believe the answer is "yes" but as we will see, it must be a qualified "yes." It must be qualified because of the context in which the old paradigm existed (and in many cases still exists). For the sake of simplicity (and without, I believe, significant loss of generality), I propose that there were only three contexts for the old paradigm: government, military, and commercial. Other contexts, such as scientific, social, and educational, fall (or can be forced) into one of these three.

Contrast this with the environment at the time of the writing of this paper: there is an "educational" paradigm that is clearly not the old educational paradigm. The old educational paradigm is concerned with the training of students to function within one of the existing contexts (*e.g.,* learning to become computer programmers), and the new one is concerned with the security aspects of using computers as an educational tool (*e.g.,* using the computer as an aide to studying history). The terms get muddied during their travels through the often polluted river of time.

A brief definition of these three contexts seems to be in order.

Government. Obviously the military is part of the government (and in some countries the other way around). However, for the purposes of this paper, I remove the military and intelligence community from the government context. In some countries the commercial sector is part of the government, but again, for the purposes of this paper I remove the commercial sector from the government context. This leaves organizational, financial/accounting, and law-enforcement tasks as the primary role of government.

Military. The military's function is almost always to protect and defend its country. To be sure, there are other roles for the military, depending on the country, but this definition will suffice for the purposes of this paper. In addition, I move the intelligence community into the military context, even though technically this should be in the government context, because there is a certain congruence between the military and the intelligence community. It is certainly easier to categorize certain items later on if this is done.

Commercial. For the purposes of this paper, commerce would be anything not included in the above two contexts. This would include such things as banking, industry, art, science, and education. Even though there might not be a profit motive for some of these things, their actions are always influenced in a major way by commercial forces.

I further propose that the type of security (and here we can define "security" as simply freedom from risk or danger, or as safety) was constrained into a paradigm I term *PIA*, derived from the initials of the well-known principles of *Privacy*[2], *Integrity*, and *Availability*. Any other concerns either are beyond the scope of this paper, or can be placed in one of these three principles.

Therefore, it is the thesis of this paper that PIA is the prime candidate for the old paradigm. Historically, there are (at least) three phases in the information processing era to investigate.

[1] This also begs the question, "Why are researchers and practitioners inventing new security paradigms?" However, the answer to this question is beyond the scope of this paper.

[2] The vast majority of the current literature refers to "privacy" as "confidentiality," however that would lead to an unfortunately confusing acronym.

1 Background: The APCIP Security Paradigm

Before computers were invented, information processing was still an extremely important and dynamic field. Even though computers did not exist, there was still an incredible need in the government, military and industry to manage information. Arguably, we could go all the way back to the Sumerians to make our case, but it is within the scope of this paper only to examine the period immediately before the invention of the computer: from the late 1880's to World War II. I refer to this period as the *Age of Pre-Computer Information Processing* or APCIP. APCIP is characterized as using pre-computer, human-intensive, machine-augmented, information processing systems.

The United States of America (U.S.A.) provides the quintessential example of APCIP. After the U.S.A.'s Civil War, industrialization of the U.S.A. proceeded at an unprecedented pace. Arguably, by the late 1880's, the U.S.A. had become the dominant industrial and technological power in the world. The famous problems with tabulating the 1880 census are a logical starting point for APCIP [3, 34, 20]. As is well known, Herman Hollerith adapted punch cards to solve this task for the 1890 census. Industrial age information processing was born (while there were earlier attempts to be sure, the scale of the 1890 census seems to be one of those defining moments in history). Soon, the Hollerith system was in widespread use [16], and not long after, in 1911 (a particularly auspicious year), the Computing-Tabulating-Recording Company (CTR), the precursor to IBM, was born [2]. Before long, all different sorts of calculating equipment was in use, made by a diverse number of companies such as Felt & Tarrant Manufacturing Company, Remington Rand, National Cash Register, Burroughs Adding Machine, IBM, Underwood Elliott Fisher, *etcetera*. Soon, scientific uses were envisioned, and devices such as Bush's Differential Analyzer [11] were created. Eventually World War II coincided with the end of this era due to the invention of the computer (since the credit for this is in some dispute between the nations of Germany, Great Britain, and the U.S.A. and is not germane to this paper, I refrain from offering an opinion as to the identity of the actual inventors of the computer). However, we may definitely conclude this era with the declassification of Project PX resulting in the unveiling of ENIAC to the public on February 14, 1946 [36].

During APCIP, history records little in the way of information processing security *per se*. It should be noted that sometimes the term "security" is used synonymously with the term "controls," especially in commercial environments. Undoubtedly security was a major factor for some installations, since it is well known that the Nazi's used information processing equipment, especially elaborate punch card systems, to tabulate the status of their victims. It is also well-known that the U.S. Navy's Ballistic Research Laboratory and the U.S. Army were concerned with the security (*i.e.*, integrity) of the ballistic tables they produced [35]. Little security documentation seems to be available from this time, however.

We can conjecture that since the equipment was used to emulate the tasks that humans had previously laboriously performed, that the security paradigm in effect was the same as that for purely manual systems. This seems reasonable. Certainly there were concerns for the actual value of the expensive and complicated equipment itself, but that is a side issue (*e.g.*, physical access, plans for disaster recovery, preventive maintenance; all these things are beyond the scope of this paper).

For the military during this period, security seems to have been particular lax in some countries, and particularly stringent in others. For example, in the United States during most of this era, proof of identity was not even required to join the military. The opposite was not true in most of Europe, especially after the Great War, when passports and visas seemed to have been widely instituted among nations (what I refer to as the "Paper's Please! Paradigm" or PPP, but this is also beyond the scope of this paper). Of course, with the tensions leading up to WWII, military security was tightened up considerably.

Obviously security problems abounded. Anecdotes about potential disasters being averted by vigilant personnel are common, and show the extent of the security problems of this era. For example, inference channels in particular seem to have been particularly common, if we are to trust some anecdotal evidence I have heard. The bottom line, if we are to trust these stories, is that there were no automatic controls, such as those that exist today in some systems, to detect security breeches.

So we can surmise that the only paradigm in use was PIA, with manual controls, and this is probably the strictest security that was ever used during APCIP. Commercially, we can assume that PIA was the strictest paradigm, since it was an emulation of the existing manual practices for proper finance and accounting [12]. As an example of "fitting" something into one or more of the three contexts, the scientific need for security would depend on the ties (if any) to the government, military, and commerce, and perhaps professional considerations (*e.g.*, privacy to maintain precedence for scientific credit).

So how would PIA actually work?

1. **Privacy**. Concerns in this area would be essentially the same for the government, the military, and commercial contexts. Authentication would

be done (if at all) by direct personal knowledge, by primitive identity cards or by physical recognition. For example, a teller at a bank would most likely be recognized personally by facial characteristics. Certainly any existing manual controls would carry over to APCIP. Inference channels would have to be detected manually. Encryption and encoding were used only in those cases where the extreme cost (by today's standards) in time, labor, and machinery could be justified.

2. **Integrity**. The same concerns that apply to Privacy apply here. Things such as auditing would be done in the same way as the existing manual controls (for example, by shuffling paper around). Most likely, the major focus would be on fraud, sabotage, and human errors (verification).

3. **Availability**. Whenever possible, manual controls would be left in place as backups (again, these would mainly fall into the "paper shuffling" category) [12]. Certainly the possibility of a mechanical breakdown or deliberate sabotage would have been a concern. So would natural forces, the availability of materials to continue processing, and the impact of warfare.

Note that procedural failures apply to all three of the above items. In the commercial world standard procedures mostly involved separation of privileges and multiperson rules [12], with the manual system being retained in its entirety. For example, in banking, it would not be allowable for only one person to move the "Boston Ledger" (the main books that the bank kept) from the "cage" (a visually surveilled access-controlled area where day-to-day ledger entries were made that was designed to make covert activity difficult) to the vault. The information processing system was used to reduce the main expense of information processing at that time (manual labor), and to provide flexibility (*e.g.*, more detailed, varied, and more quickly produced reports). Most output from the automated systems would be destroyed when appropriate, whereas source documents from the original manual system would be retained for an indefinite time (effectively, as if forever).

So essentially, the security paradigm of APCIP was just the original manual paradigm, adapted (if at all) to the existence of primitive information processing equipment. It is important to note that a point of confusion regarding research into this era exists in that there is a transitional era around 1930–WWII, where more and more computer-like devices were being devised (both analog and digital) [12].

2 Is There an ACE Paradigm?

We may call the time immediately after the invention of practical, stored-program computers, which coincides with the end of World War II, the Age of Computer Emergence (ACE). ACE is characterized by extremely large, mostly "one of a kind" machines, requiring substantial specialized knowledge to control, and requiring specialized maintenance. Examples of these types of machines would be ENIAC and EDSAC [33]. Standards were mostly nonexistent. While ACE is of interest historically, as far as the scope of this paper it is uninteresting, since the security paradigm was essentially just APCIP, with perhaps more physical security due to the expensive and critical nature of the early computers. Therefore, there probably wasn't an ACE paradigm, or at least one different from the previous "old" paradigm.

3 JASP, First Period

When the state of the art reached the point where computing equipment was being standardized and mass-produced (by "mass-produced" I mean that more than one machine of the same design was made and that the mechanical design was modular so that no manual "fitting" was required to exchange the parts of one machine with another), we reach what Greenwald has termed the "Jurassic Age Security Paradigm" (JASP) [17]. JASP is characterized by large, centralized, and dedicated machines. A hallmark of JASP is the system administrative "priesthood" that took care of the computing environment.

We may arbitrarily set the date for the start of JASP as that of the Korean War (June 1950). By 1950, there were many products available that are best characterized as "computer-like" in that they performed the tasks that computers would later perform, but did not meet the definition of a stored program computer (for example, punch card equipment). When the Korean War broke out, IBM did an assessment of the need for computers in the military [22]. In 1952 the IBM Defense Calculator (later renamed the IBM 701) started production, slightly behind Remington Rand's UNIVAC. The "Jurassic Age" had started.

In addition, militarily, at about the same time, SAGE (Semi-Automatic Ground Environment) became activated (1958 [15], although development of the Whirlwind computer that SAGE was based upon started around 1952 [31]). Some may know this as Project Whirlwind (the name of the actual computer component). With the advent of more advanced computers, and 29 SAGE installations, it quickly became apparent that the critical need for this system was availability.

The systems had to be highly reliable, and any failure of a SAGE computer during actual operations, for any reason, was unacceptable, leading to the solution of the duplexing of computers at each center (not two computers, but duplicating the CPU and memory units in one system). This led to the idea of *fault-tolerant systems*. Unfortunately (for the purposes of scientific inquiry), the U.S.A. was never attacked by hostile Soviet bombers, so we will probably never know if SAGE would really have worked.

Initially, there were few computer installations, but as we all know, that changed rapidly. By around the mid-1960's, most commercial banks began installing computers (it was probably City Bank that installed the first banking computer system, followed almost immediately by Chase Bank; a host of smaller banks followed suit rapidly). In addition, the idea of the *service bureau* evolved, especially as regards ADP, Inc., which serviced the payrolls of an unknown (but undoubtedly huge) number of corporations. Obviously privacy was a main concern while handling such things as payroll. Integrity, of course, was essential to everything. At this point, we may consider this the first half of the "Jurassic Age," and an enumeration of PIA in context at this point is in order.

1. **Privacy**. Concerns in this area began to radically diverge regarding the government, military, and commercial areas.

   (a) Government would be concerned mainly with saving money by using computers to replace such manually intensive tasks as payroll, accounting, and other financial applications. In addition, the area of law-enforcement started making use of computer technology. Obviously, privacy and integrity would be a paramount concern for law-enforcement.

   (b) The military would only be concerned with privacy as it related to intelligence matters (using the military definition of "intelligence" which, I freely admit, is arguably cheating). One of the difficulties with a (somewhat) arbitrary classification divorcing the government from the military is that these areas start to "grey out." Obviously the intelligence community would have an extremely great interest in privacy.

   (c) Commercial sites, such as banks or companies using computers for payroll would have extreme needs for privacy. Banking, in particular, was quite vulnerable to inference attacks if payroll information was divulged. In addition, there were fiduciary aspects regarding keeping customer account information confidential.

   Such things as authentication could now be done by automatic means, if necessary (*e.g.*, passwords). Again, any existing manual controls would almost certainly carry over to JASP. Inference channels would have to be detected manually (to my knowledge, there were no automated tools available at this time to detect inference channels). Encryption could now start to be used more extensively and more inexpensively.

   So at this period, we can see that privacy is starting to become a major issue.

2. **Integrity**. Again, the major focus would be fraud, sabotage, and human errors (verification). However, surprisingly little interest in integrity seems to have been documented. This could be because integrity was assumed to be an issue, or because it was not very well defined.

3. **Availability**. A great divergence now becomes apparent between our three areas.

   (a) Government would be concerned with availability only insofar as it did not become a great inconvenience. The financial aspects of government would most likely be satisfied with delays of up to one day (perhaps more). The needs of the law-enforcement community would probably have the same availabilty requirements.

   (b) The military had critical availability requirements, as previously noted by such systems as SAGE.

   (c) The commercial need for availability varied tremendously. Some sites had manual systems in place, running in parallel, so that large amounts of down time were acceptable. Other systems, such as the SABRE airline reservation system [10], had critical availability needs (SABRE was basically a spinoff from SAGE started by IBM in 1954 for American Airlines, and was in full operation in 1964 as the largest commercial real-time networked system).

The first period of JASP essentially ends around the mid-1960's. After this point, computers proliferated at an even greater pace, and the second half of JASP took place.

4 JASP, Second Period

At some point in the 1960's, the interest in computer security reached enough of a critical mass that we can

say it developed as a separate field. This is the point in time of the start of the second period of JASP. While JASP has never ended in some places, it became possible to take more than a theoretical interest in new security paradigms sometime during the late 1970's with the advent of the semiconductor revolution and microcomputers, so we can arbitrarily end it there.

During this period, the scientific community and the military in particular were extremely concerned with information security and computer security. And it is at this point that we can probably say that our true "old" PIA paradigm was tacitly adopted. The seminal moments in its formation follow. I will not delve very deeply into each individual item, as any serious student of computer security should be familiar with these items.

1. Lampson's 1971 access control matrix model [25] was probably the first true paradigm, in that it was a model (indeed, a formal model) and therefore something that could be compared against. In fact, this is exactly what happened in a host of successor access control works exemplified by the HRU model [19, 18]. From this paper's standpoint, privacy and availability are the focus of this model.

2. The mention, in 1973, of covert channels (we can hardly call the original note a model) developed by Lampson [26] certainly added to this paradigm. Privacy is certainly the only issue regarding covert channels.

3. Denning's 1976 lattice model [13] extended the access control matrix model by adding information flow.

4. Certainly the 1973 through 1976 development and publication of the Bell-LaPadula Model (BLP) [5, 28, 4, 6, 7] was a seminal event in the history of computer security. This attempt at modeling military type security is probably the most cited reference seen in the computer security literature following its publication. Having the framework of military security as perceived by the computer security community at that time, it was incredibly influential, despite flaws that later became apparent [29]. Its focus was (mostly) on privacy.

5. Biba's 1977 integrity model [8] added integrity to the old paradigm.

6. The 1985 publication of the "Orange Book" [14] (the *Department of Defense Trusted Computer System Evaluation Criteria*), along with the rest of the Rainbow Series, was probably the landmark event that crystallized the old paradigm. It is at this point that we have an actual, complete, PIA paradigm that we can point to and "poke with a stick." Ironically, if the thesis of this paper is correct, the Orange Book was already being supplanted by "new" paradigms at the time of its publication (such as the NRL Military Message System [27]).

I would welcome any information on exactly when the "milestones" of adoption happened for the areas of denial of service, and non-repudiation.

5 Through the Modern Age and Beyond

The modern age is characterized by such features as personal computers, widely distributed systems, much more control by the user, widely available communications, a high degree of interactivity between the computer system and the user, and the advent of widespread computer games and consumer electronics in general.

I propose that the widespread use of computer games seems to be a good indicator for when the "modern age" began. Before then, typically only those privileged to have access to a Jurassic Age system could play computer games. However, starting about 1980 microcomputers started to become cheap enough and simple enough to operate so that non-technical consumers could buy them for gaming. The list of innovations in the field since that time would literally fill volumes. It is at this point in time where our "new" security paradigms may have come into their own (and coincidentally, is when computer networks also started maturing, bringing all their attendant security problems). This period can serve as an arbitrary delimiter for when "new" paradigms started to really branch out and come into their own.

With a tacit foundation of PIA as the "old" paradigm, researchers started coming up with new paradigms challenging the older one. I could easily give a lengthy bibliography of these new paradigms, but to save space I will instead direct the interested reader to the proceedings of the New Security Paradigms Workshop. But the important point is that if there is work being done with new paradigms, then there *must* be tacit acceptance of *something* as the old paradigm. What better candidate for the old paradigm than PIA is there?

6 Conclusions

If PIA is the old paradigm, then it is certainly in our interests to defend the fact that it is the old paradigm, to conceptualize it as best we can, and to model it both formally and informally. Without doing this, we cannot say with *any* degree of scientific certainty that we

have, in fact, come up with any new paradigms. Until we reach a consensus as to what, exactly, is the definition of the old computer security paradigm, we cannot answer the "simple" question, *"what is the old security paradigm?"* This is not a good position to be in: if we cannot answer a question as simple as this, then we may be on very shaky foundations when we build our new paradigms. One anonymous NSPW reviewer of this paper had the following comments that I strenuously agree with.

> What is required now is more work in identifying historical examples of standards, experiences, mistakes, technology and lessons learned to add to our understanding and knowledge of the PIA paradigm.

If a paradigm is something to compare against, then we need a rigorous definition of PIA, so that future work in this field will have that basis of comparison, and so that we will be able to argue whether any "new" paradigms are, in fact, truly new. The definition of the old paradigm should be as valid, simple, formal, correct, and useful as possible. Not only will these traits benefit the designers of new paradigms, but they will have a useful pedagogical function. Simply put, a well defined old paradigm can serve as an anchor for our field.

As we have seen, there are a number of other (usually) rigorous works that evolved into the old paradigm, but there is no single definitive source that explicitly tells us, "*this* is the old paradigm." I anticipate a great deal of discussion as to exactly what the old paradigm is, since this paper is just a first step. I hope that this first step will lead us down the path towards defining one of the elements necessary to the identity and usefulness of our field.

7 Epilog

As mentioned in the abstract, I decided, upon much deliberation, to leave this paper untouched after NSPW 1998, with the exceptions of the last paragraph of the abstract, this epilog, and the references contained in this epilog (and of course the acknowledgments). It was a difficult decision. On the one hand, I believe that revising this paper based on the input of the participants of NSPW 1998 would have produced a much better work *in toto*. On the other hand, leaving the presentation paper virtually untouched, while adding this epilog, gives the reader a glimpse into the workings of a typical NSPW discussion, without any loss of material, and allows a bit of the extremely dynamic nature of NSPW to be captured. It also allows attribution for some of the more profound observations of the participants who rightly deserve recognition for their contributions in a more dynamic style.[3] After much deliberation, I decided on the latter course for the reasons given, and I fervently hope that I have succeeded in conveying the truly unique nature of NSPW. If this is successful, it is due to the participants of NSPW 1998, without whom, this section would never exist.

Finally, while I believe attribution is desireable, I very much wish to avoid putting words in people's mouths that they might not have said. In order to keep this record relatively informal (indeed, since a tape recorder was not present, it could be nothing other than informal), I do not directly quote individuals, instead paraphrasing them (and many times adding some of my own comments). Please do not construe any remarks attributed to anyone below as necessarily their actual position on the subject unless you verify it with them.

7.1 A Title With a Difference!

After being introduced, I presented my title slide, which contained the standard obligatory material, and nothing of consequence other than the title. Usually the time that title slides are exposed to the audience is measured in seconds at the most. Imagine my surprise when suddenly a full-blown discussion erupted right at that moment! I believe that I could have thrown away the rest of my slides, and let the discussion commence unconstrained. Of course, I can not verify the following, but I do believe I now hold the world's record for the most discussion produced by a title slide in history. I would estimate that the discussion at this point lasted at least 10 minutes. I was totally unprepared for such an event, and perhaps unwisely quieted down the discussion to present the discussion topic in the way I had prepared.

A few snippets of this beginning part of the discussion that were noteworthy were Cathy Meadows saying that the old paradigm is to look at the system, figure out where the trust belongs, and then devote resources to protecting those areas.

Marshall Abrams nominated as the old paradigm "Evaluation, Plugability, and Layerablity" which was essentially the Rainbow Series paradigm, and which the Joint Security Commission declared invalid in their report to the Secretary of Defense and the Director of Central Intelligence [23]. This paradigm assumed that separately evaluated systems can be composed, and the resultant systems be secure at the level of the weakest system in the resulting composition (which we now know to be a wrong assumption).

Someone mentioned that just because we are using a paradigm in the modern age, it doesn't mean it is not

[3] As opposed to recognizing them in something like a footnote.

obsolete. The old paradigms are still out there, working away. A comment was made that old paradigms can be embedded in new ones. This, to me, is an extremely important point, as it underscores the importance of formalizing the old paradigms. I offer this point as a refutation or caution to some of the participants who felt that NSPW should only be forward-looking and that we should not look back at the old paradigms, and therefore that this discussion was off-topic for the workshop. Well, if it is true that the old paradigms are embedded in some of the newer ones (and I believe this to be true), then it is sometimes possible that we *are* looking forward when we look at history. Given the results of the discussion, I believe this to be a critically important point.

7.2 Order Please!

John McDermott wondered if the contexts as presented in this paper were actually ordered. I replied that I had given the definitions in no paritcular order. John then suggested that there might be a proper order, and it could be "commercial < government < military" where the "<" relation means "appeals to in disputes."

The significance of this in the context of the history of computer security seems retrospectively obvious.

7.3 Privacy Does Not Equal Confidentiality

At one point, the discussion was as to whether, in the context of information security, privacy is the same as confidentiality. I had chosen to use "privacy" as the term for the old paradigm because I didn't want a possibly confusing acronym if I used "confidentiality." In addition, prior to NSPW 1998 I viewed privacy and confidentiality as synonyms. It was obvious that a consensus had emerged that privacy is not the same as confidentiality.

One of the wonderful benefits of NSPW is that it allows the author to return to the drawing board, when necessary, because we publish our proceedings after the conference. So what, exactly, is the difference between these two terms?

It became clear that privacy was something that applied to people, and confidentiality something that could apply to organizations. Without giving lengthy definitions, I believe it boils down to the following. Privacy is the *right* that individuals have to determine which information they wish divulged about their personal lives. Confidentiality is the flip side of this; the *property* that protects against the improper release of information to people or organizations who wish to get that information.

So it is clear that "privacy" is not the correct term and that it should have been "confidentiality."

7.4 A Failure To Communicate

Jim Wallner pointed out a glaring omission in the paper. Namely that I focused on COMPUSEC (computer security) but ignored COMSEC (communications security).

This is a very important point. I believe this omission resulted from a more modern paradigm shift: the merging of COMPUSEC with COMSEC possibly leading to a bias on my part and on the parts of the NSPW referees.

As history has shown us, the two were not always the same. However, in the context of information security, it seems quite proper to include COMSEC.

A very interesting discussion then began about SIGINT (signals intelligence). The discussion went back as far as the U.S. Civil War and focused on telegraphy. It seems that a lot of cloak and dagger stuff went on back then. For example, it was possible to identify the individual telegraph operators by their "fist" (i.e., the characteristics they used when keying morse code). John Michael "Mike" Williams mentioned that some of the other things done during this war included interception of messages, blocking of messages, decryption, and the insertion of deception traffic. It seems this was a very lively area during that period. As an aside, some military historians view the Civil War as the first "modern" war (i.e., in which large scale strategy and tactics were first used). It would seem that this observation might apply to COMSEC as well.

7.5 Brother, Can You Paradigm?

When I noted that SAGE was the impetus for SABRE, the discussion then turned towards some of the commercial systems. Of particular interest were those systems that were responsible for the development of transaction processing and the immense amount of underlying theory and properties that have emerged.

Mike described an interesting fault-tolerant design for 1950's era UNIVAC tube systems. He also mentioned that from the mid-1950's to the present, serial sharing of computer I/O devices was done and this resulted in *periods processing* procedures with two techniques being required for security. First, software was required to *label* High and Low data on punched cards, tape, and I/O devices. Second, software was needed to "scrub" (sanitize) main memory, disk drives, and to force dismounts when required.

Mike and Marv Schaefer had a wealth of information on specific hardware configurations as the multi-tasking/multi-programming/multi-processing/timesharing era started. Mentioned were such things as a pre-1962 project for the NSA named Q7/TSS-SDC, the IBM/UM TSS, the B5000 MCP, the UNIVAC 1107/1108, the UNIVAC III, and the GE 630+, the ICL Atlas, and the 1964 Multics/GE 645 and the 1974(?) SCOMP/Multics MLS ("AIM").

A special mention for influential old systems is in order for the 1966 ARPA contract to SDC to build the Adept-50 (IBM 361-50) designed for multi-level security (MLS) for the military which anticipated the BLP *-property, but not containment or trojan horse defenses.

I don't want to give the impression that Mike, Marv, (and others) rattled these off all at once. These were just some of the systems that I was able to recall during the discussion. No doubt I am missing many others.

There was some comment that in the 1960's, during the period when most commercial banks had installed computer systems, the genesis of the Y2K problem occurred. It was noted that obviously the banks (and insurance companies) had some method for keeping track of customers born before the year 1900.

7.6 Papers Please!

It was noted that I failed to mention many influential reports and papers that were historic and germane to the discussion. This is true enough. However, I can not overstate the difficulty of discovering and obtaining these sources when you are not an old-timer. However, since the original writing of this paper, some of these sources have become much easier to obtain (some were originally classified documents). Here is a list of some influential papers I was able to obtain after NSPW 1998, including some that were mentioned during the discussion. In addition, I found many others that were not mentioned but that most definitely deserve attention (out of the context of this paper). A lot of credit should go to the UC Davis History of Computer Security Project [4], which I found out about after presenting this paper.

- The "Ware Report" [37]. Concerned with the security problems resulting from "multi-access resource-sharing computer systems." (page xi). This is a seminal paper in the history of computer security. Annex A of [37] entitled "Formal System Access Specification" is written in a modified Backus-Naur Form system, and I found it quite impressive, considering the time-frame in which it was written. It is certainly a candidate for an old paradigm and was the subject of much discussion.
- The "Anderson Report" [1] of 1972. This is a detailed planning study for US Air Force computer security requirements, specifically MLS and some communications issues. In it, (page 48) we find mention of formal approaches "to the development of reliable software" that they call "proof of correctness." This involved formal specifications that can be turned into formal logic so that statements about the specifications of programs can be proven. Again, a case can be made that this is an old paradigm, and it was the subject of much discussion. Some felt that it was "the" initial formal model, but after reading the report, I disagree, as the formal aspects seemed highly exploratory in nature.
- *Preliminary Notes on the Design of Secure Military Computer Systems* [32] of 1973 contains some interesting models, and should not be neglected in any survey of early security
- *A Provably Secure Operating System* [30] of 1975 could be one of the first reports where formal methods are the emphasis of design. The authors prove each step of their designs before any implementation is supposed to occur. A methodology for design is introduced, there are security properties that are proven, and implementation considerations are noted, as well as an approach to monitor the security of the resulting system. In addition, there seems to be a wealth of historical information contained in this report.
- Kahn's book, *The Code-Breakers* [24] was recommended as a beginning book for commercial cryptography, and a good overview of how certain events in World War II were the foundations of modern military cryptography. The original 1967 work is now revised and updated in an 1996 edition.

7.7 Miscellaneous Discussion

Many other odds and ends were brought up during the discussion, that aren't easily categorized.

It turns out that the Orange Book was first published in 1983, and reissued with modifications in 1985. In addition, there are many misconceptions regarding the Orange Book, such that it was an all or nothing approach, and that it was thought to solve everything. The authors were aware that there were many levels involved and that there was an area that went beyond A1, to name a few of the unsolved problems, and future directions of which they knew.

Marshall Abrams noted that the history presented in this paper is U.S.-centric, to which I heartily concur.

[4] http://seclab.cs.ucdavis.edu/projects/history

Aside from finding it difficult to get much of the important source material of the U.S., I find it virtually impossible to get anything from outside the U.S. I hope this will change in the future, and certainly do not mean to imply that it was solely the U.S. that led all development in the old paradigms. The NATO conference was mentioned during the discussion as a seminal event in this field, but I have yet to be able to obtain any non-anecdotal information on it.

Hillary Hosmer cited her 1992 NSPW paper [21] which identified the Rainbow Series as the old paradigm. I can't agree that this is the final word on the subject because it is too "military-centric" in my opinion, but I leave this to the interested reader to decide (or perhaps for future debate/research). It is important to note, in the interests of fairness, that nowhere is it written that we can't have more than one old paradigm, so I am willing to give this the benefit of the doubt. Also, Bob Blakley's 1996 NSPW paper [9] is probably relevant in this context, as it is also an attempt to define what the old paradigm is, as the "Information Fortress Model."

Darrell Kienzle mentioned that he would have preferred more detail here on the modern age. Sorry Darrell, but that's just way out of the scope of this paper.

Undoubtedly I am missing much of what went on during the discussion, as it was fast and furious, and our scribes can only write/type so fast (and of course were also often involved in the discussion themselves).

7.8 So Was It Worth It?

Several people felt that NSPW should look towards the future, and not towards the past. I feel that I have addressed those issues in this paper already. But it is noteworthy that those people are "old-timers" in the field (I don't want to name names, lest I get into any more trouble than I'm already in). However, I think it bears emphasizing again that aside from issues of identification and rigor that might not be so terribly important for NSPW, we must acknowledge that there are many self-identified "new paradigm" security systems that have incorporated old paradigms in part or in whole. I believe this fact alone makes the exploration of this area important and worthwhile. Far from looking back, it can be construed as a type of looking forward, as in looking for obstacles in one's path.

However, assuming my critics are correct, then one amazing fact stands out. A lot of the newer people to our field are not aware of some of the important historical events and publications that exist (and I include myself in this statement). There are various reasons for this, including the fact that a lot of the knowledge out there is institutionalized and not very well recorded, and it was not easily available. But the fact is that this is not a good thing, for we are in danger of losing the knowledge that was so painfully gained during the past, at great expense, and by great people.

Acknowledgments

I would like to give a special acknowledgment to Stephen D. Corriss for his invaluable historical information and insights regarding early banking systems. I would also like to acknowledge the valuable input of Laura Corriss, Alfarez Abdul-Rahman, Cristina Serban, Mary Ellen Zurko, and the 1998 NSPW referees and I would like to give special thanks to Craig Raskin for his technical assistance regarding the submission version of this paper.

In addition, I wish to thank everyone in attendance at NSPW 1998 when this discussion topic was presented. There was not one person who did not contribute something of value. I would particularly like to thank Bob Blakley for acting as the "scribe" during the discussion, and without whom much of the material would either have been lost or garbled. Bob, you did a great job! I would also like to give special thanks to Mike Williams, who presented me with a copy of excellent notes that were not food for thought, but a feast for thought. And I would also like to thank Mary Ellen Zurko for her review of NSPW 1998 in CIPHER [38], where she also provided information on this discussion topic. Without the selfless work of these people, much of the process that went into the epilog would have been lost. If this paper is a success, we owe them a great debt.

This paper is dedicated to the memory of Dak Q. Rambeaux, the pseudonym I used when submitting this paper to avoid a conflict of interest.

References

[1] J. P. Anderson. Computer security technology planning study. Technical Report ESD-TR-73-51, Vol. II, Deputy for Command and Management Systems HQ Electronic Division (AFSC), L. G. Hanscom Field, Bedford, Massachussetts 01730, October 1972. Available from the National Technical Information Service as report number AD-758-206.

[2] S. Augarten. *Bit by Bit.* Ticknor & Fields, New York, 1984.

[3] G.D. Austrian. *Herman Hollerith: Forgotten Giant of Information Processing.* Columbia University Press, New York, New York, 1982.

[4] D.E. Bell. Secure computer systems: A refinement of the mathematical model. Technical Report ESD-TR-73-278, Volume III, Electronic Systems Division, Air Force Systems Command, Hanscom Air Force Base, Bedford, Massachusetts, April 1974. Available from the National Technical Information Service as document number: AD 780 528.

[5] D.E. Bell and L.J. LaPadula. Secure computer systems: Mathematical foundations. Technical Report ESD-TR-73-278, Volume I, Electronic Systems Division, Air Force Systems Command, Hanscom Air Force Base, Bedford, Massachusetts, November 1973. Available from the National Technical Information Service as document number: AD 770 768.

[6] D.E. Bell and L.J. LaPadula. Secure computer systems: Mathematical foundations and model. Technical Report M74-244, The MITRE Corporation, Bedford, Massachusetts, October 1974.

[7] D.E. Bell and L.J. LaPadula. Secure computer system: Unified exposition and multics interpretation. Technical Report MTR-2997, The MITRE Corporation, Bedford, Massachusetts, March 1976. Available from the National Technical Information Service as report number: AD A023 588.

[8] K.J Biba. Integrity considerations for secure computer systems. Technical Report MTR-3153, Revison 1, Electronic Systems Division, Air Force Systems Command, Hanscom Air Force Base, Bedford, Massachusetts, April 1977. Available from the National Technical Information Service.

[9] B. Blakley. The emperor's old armor. In *Proceedings of the 1996 New Security Paradigms Workshop*, Lake Arrowhead, California, September 1996.

[10] G. Burck. 'On Line' in 'Real Time'. *Fortune*, page 141, April 1964.

[11] V. Bush. *Pieces of the Action.* William Morrow, New York, 1970.

[12] S. Corriss, 1998. Retired commercial banker. Lecturer at American Management Association and the Federal Reserve Bank of New York. Personal communication with author.

[13] D.E. Denning. A lattice model of secure information flow. *Communications of the ACM*, 19(5):236–243, May 1976.

[14] Department of Defense. Department of defense trusted computer system evaluation criteria. Technical Report DOD 5200.28-STD, Department of Defense, Washington, D.C., December 1985.

[15] R. Everett, editor. Special issue: SAGE (semi-automatic ground environment). *Annals*, 5, October 1983.

[16] J.K. Gore. *Apparatus for Sorting Cards and Compiling Statistics.* U.S. Patent Office, Washington, D.C., April 1894. U.S. Patent No. 518,240.

[17] S.J. Greenwald. A new security policy for distributed resource management and access control. In *Proceedings of the 1996 New Security Paradigms Workshop*, Lake Arrowhead, California, September 1996.

[18] M.H. Harrison and W.L. Ruzzo. Monotonic protection systems. In *Foundations of Secure Computation*, pages 337–365, New York, 1978. Academic Press. Papers presented at a 3 day workshop held at Georgia Institute of Technology, Atlanta, Georgia, October, 1977.

[19] M.H. Harrison, W.L. Ruzzo, and J.D. Ullman. Protection in operating systems. *Communications of the ACM*, 19(8):461–471, August 1976.

[20] H. Hollerith. An electric tabulating system. 1889. In B. Randell, editor, *The Origins of Digital Computers*, New York, New York, 1982. Springer-Verlag.

[21] H. H. Hosmer. The multipolicy paradigm for trusted systems. In *Proceedings of the 1992 New Security Paradigms Workshop*, Little Compton, Rhode Island, September 1992.

[22] C.C. Hurd. Computer development at IBM. In J. Metropolis, N. Howlett and G. Rota, editors, *A History of Computing in the Twentieth Century*, pages 389–418, New York, New York, 1980. Academic Press.

[23] Joint Security Commission. Redefining security. Technical report, U.S. Security Policy Board, Located somewhere in the bowels of the executive branch under the Assistant to the President, National Security Affairs, February 1994. Available at http://www.spb.gov/html/jscrpt.html.

[24] D. Kahn. *The Code-Breakers.* Scribner, New York, New York, 1996.

[25] B.W. Lampson. Protection. In *Proceedings of the 5th Princeton Symposium on Information Sciences and Systems*, pages 437–443, Princeton, New Jersey, March 1971.

[26] B.W. Lampson. A note on the confinement problem. *Communications of the ACM*, 16(10):613–615, October 1973.

[27] C.E. Landwehr, C.L. Heitmeyer, and J. McLean. A security model for military message systems. *ACM Transactions on Computer Systems*, 2(3):198–222, August 1984.

[28] L.J. LaPadula and D.E. Bell. Secure computer systems: A mathematical model. Technical Report ESD-TR-73-278, Volume II, Electronic systems Division, Air Force Systems Command, Hanscom Air Force Base, Bedford, Massachusetts, November 1974. Available from the National Technical Information Service as report number: AD 771 543.

[29] J McLean. A comment on the "basic security theorem" of Bell and LaPadula. *Information Processing Letters*, 20(2):67–70, February 1985.

[30] P.G. Neumann, L. Robinson, K. N. Levitt, R.S. Boyer, and A.R. Saxena. A provably secure operating system. Technical Report SRI Project 2581, Stanford Research Institute, Menlo Park, California, June 1975.

[31] K.C. Redmond and T.M. Smith. *Project Whirlwind: The History of the Pioneer Computer.* Digital Press, Bedford, Massachussets, 1980.

[32] R.R. Schell, P.J. Downey, and G.J. Popek. Preliminary notes on the design of secure military computer systems. Technical Report MCI-73-1, Electronic Systems Division, Air Force Systems Command, L.C. Hanscom Field, Bedford, Massachussetts, January 1973.

[33] N. Stern. *From ENIAC to UNIVAC: An Appraisal of the Eckert-Mauchly Computers.* Digital Press, Bedford, Massachussets, 1981.

[34] L.E. Truesdell. *The Development of Punch Card Tabulation in the Bureau of the Census, 1890–1940.* U.S. Government Printing Office, Washington, D.C., 1965.

[35] U.S. Department of the Army. *Firing Tables for 155-mm. Gun, M1917, M1917A1, and M1918M1: Firing Shell, H.E., MK.III.* Department of the Army, Washington, D.C., 1933.

[36] U.S. Department of War, Bureau of Public Relations. Five news releases on the development, operation, and application of ENIAC, February 1946. Available in the archives of the University of Pennsylvania.

[37] W.H. Ware. SECURITY CONTROLS FOR COMPUTER SYSTEMS (U) report of defense science board task force on computer security. Technical Report CONFIDENTIAL (declassified), The Rand Corporation for the Office of the Director of Defense Research and Engineering, Washington, D.C., February 1970.

[38] M.E. Zurko, Associate Editor. Cipher. Newsletter 29, IEEE, October 1998. Available from htttp://www.itd.nrl.navy.mil/ITD/5540/ieee/cipher/old-issues/issue9810.