Global Information Assurance Certification Paper

Security—What Does "Trust" Have To Do With It?

Ken Lange
GIAC Security Essentials Certification
Version 1.4b (amended September 4, 2002)

Abstract
According to Webster the definition of Palladium is;
"1. (Greek Antiquity) Any statue of the goddess Pallas; esp., the famous statue on the preservation of which depended the safety of ancient Troy.
2. Hence: That which affords effectual protection or security; a safeguard; as, the trial by jury is the palladium of our civil rights. --Blackstone."[1] In addition to the classic definition of the word, Palladium is also a philosophy maintained by John David Pierce at his website, which states; "Even a cursory look at history reveals that the erosion of the structure that has held a society together eventually but inevitably leads toward the erosion and fall of the society itself."[2]

According to a White Paper on Intel Corporations website, "In the Spring of 1999, the Trusted Computing Platform Alliance (TCPA) was chartered to encourage industry participation in the development and adoption of an open specification for an improved computing platform. The TCPA participants agreed that the specification for the trusted computing PC platform should focus on two areas – ensuring privacy and enhancing security. TCPA members include Intel, Microsoft, Infineon, National, Atmel, and a large number of other organizations."[3] Subsequent searches on the internet on December 26, 2002 revealed no website for this organization or alliance, and the actual membership could not be verified as of this writing. However, many anti-TCPA websites were up and running and also stating that the membership in the alliance was being kept from public scrutiny and indeed password protected.

A large part of the technology industry is concerned with information security and trustworthy computing, and the purpose of this paper is to determine how the infrastructure and relationship between trust and security has evolved in technology. The growth of the internet and its underlying technology and applications give all of us greater functionality. Identity theft and other vulnerabilities have been exploited in the past and continue in the present, and despite greater technology, will be here in the future. While we strive to minimize the risk we face in protecting our security; in the form of Confidentiality—Integrity—Availabilty we will see what Trust has to do with it.

Introduction—Security Past, Present, and Future

What is security? According to the internet's Webopedia, security "Refers to techniques for ensuring that data stored in a computer cannot be read or compromised."[4] Of course if you are authorized to read or store that data, you can be trusted with it and you are granted access to do what you want with the data. The job of security then becomes a matter of determining how much trust to allow or verifying authorized users. Additional measures to ensure that data is secured involves encryption and decryption, firewalls with blocked internet traffic, and host-based and network-based intrusion detection systems. Security management also involves the recording and monitoring of security and access logs. The goal of a secure system is to provide confidentiality, integrity, and availability to its users. There are varying degrees of security and methods to use based on what you are protecting and in some cases where you are located. National and state laws may also apply as well as federal guidelines relating to privacy of information, or the need for public availability of information. In order to determine the relationship between "trust" and "security", let's look at the evolution of information security.

The Ghosts of Security Past

The November 2002 issue of CSO Online includes a debriefing document that highlights "Significant Moments in Security History…such as the incident in the fall of 1066 when William the Conqueror takes advantage of mis-configured firewall. Saxons use too much hot tar, accidentally burn down their own fort at Hastings and King Harold loses England."[5] While this is not a serious comparison to the technological world of today, it does present us with the notion that security as a whole can mean more than breaking into a computer, or computer account. Physical security can sometimes be overlooked in the technology budget and planning stages. However, physical security and trust are very much related. You do not leave your children with a baby-sitter you do not trust. As an employer, you do not trust someone with access to critical data, even if it has been secured properly, if you know that the employee will use this data in an illegal manner. When you trust someone with physical access to your system, security up to that point is no longer a concern. The next level of access may be secured and the "trusted" person up to that point has to therefore prove once again he can be trusted. How he does that is what defines the level of security.

In a more current look at security problems, the SANS Institute created "The Top 10 Most Critical Internet Security Threats List"[6] in June of 2000 and gave the information security community an invaluable tool to help defend against unauthorized activities in their domain of influence and trust. The ability for network administrators to look at one document that coordinated the efforts of many professionals in the security industry has been very beneficial, and continues to be a well-documented and very definitive point of reference concerning security vulnerabilities. The concept of sharing the knowledge between professionals is not new, but this was the first best case of how to apply the shared knowledge to protect against potential security threats. Not only did we have a single source that defined the vulnerabilities, but better still we now had and still have a

document with information on how to protect against these particular vulnerabilities. At the same time, all of the potential bad guys in the world can look at this document and possibly learn some techniques and vulnerabilities that they were not aware of. Do the creators of the Top 20 List trust everyone who reads it to use it for good purposes? How can they when they have no control over who reads it? This list is public domain, and like all things in the public domain, it is not secured from unwanted access and trust does not factor in. Trust is explicitly granted to everyone.

What about security problems from the recent past that we know about? In the course material for the SANS Security Essentials training, we are presented with "Four Lessons From History"[7] They are;

- Morris Worm – Availability – 1988
- Melissa – Availability – 1999
- W32.SirCam Worm – Confidentiality – 2001
- Code Red II – Integrity – 2001

These specific security breaches deal with a particular aspect of security. The Morris worm attacked availability while Code Red II was meant to compromise integrity. Each of these instances could have been avoided if the right security measures or a defense-in-depth had been established. I am sure that in each case, the unauthorized access was not a trustworthy operation. Trust was not established because in most cases, identity was not established. Security and its components are based upon a defined set of authorized, or trusted, users with specific levels of access base don how much they are trusted or allowed to do. When an identity is simulated or bypassed altogether, trust cannot be established and security has been negated. The lesson learned from these instances was that vulnerabilities exist and they will be exploited. One type of defense is not enough. A layer of defensive procedures must be established to create layers of trust. Access to one layer does not always give access to the next layer. Security can only be maintained when identities can be confirmed. When an identity is spoofed, all bets are off.

The Ghosts of Security Present

As the Top 10 List grew over time, it has evolved into today's version; "The Twenty Most Critical Internet Security Vulnerabilities (Updated) – The Experts Consensus"[8] This document continues to provide information and is a living and trusted document. We have learned from past experiences what works and what doesn't work. We have established a defense against the top vulnerabilities and methods used to bypass security. We have we learned and we continue to learn. They also have learned and continue to learn. A firewall does specific things to block out traffic coming into our system that we don't want. We don't trust it because either we know what it is and have identified it as dangerous to our system, or we don't trust it because it can't be identified as legitimate. An intrusion detection system is used to determine what type of activity is taking place on the wire. Is all of the activity serving a specified purpose or is it

unidentified traffic that is searching for a way to exploit our system? A firewall may allow traffic past its border that appears legitimate or is disguised as a legitimate request. The next level of security, intrusion detection, does not necessarily trust what it sees or hears. It may merely report and log activity, it may sniff out suspicious activity and trace it back to its source. Trust at one level does not always mean trust at every level. The ability to watch what is going on in real-time is part of the security procedure, but is time-consuming and takes resources away from the system. Reviewing log files for what has happened in the not-to-distant past is also time consuming, but they are both necessary parts of maintaining a secure system.

Just because we know what the vulnerabilities are does not mean that we are protected against them all of the time. If we do not take the measures specified to protect our systems, knowledge is meaningless. Patches that are not retrieved and applied are not doing any good, and in some cases patches that are retrieved can cause additional problems. How do you know which patches to trust and which ones to leave alone? This is a major concern of network administrators the world over, and has been given quite a lot of attention at software companies like Microsoft recently. They are aware of the inherent lack of trust that the general public has in software and the internet in general. Microsoft is doing something very specific to address this lack of trust which will be addressed later, but the fact that there is this lack of trust makes the presence of security even greater. In many cases, a simple warning or disclaimer of no trespassing may deter the simple attempt to look at your data. However, most current cases of security problems are driven by greed and blatant attempts to disrupt the fabric of the internet for national and global reasons. These attempts have driven the federal government to create and maintain a Critical Infrastructure Protection Board and a National Strategy to Secure Cyberspace. This Strategy will be a combined effort of public and private industry sectors, encompassing many different industries. The internet is the fabric upon which commerce has found a new home. The communication and ability to share knowledge is a big factor, and we often find ourselves wondering if we can trust everything we read on the net. Commerce and the ability to buy and sell has driven the economy in the United States for a number of years, and the concern that the internet as a medium could have its integrity or availability compromised is the main concern driving this National Strategy. Are we being reactionaries? Are we paranoid, or is their a threat to the security of cyberspace? Can we trust the transactions that take place on the internet everyday?

The Ghosts of Security Future

As technology advances and as experts learn how to use new techniques for defending against vulnerabilities, the threats will also advance. If we think that the bad guys are standing still, then we are mistaken, and some people argue that they may be learning faster. One of the advantages that we have is that we control the system and we hold the keys. We must use this advantage and others and as technology advances, security processes must also change and advance.

In a recent bonus issue of the email newsletter from SANS Institute Experts Predict the Future of Computer Security[9], the following comments were made;

- Bruce Schneier, CTO of Counterpane Internet Security, Inc.
  - "Our hardest job, and the thing we spend the most time worrying about, is catching the real criminals among the hundreds of annoying hackers."

- Bill Murray, Executive Consultant, TruSecure Corporation
  - "While we will continue to experience attacks and breaches to define the limits of our success, security will continue to be just barely good enough to escape chaos and preserve public trust and confidence."

- Stephen Northcutt, Director of Education, The SANS Institute
  - "We need to develop the laws, processes, even terminology to effectively manage and protect digital property."

These comments are directly related to the trust issue in security. We would not trust a criminal in our system and we design our security to keep them out, and if possible, catch them. Technology is the resource we have to build security systems to determine annoyances from true intrusion. We learn, they learn…we change, they change. It will be a continuing battle to stay ahead of those people or those systems we don't trust, identify them, and exclude them. How we do that and how we determine "trustworthy" is what the future holds. In some cases, we don't even have the correct words to describe what we are trying to protect, identify, or exclude. The definition of authorized access or use is sometimes mangled and misunderstood, and criminals as well as everyday users will continue to misuse the system. Security problems in the future will continue to be about confidentiality, integrity, and availability. Trust in the future will continue to be an objective thing based on what you think you know about somebody or something. Trust is what you grant to someone…security is the procedure whereby you grant that trust. This is the definitive relationship between security and trust and it will continue to be the definition in the future. As Microsoft and Intel and the government continue to define "Trustworthy Computing" we will continue to monitor access to our systems and we will hopefully continue to control access based on our definitions of who we trust.

Trustworthy Computing

In an Executive Email from Microsoft[10], Bill Gates says…"Creating a Trustworthy Computing environment requires several steps: Making software code more secure and reliable…Keeping ahead of security exploits…Early recovery in case of a problem" The process outlined by Mr. Gates is a complex issue that will require cooperation among industry peers in the security field and between hardware and software manufacturers. Public and private sector enterprises need to work together, and not withstanding of these efforts, the day-to-day goal of maintaining profitability will surely remain a constant factor. I believe that the government wants to create a secure infrastructure,

but at what cost? I believe that Microsoft and Intel, and others, want to provide a safe and "trustworthy" computing platform, but who will control it? They all say that we, the consumer, will retain control and can choose to implement or not to implement the enhanced security that will be available on future systems. Even if that is true, if we do not implement the new features, then we have cut ourselves off from the rest of the world. A man stranded on an island is unlikely to need a firewall. This type of control feature is not truly beneficial to the user, in order to maintain control, or access, or trust to our systems, we need to work with the system. If we merely make our own rules and play a different game, then we are not part of the cooperative effort to be part of a secured and trusted world of computing.

"Trust between computers describes the authentication (or lack of authentication) required and the actions that can be taken by a user on a remote system."[11] In a world where authentication and identity are digitalized and transmitted thousands of times a day, which ones can you trust and why? Can Microsoft and others really do something to help, or are they just looking for a way to control the trust relationship? Trust can be a one-way street or a two-way street. If I trust you, then I give you complete and unsecured access to my system, but if you don't trust me…it is a one-way relationship. If you are trusted, is that the same thing as being secure? Not really, if you are trusted then you are free to do what you want...and you could disrupt the confidentiality, integrity or availability of a system. If you are trusted, then you are beyond the scope of security tools…if you are trusted, you don't need to be secured. However, you must first be identified and be known as an authorized user of the system. You can't trust what you don't know.

Palladium

What is Palladium? Microsoft has created a technology called Palladium that will be part of the Windows operating system and will rely on protected data storage capabilities of hardware components. There are many technology papers available on the internet that describe it in detail, and Microsoft has several white papers that discuss this new technology in concept and delivery. While there are many differing opinions on what it is or what it does, the one thing we can all agree on is that we need a tool in our set of defenses that helps us determine ownership of property and positive identification. These concepts are the basic building blocks of security in the future, and must first be defined before trust can be established. Up until now we have been talking about trust as something that is given or defined that controls the access you have to a system. We have been talking about security in the concept of tools or procedures that are put in place to determine identity or authorization. Does Palladium or the initiative to create a Trustworthy Computing platform change this?

In an article at PC World.com[12], Microsoft security executive Craig Mundie states that "Security is a priority in future products, we view this as a long journey. The stage right now is remediation, fixing sins of the past, and making design changes for the future." This is not something that will spring onto the markets and into products anytime soon. It will change numerous times before it gets released. Microsoft is taking the

responsibility here for the mistakes it has made, but what are they offering? Is Palladium their remediation? Is better software with fewer bugs their remediation? That is something we will have to wait and see, but we need to implement the newer products today. The article continues…"Palladium is designed to help devices that communicate with each other clearly identify their origin, including the software they're running and person using them, to enable greater trust and smoother information exchange..." This is a concept that bears looking at more closely. If identity is embedded into the devices that are communicating with each other, then the process of falsifying identity becomes harder to do. If the individual who is trying to gain unauthorized access cannot confirm the identity of the resource he is using, then trust cannot be established, no matter what identity or authorization he has as a user. If the process of authorization becomes one of hardware versus software, then we change the rules and we make it a different game. Does this mean that hackers and bad guys can't work around this and that this will solve the security issue once and for all? Not really, it just puts up some new roadblocks, and at the same time may make it harder for illegitimate users of copyrighted material to use the material.

In a related context, David Coursey at AnchorDesk.com writes; "Palladium was originally intended to be a rights management system…Whether we do or don't get real trustworthiness with Longhorn, we must have a solution to rights management issues. However, this is as much a matter for the Congress and courts as it is for technology people."[13] This statement seems to agree almost verbatim with the comments of Stephen Northcutt earlier. The courts and the government have still to be heard from on many of the technology issues as it relates to unauthorized access, copyright issues as it concerns digital property, privacy issues, and even cloning issues. With the ability to clone people, will a fingerprint or retinal scan determine authorization in the future? The right to protect something is not as clearly defined in the digital world as it is in the physical world and as the laws and regulations evolve, technology will continue to stay one-step ahead of it. This statement also seems to state that Palladium is not about security, but more about the ability to confirm ownership. While the ability to confirm ownership, or identity can certainly help create a more secure system, it is not the

"Trustworthy"

This word conjures up many meanings and is related to the computing world and security in a variety of ways. In a recent Wired News article by Lauren Weinstein entitled "Is Microsoft Truly Trustworthy" the author states "Security problems in Microsoft software, or any software for that matter, are critical issues. But it's crucial that computer users themselves have the final say over how security will be handled on their own systems."[14] This confirms our earlier concerns that security is only as good as the person or persons who control the access. If control passes away from the individual user or enterprise organization in charge of controlling access to their network, then the ability to trust, and the right to privacy becomes the issue. Information may be secure, and identity may be confirmed, but is it available and is it confidential, and can you confirm the integrity of the data? Not if you don't control it. What if you share control?

What if Microsoft or Intel or some combination of forces confirmed the identity of those resources attempting to connect to your resources, but you determined availability, confidentiality and integrity? A shared control approach is the only way that this type of initiative would work, and then with audit and control procedures put in place and monitored to determine the confidentiality, integrity, and availability of the system itself. In order for Palladium, or security in general to work, we have to trust somebody.

Forcing Compliance

Microsoft is willing to break a few eggs to make Windows secure…and the applications that run on them. According to Craig Mundie, Microsoft Security Executive, "Even if it means that we're going to break some of your applications, it's going to make things more secure."[15] This is a pretty bold statement that has already created a lot of feedback as you can imagine, but it is not anything new for Microsoft. Industry veterans are not shocked or surprised by this statement, and it just gives Microsoft another excuse to use whenever one of their patches creates additional problems…they were just making it more secure.

The real problem with the Microsoft updates is not that they may break other applications or even that they are needed, but that we may be forced to get them to prevent an exploit into a key part of our system. It is too late, we are already at that point. With the numerous exploits and vulnerabilities in the Windows operating system, we cannot afford NOT to patch a possible vulnerability. This process which I call forced compliance brings a whole new set of issues and concerns to the technology folks who maintain the network. We lose control of what is installed on our systems because we have lost control of the system. We cannot maintain a secure and an open system when we cannot control which patches we want, which vulnerabilities we can have or not have. We lose the ability to choose and the ability to control.

The Last Word

Bob Cringely doesn't think Microsoft can be trusted. In a recent online edition of "I Cringely, The Pulpit" he states "The world is a dangerous place and finding ways to make people responsible for what they do on the Net is probably good, not bad. I just don't think we have the right people on the job."[16] He further elaborates that it is all a part of a plot by Microsoft to control the internet, and who knows maybe he's right. Regardless, he makes a good point in that the world is a dangerous place, and making people responsible for their actions is a good thing, whether it is on the internet or on the streets, but how do you do that? It is a struggle that has been going on for ages, and just like King Harold, we must watch how we configure our firewalls, or we will get burned in the process.
Information technology and the issue of how security is maintained will be an industry of growth for many years, simply because technology is here to stay and the internet will continue to be the backbone of our communication. Its integrity must be maintained, its

confidentiality must be bullet-proof and it must be on all of the time. How we do that is just as much a matter of trust as it is technology. Knowing who someone is is one thing, but knowing what they are capable of doing and why they are doing it is a matter of trust. When you get right down to it, security of a system has nothing to do with trust…you must trust no one.

In the November 2002 online feature for Info Security Magazine, "The Influence List" [17] includes the vendors, technologies and people that shaped our past and frame our future. Weighing in at number 2 on the list is…Microsoft. Why? Here is what they say; "Hardened infosec veterans may scream at the inclusion of Microsoft on this list. After all, Windows is the root of all evil, right? But like it or not, the software giant has had an undeniable impact on IT security, and its influence—for better or for worse—will continue over the next half-decade and beyond. Will Windows ever be likened to a "trusted OS?" Unlikely, but Microsoft is paying more attention to security, and over the next five years that will have an unmistakable effect on how we secure our enterprise systems." Whether we trust Microsoft, or whether we don't trust Microsoft is not the real issue either. There will always be those people who bash Microsoft and those people who don't. Microsoft will continue to make products and be a leader in the software and operating system business. We will continue to love and hate Microsoft, but we will also continue to have security problems. No matter what Microsoft or Intel or anyone else does, we will still have security problems. They will be different problems and this will require different solutions. We will continue to require multiple layers of defense and we will continue to learn and share our knowledge. But whether we trust Microsoft or not is not the key issue. We need to know who is using our system, who is accessing our system, and we need to know if we can trust them.

References

[1] *Webster's Revised Unabridged Dictionary, © 1996, 1998 MICRA, Inc.*
[2] Palladium Philosophy, John David Pearce. Retrieved from the World Wide Web on December 26, 2002 at URL: http://home.earthlink.net/~jdpierce/palladium/philos.htm
[3] Bajikar, S. "Trusted Platform Module (TPM) based Security on Notebook PCs – White Paper" Retrieved from the World Wide Web on January 13, 2003 at URL: http://www.intel.com/design/mobile/platform/downloads/Trusted_Platform_Module_White_Paper.pdf
[4] Webopedia. Retrieved from the World Wide Web on January 13, 2003 at URL: http://www.pcwebopaedia.com/TERM/s/security.html
[5] CSO cso online.com "Significant Moments in Security History" Retrieved from the World Wide Web on December 26, 2002 at URL: http://www.csoonline.com/read/110802/debriefing.html
[6] SANS Resources – How To Eliminate The Ten Most Critical Internet Security Threats. Retrieved from the World Wide Web on December 26, 2002 at URL: http://www.sans.org/topten.html
[7] SANS Institute, SANS Security Essentials II: Network Security p1-10
[8] SANS/FBI The Twenty Most Critical Internet Security Vulnerabilities. Retrieved from the World Wide Web on December 26, 2002 at URL: http://www.sans.org/top20/
[9] The SANS Institute, NewsBites@sans.org "SANS NewsBites Bonus Issue – December 13, 2002
[10] Gates, B. Microsoft Executive E-mail "Trustworthy Computing" July 18, 2002. Retrieved from the World Wide Web on December 26, 2002 at URL: http://www.microsoft.com/mscorp/execmail/2002/07-18twc.asp
[11] Eric Cole, Mathew Newfield and John M. Millican. SANS GIAC Certification: Security Essentials Toolkit (GSEC), Chapter 2, p 41
[12] Watt, P. "Microsoft Outlines Security Policy" PCWorld.com, Thursday, November 14, 2002. Retrieved from the World Wide Web on December 12, 2002 at URL: http://www.pcworld.com/resource/printable/article/0,aid,106928,00.asp
[13] Coursey, D. "Here's what I think the next Windows will look like" from ZDNet UK News. Retrieved from the World Wide Web on December 12, 2002 at URL: http://comment.zdnet.co.uk/cgi-bin/uk/printerfriendly.cgi?id=2127205&tid=479&b=cm
[14] Weinstein, L. "Is Microsoft Truly Trustworthy?" Wired News. Retrieved from the World Wide Web on December 12, 2002 at URL: http://www.wired.com/news/print/0,1294,56490,00.html
[15] Berger, M. "Mundie grades Trustworthy Computing after first year" November 13, 2002. Retrieved from the World Wide Web on December 26, 2002 at URL: http://www.infoworld.com/articles/hn/xml/02/11/13/021113hntrustworthy.xml?s=IDGNS
[16] Cringely, R. "I Told You So" I Cringely | The Pulpit. June 27, 2002. Retrieved from the World Wide Web on December 26, 2002 at URL: http://www.pbs.org/cringely/pulpit/pulpit20020627.html
[17] Briney, A. "The Influence List" Info Security Magazine Online. November, 2002. Retrieved from the World Wide Web on December 12, 2002 at URL: http://www.infosecuritymag.com/2002/nov/influence.shtml