Global Information Assurance Certification Paper

Business Consideration and Network Implementation of Generally Accepted Security Standards

Patrick Nolan

Practical Version 1.2c

It has been and still is apparent to anyone that reads the GIAC detects webpage that first "Integrity" is compromised and then "Confidentiality" is lost on hosts and networks for days, weeks, and sometimes months from initial Intrusion Detection to final fix of the data hemorrhage. And "an ounce…"

My starting points for this practical have been many and a crystallized view is contained in the following quote from a SANS resource article by J. Christian Smith:

> "A more viable approach has to start from the inside, with the basics, preventing trojans and backdoors from becoming inserted in the first place. It bears repeating that this is only going to occur when users are properly educated about security policy and procedures, are provided useable tools for information assurance, and the security of the multilevel system that is a computer network is regularly audited for compliance." **1.**

And I discovered that if you "start from the inside" then it followed that Operating System and Application Integrity and Auditing are synonymous. There are many ways to enhance network security and in this paper I try and apply general standards to specific network security issues that should be goals added to the already numerous demands placed on network security administrators.

Experience and education dictate my selection of "business perspectives". Even a cursory reading of voluminous **generally accepted security standards** compels the inclusion of business perspectives in any practical on the subject of network security. The Standards include huge amounts of information on why preemptive protection of any network's **Customer's** networks and computers is important.

Please bear with me as I use the word Customer. I learned long ago that using generalized terms like "user" and other abstract terms can lead otherwise great people to lose site of the fact that the Customer is the most important part of any business endeavor.

My goal for this practical is to add to and reinforce the many efforts by security organizations that show the intrinsic value of a distributed effort to develop and implement host based Integrity and Auditing programs that include Customers.

Business Perspectives

Protecting any network to ensure the continuity of a business is important. However the continuing compromise of networks begs the question "Where and to what state do you want your network security defenses to fail to?" Certainly failure to a secure host is an achievable goal of a layered approach to security. In this practical I include Customer's networks and hosts in my definition of a network. And since the most vulnerable component of most networks are their Customer's networks and computers my approach is to consider the Customer's security. Much has been published about why the Customer and their network and host computers should be explicitly included in defining network security initiatives. Reasons given were common sense ones. The "bottom line" concern though is that if a network's Customers can't log on to the network to spend their money someone's job is at jeopardy.

Beyond the published concerns of Organizations or Vendor$ there is a demonstrable lack of **proactive**, consistent, uniformly presented Network Security Administration efforts for the Customer's network and host computer security. Part of my observation is based on personal experiences with Security Response Centers, Product Support operations, Network Operations Centers (NOC), Network Security Operation Centers (SOC), email responses to "abuse" reports, and phone conversations with NOC and SOC staffs.

For instance in the comprehensive paper "Consensus Roadmap for Defeating Distributed Denial of Service Attacks" prepared by CERT, SANS and CERIAS, (Version 1.10 February 23, 2000, A Living Document), the authors note that:

> "Currently, there are tens of thousands – perhaps even millions – of systems with weak security connected to the Internet… The number of directly connected homes, schools, libraries and other venues without trained system administration and security staff is rapidly increasing. These "always-on, rarely-protected" systems allow attackers to continue to add new systems to their arsenal of captured weapons." **2.**

The authors go on to list the following as their first immediate step to help limit the potential for network damage:

> "industry and government will cooperate to educate the community of users – about threats and potential courses of action – through public information campaigns and technical education programs." **2.**

While researching what "public information…. And technical education programs" to "educate the community of users" existed I was struck by the varied and incredible number of websites purported to be about security. However not one website had a simple, comprehensive list of basic steps that the average Customer could follow to secure their computer.

To correct the omission of step by step help for Customers I spent the paltry sum of $170. I obtained a domain name and put up a website with a step by step format. I proceeded to ask security-oriented organizations with websites that Customers might frequent to post a link. I was not surprised when CERIAS at Purdue University posted a link and said of my website "It's close to the best, if not the best, and simplest Windows® Security links and recommendation site for home computer users interested in securing their windows os." I was not surprised because I had not seen such a simple format like the one I adopted at any ISP security information webpage. My point here is that if I can take $170 and accomplish something that Customers rave about and CERIAS appreciates, then what improvements in network security might be accomplished if every network used such a simple format for it's Customers? Even the best security information websites are "network oriented" and thus not "Customer friendly". The addition of one or two WebPages with step by step instructions and links would go a long way towards both educating Customers and in defining their responsibilities as a network user. And defining Customer's responsibilities has many benefits.

As an additional illustration ask why, if Steve Gibson's Shields Up security website or Symantec's Security and Trojan Test website are so popular, most network's have little that comes close to helping Customers as much, and many fail to even post security information links for their Customers to use. Vendor neutral information should be widely available to Customers.

Liability Issues

How much would it cost (directly, indirectly and include fully absorbed costs if you care to) to establish network based email Antivirus or attachment filtering. What cost is there involved in blocking outbound non-network source IP originating packets? I'm sure if you ask that to a company's auditor he will come up with direct, indirect and fully absorbed costs for these network security measures that are far less than the costs of a loss of network based business income. I'm also sure you'll be told the same thing if you ask a companies lawyer about the cost of a loss from a "Customer" class action lawsuit for negligence in protecting a Customers computers because **generally accepted security standards** were not followed. The cost of following generally accepted security standards as they apply to a network's Customers, before a problem arises, will be far less than either of the two losses I mentioned. And a network that follows standards and helps Customers protect their networks and hosts not only generates goodwill with Customers, it establishes clear evidence to help protect the business in the event of a lawsuit. Consider this:

"Site Security Standards: Security Incident Handling Liability Warning

It is possible that in the near future organizations may be held responsible because one of their nodes was used to launch a network

attack." (My Note: A good lawyer will read "node" as "your Customer") "In a similar vein, people who develop patches or workarounds may be sued if the patches or workarounds are ineffective, resulting in compromise of the systems, or, if the patches or workarounds themselves damage systems. Knowing about operating system vulnerabilities and patterns of attacks, and then taking appropriate measures to counter these potential threats, is critical to circumventing possible legal problems." [3].

I find the last sentence in the above quote very interesting. Since most network security employees are paid to know about operating system vulnerabilities and patterns of attack, what would that employee testify to in a lawsuit brought by Customers who were harmed by a lack of network effort to use generally accepted security standards? Both older and new generally accepted security standards explicitly specify Internet and Intranet host protection as a fundamental standard. And if it's a "standard" that's "accepted" you can bet a lawyer is going to use it against a network soon if their Customer's network and host protection is not an active part of a security program. Rue the day that as a Network Security Administrator you are on the witness stand as a defendant and the plaintiff's counsel asks you over and over if you followed each instance of applicable "Customer network or host" oriented generally accepted security standards and you answer "No". And if it happens in front of a Judge or Jury that doesn't care about a job or employer's priorities and limitations, your defense attorney just had "triple damages" leap into his mind.

Waiting for a Customer's lawsuit is something that even AOL/TimeWarner no longer ignores, witness their recent decision to not forward to their Customers a myriad of email file attachments. (TimeWarner/RoadRunner does not yet follow this precaution, allows outbound non-network source IP address traffic, and still passes email usernames and passwords in readable form).

Even Microsoft posts this interesting warning in its new .NET application developers information. "Using code access security can reduce the likelihood that your code can be misused by malicious code. **It can also reduce your liability** because you can specify the set of operations your code should be allowed to perform as well as the operations your code should never be allowed to perform."

In addition to the liability concern the demonstrable lack of effort to follow generally accepted security practices for a Customer's network and host security will repeatedly result in the widespread loss of the Customers ability to spend their money on a network's services and products. Whether this loss of business income started with a script generated polymorphing virus or was a distributed act of electronic warfare will not matter. Can any network's income be reduced by 5%, 10%, or 30% for a day, a week, or a month?

Some OS and Application Integrity and Audit Standards

The Center for Internet Security's Foundational Standards as of 14 October 2000 can be found by using this link: http://www.cisecurity.org/standards.html. The webpage provides links to numerous Standards Organizations that were the source of the Center's foundational standards.

An exhausting review of the Center for Internet Security's Foundational Standards sets the following as generally accepted OS and Application security standards (For the sake of brevity I will rely on the Standards that are most relevant to this practical. Ignoring the "business" inclusive concerns of the other foundational standards not covered here is perilous).

OS and application software integrity is paramount. Expressed concerns on this issue include the warning that during an attack on a Customer's network or host:

> **"System software is the most probable target. Preparation is key to be able to detect all changes for a possibly tainted system. This includes checksumming all media from the vendor using a algorithm which is resistant to tampering. (See sections 4.3) …… In all cases, the pre-incident preparation will determine what recovery is possible."** [3].

> "One way to provide this is to produce a checksum of the unaltered file, store that checksum offline, and periodically (or when desired) check to make sure the checksum of the online file hasn't changed (which would indicate the data has been modified). Files can be modified in such a way as to preserve the result of the (...) sum program! Therefore, we suggest that you use a cryptographically strong program, such as the message digesting program MD5 [ref], to produce the checksums you will be using to assure integrity." [3].

How exactly does this apply to a Customer's OS and Application Integrity? Although it's clear that using checksums is a "standard" it is also "suggested" that you use a "cryptographically" strong program …….. to produce the checksums you will be using to assure integrity". I note here that suggestions "should" be adopted, and if you have a good auditor and you are not following the "suggested" standards, I'm sure he's already nailed you on the issue. If it's a generally accepted security standard that these checksums, principally described to be used on a network OS and Application for after the fact integrity auditing purposes, should be protected by a cryptographically strong program, it automatically follows that the same cryptographically strong protection be applied to the Customer's unaltered, critical OS, Application and Network Communication files. This certainly is an achievable goal.

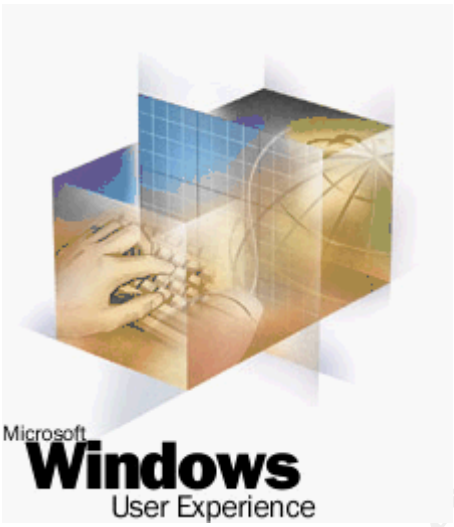
Next the "standards" recommend that "auditing" should be performed. Generally accepted security standards for Auditing are well established, comprehensive and fall outside the scope of this paper. I would like to note that Auditing as used in the foundational standards is chiefly concerned with an Audit in the traditional sense. Generally the standards do not specify detailed OS and

Application Auditing methods, but an auditor will Audit you and ask you how you specifically perform Integrity checking. A brief description includes the following:

> "Audit data should include any attempt to achieve a different security level by any person, process, or other entity in the network." 3.
>
> "SysTrust™ Principles and Criteria for Systems Reliability Version 2.0,Copyright © 2000 by the American Institute of Certified Public Accountants, Inc. and Canadian Institute of Chartered Accountants.
>
> S2.7 There are periodic checks of the entity's computers for unauthorized software.
>
> M2.3 There are procedures to ensure that only authorized, tested, and documented changes are made to the system and related data." **4.**

So the generally accepted security standards are a little vague on the specifics of an OS and application Audit but mention that "Audit data should include any attempt … by any person, process, or other entity in the network." And since this is not an issue that can be directly addressed by a network it falls into an area where networks can use their knowledge and financial clout to accomplish developments in security software that benefit the Customer and network security. The development needed here is in making information generated from security applications that the Customer's and Network's currently use much more useful to both the customer and the network.

To summarize this section, OS and application Integrity and Auditing are virtually (no pun intended) synonymous. Comprehensive, Customer friendly OS and Application Integrity and Audit support is the overall issue because it cannot easily be achieved with today's OS's and Applications. And the fact that there is no easy solution is clearly illustrated by Microsoft's own references to **their** "DLL Hell", and nowhere as rosy as the next Microsoft graphic depicting a Microsoft Customer's experience. Does it look anything "DLL HELL" to you?



Since we all know that the complete protection of the different Windows® OS's and Applications on a computer connected to a network or Internet is "virtually" impossible for Customer's I next try to apply information about generally accepted network security practices to achievable Customer security efforts that are mentioned in the Standards.

Ten specific ways to help Customers Secure Networks

1. **Help Customers secure their OS**. Recommend that Customers buy the commercial version of FreeVeracity for a fairly comprehensive Integrity and Auditing solution. And recommend the use and purchase of products such as "GoBack" and "Ghost" for those Customers whose OS does not come with a "rollback" feature. FreeVeracity will operate on standalone hosts as well as networks. There is also a practical about FreeVeracity in the SANS reading room, **File Integrity Assessment Using FreeVeracity, Jason Amsden, February 4, 2001**. Obviously this is the most difficult of all issues for Customers, me included. There will never exist "easy to follow" OS and Application specific lists of the important files, checksums and registry entries that can be secured and periodically compared with an installation list of originals that every OS and Application developer should have available for customers. The development of OS and Application Update Sites with Auditing and Integrity Checking features would be great.

2. **Recommend that Customer's and Networks use host-based firewalls that control the Network Driver Interface (NDI) and allow MD5 encryption of those network communication critical files that use the NDI.** This is a simple addition to a layered defense and unlike some well-known firewalls and port blockers it incurs little processor overhead. Currently Tiny Software, ZoneAlarm, and another firewall, Sphinx, (I have not tested Sphinx yet) advertise that they control the NDI and use MD5 Encryption to protect network communication programs. Tiny Firewall, ZoneAlarm and Sphinx are

commercially available for business host deployment. Tiny and ZoneAlarm have free versions for home use. Its only limitation is that some network communication methods bypass NDI drivers and access the NIC directly.

3. **Sell specific USB security appliances and NIC's to Customers that functionally address network security.** NIC's and USB security appliances that enhance Customer security and can be hard coded and preconfigured for the host network security are just coming to the marketplace. It's amazing how Vendors will respond to market demands.

4. **Define Customer responsibilities** for their OS and application security. An industry wide agreement of defined Customer responsibilities would go a long way towards reducing everyone's liability and vulnerability.

"Site Security What Makes a good Security Policy

What Makes a Good Security Policy? The characteristics of a good security policy are: …… (2) It must be enforcible with security tools, where appropriate, and with sanctions, where actual prevention is not technically feasible. (3) It must clearly define the areas of responsibility for the users, administrators, and management." 3.

5. **Make Customers keep their OS, Browser and E-Mail client patched.** If I owned an ISP I could accomplish this easily. I would increase my Customers monthly access charge and at the same time offset the charge by offering some free access equal to the fee increase for those customers that came to my website and let me determine that they had the latest security patches. That would also shift the financial burden of increasing network security costs to those Customers that have insecure systems. ISP's and Networks can determine a Customers OS, Browser and Email Client versions when the Customer signs on for the service.

6. **Require Customer maintenance of the OS and Application patches as a Term of Service** that, if violated, will lead to termination of services. Include Antivirus, anti-trojan and script protection software as Customer responsibilities. Automatically e-mail patch availability notices. An ISP lawyer will love it. Make the Customer visit your website for regular determinations as to verify installation of the latest patches. Microsoft, ISP's, and any other website operator that uses proxy hosted network communication should specifically require maintenance of OS and site specific Application patches as a Term of Service. If this cannot be accomplished then email the Customers copies of the GIAC daily intrusion detects and show them how many networks without patches are being hacked every day. As I noted before if AOL/TimeWarner and Microsoft are taking obvious steps to minimize their liability it's a good indication everyone else should.

7. **Address patch and application "Known Issues"** for Customers. Having

this information delivered to a Customers desktop while they are at an update site such as the Symantec/ZDnet Web Services Application update would be great. And it would certainly make subscribing to the service more enticing. The lack of Customer patching to prevent stability problems on their networks and hosts is a legitimate Customer concern. At a minimum easy access to "Known Issues" and "User Forums" should be available to Customers.

8. **Demand Security Applications that have simple, useful GUI's and useful reporting options**. Useful means that the security industry has to establish a set of generally accepted security application reporting standards. Working with Security Application vendors to get what you know is useful on the GUI is much easier while they are developing applications. It's up to each network security administrator and Customer to specify to application vendors that we no longer want applications that require us to do work that they can easily accomplish with the existing exhaustive process and thread information available to their programs. Customers need to be able to read "The program "unknown" is trying to connect to "Internet Explorer" or "The program "unknown" connected to "Internet Explorer and has established a connection with Korean IP address x.x.x.x". And they have to know that this is a security problem. The actual details of how this occurred on their host should also be available too, but most current Customer applications fall far short of providing friendly GUI's that enhance useful Customer and Network security efforts.

9. The usefulness of Customers reports of security related information can be as valuable to Microsoft, ISP's and networks as the information that is analyzed by the SANS GIAC is to network security administrators. I have only seen one ISP with a "Customer" friendly incident reporting webpage and it displayed a nice **form** for the Customer to complete. All the Customer had to do was enter as much information to it as they could determine from whatever security applications they were using. That ISP knows a lot more about abuse and trends on it's network than others that blindly require the Customer to e-mail in information they often don't have a clue about finding. This is to me a critical issue. I would like to point out that the model provided by the phenomenal success of the Global Incident Analysis Center and other organizations concerned with network security begs the question of why isn't a similar one in place for Customers. **The development of uniform Customer reporting methods and forms recommended in various "Standards" should not be left to individual application vendors, a few privately funded website operators and ISP instructions to email "abuse@" or "support@" with information most Customers cannot access.** Relevant "Standards", although written for network users, include:

> **"users must know how to report suspected incidents. Sites should establish reporting procedures that will work both during and outside normal working hours.**[3]

"it might be necessary to fill out a template for the information exchange."[3].

10. **Provide "step by step" information to Customers** and provide a range of specific options to help them accomplish security for their hosts. Many good things besides having secure Customers will happen, like praise from your Customers and CERIAS.

Some Tools

- RockSoft carries the commercial version of Veracity for Windows®. Veracity http://www.rocksoft.com/rocksoft/veracity.shtml a great Integrity and Audit tool for Windows® Customers.
- 3COM has new NIC's that can be preconfigured to protect host networks. http://www.3com.com/corpinfo/en_US/pressbox/press_release.jsp?INFO_ID=2002706
- Tiny Firewall http://www.tinysoftware.com , my favorite, it's never failed and if it did while I wasn't there I'm sure of the "fail to" state. Nmap, queso and a myriad of other programs have failed to elicit a response from Tiny after tens of thousands of tries on my Win98 based pc at home.
- ZoneAlarm http://www.zonelabs.com (made the GIAC detects page recently. Don't let that stop you from evaluating it it's a great program).
- Sphinx http://www.biodata.com reads like a great program.

Sources

1. **Covert Shells,** J. Christian Smith, November 12, 2000 **Information Security Reading Room,** © 2000, The SANS Institute

2. **Consensus Roadmap for Defeating Distributed Denial of Service Attacks**, A Project of the Partnership for Critical Infrastructure Security, Version 1.10 - February 23, 2000**, Prepared for the Partnership By:CERT/CC at Carnegie Mellon University (Rich Pethia*), The SANS Institute (Alan Paller*), and The Center for Education & Research in Information Assurance & Security (CERIAS) at Purdue University (Gene Spafford*)

3. "**Site Security Standards: Security Incident Handling Liability Warning,** Network Working Group, B. Fraser, Request for Comments: 2196 Editor FYI: 8 SEI/CMU Obsoletes: 1244 September 1997 Category: Informational. http://www.ietf.org/rfc/rfc2196.txt?number=2196

4. **AICPA/CICA SysTrust™** Principles and Criteria for Systems Reliability Version 2.0 "Copyright © 2000 by American Institute of Certified Public Accountants, Inc. and Canadian Institute of Chartered Accountants. Used with permission."

References

CoBIT, 3rd edition, 6 sections, July, 2000, Released by the CoBIT Steering Committee and the IT Governance Institute.

GAO Accounting and Information Management Division, Federal Information System Controls Audit Manual, January 1999

NIST Generally Accepted Principles and Practices for Securing Information Technology Systems, Marianne Swanson and Barbara Guttman, September 1996

Computer Security, Edward A. Roback, August 2000, NIST Guidelines to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products.

MINIMUM SECURITY REQUIREMENTS FOR MULTI-USER OPERATING SYSTEMS, NISTIR 5153, March 1993, Computer Security Division, Computer Systems Laboratory, National Institute of Standards and Technology, A Protection Profile for the U.S. Information Security Standard, National Institute of Standards and Technology, Gaithersburg, MD.

Exposure Draft, AICPA/CICA, SysTrust™ Principles and Criteria for Systems Reliability, Version 2.0, Copyright © 2000 by American Institute of Certified Public Accountants, Inc. and Canadian Institute of Chartered Accountants. Permission is granted to make copies of this work provided that such copies are for personal, intraorganizational, or educational use only and are not sold or disseminated and provided further that each copy bears the following credit line: "Copyright © 2000 by American Institute of Certified Public Accountants, Inc. and Canadian Institute of Chartered Accountants. Used with permission."

ZoneAlarm TrueVector Technology White Paper, PC-based Internet Traffic Monitoring, 2000 Zone Labs, Inc. Available on their website.

Defense In-depth, White Paper, Michael Howard / January 23, 2001, Using IPSec effectively in Windows 2000.

Guest Feature: Cautionary Tales: Stealth Coordinated Attack , by Dragos Ruiu dr@netsentry.net
Article originally published in Digital Mogul Volume 2-7, July, 1999.

MD5 Homepage (unofficial)
http://userpages.umbc.edu/~mabzug1/cs/md5/md5.html
MD5 was developed by Professor Ronald L. Rivest of MIT