The Internet Rules but the Emperor Has No Clothes

Abstract

Today's Internet is a virtually free resource. Its existence is based upon end-users freely communicating in an open environment. However, this free and open environment does not imply any value beyond the ability to communicate. Thus most of the information currently being exchanged is not deemed "valuable" in the business sense. However, as more and more business-related information is made available on the Internet, the exposure of that information to unauthorized disclosure or modification becomes a real issue. What a competitor or opponent may discern to be of value establishes a threat to any non-trivial communication. Opponents can decide what information is valuable to them whether or not the owner recognizes the threat.

The crowning achievement in the Internet is the complete, wide open interconnection between information resources and end-users. Yet it is this very interconnection which renders the Internet an unsuitable repository for valuable information. To use an analogy from the familiar tale, "The Emperor's New Clothes," the Internet/Emperor is well connected, but he apparently does not recognize the need for security/clothes. There is no lack of solutions to this distressing situation: adequate technology exists to clothe the Emperor, but many tailors are idle. One can only hope that customers will demand, and that vendors will produce, an abundant number of secure solutions.

Implications of a Wide Open Internet

In light of the voluminous discussion surrounding the growth of the Internet, it is easy to recognize a growing dependency on the Internet. Yet businesses have been reluctant to embrace the real value of Internet communication: electronic commerce. The lack of effective computer security on the Internet is a primary force inhibiting the implementation of information technologies in today's business environment. In particular, there is no rapid growth of electronic commerce. The lack of trust surrounding security for Internet applications is forestalling what otherwise might be significant progress toward electronic commerce.

In contrast to what is occurring on the public Internet, more and more corporations are storing valuable electronic documents and transactions on local area networks (LANs). Many are even setting up corporate "intranets" for easy internal access to information. The corporate information being stored on and exchanged over these private and semi-private computer networks is increasingly valuable. As with Internet connections, increased levels of connectivity bring increased risk and vulnerability, even to LAN-based information. Primarily, the risks and threats come in the form of attacks by maliciously inclined users or actively malicious software.

When It Pays to Be Hostile

When asked to identify the primary threat to the security of networked computer systems, many people point the finger at high school aged "hackers" armed with personal computers and modems. But amateurs who try to break into your system for the fun of it don't pose nearly as much threat as dedicated individuals and groups motivated by the prospect of financial gain. The commercial value of the intellectual property (products and trade secrets) that will become available electronically will provide a strong motivation for new classes of attackers. As the value of the information stored on information systems increases, so does the threat of deliberate, malicious attacks on those systems. Some of these attacks will undoubtedly originate with agents external to the organizations that own and use the networked systems and resources.

To safeguard valuable information against malicious attacks, there is a growing need for both hardware- and software-based protections that prevent any unauthorized monitoring, modification, or disruption of a company's computer activities.

When Software Is Malicious

In a distributed computing environment, there is significant opportunity for malicious software to intervene between user and data, thus subverting the intent of well-meaning users. For example, such software could be introduced as an authorized user gains access to intellectual property such as a computer program or entertainment product. The intruding software could then transmit the program to a third party, thus undermining the integrity of the licensing transaction and making it impossible to tell exactly who has gained access to the information and what actions an individual actually took and is accountable for.
Malicious software of this sort is known as a “Trojan Horse.” It is characterized by the fact that it is present without the knowledge of the system’s user and performs functions that the user did not desire, expect, or intend. Certain computer viruses that have received a great deal of publicity and caused noticeable damage to personal computers are unsophisticated forms of Trojan Horses. In networked environments where information is shared and communicated over wide areas, Trojan Horses are easily distributed and have ample opportunity to cause harm.

When Indirect Access Is Easy

Users of unprotected computer systems and networks will prove easy prey to those seeking unauthorized and uncompensated access to information. The legitimate purchasers of intellectual property may serve as unwitting conduits through which hostile software is able to receive intellectual property and forward it on for further unauthorized and uncompensated distribution. Traditional protections such as physical isolation and manual review of information before release will prove largely ineffective against such attacks. It is nearly impossible to physically isolate data when pervasive interconnection is the basis of commercial activities, and when most electronic information is being distributed in a form that is not readable by humans.

Accountability: Who Is That User?

Processing valuable information requires levels of accountability commensurate with the value of the information. Yet the perceived value of real accountability is often misunderstood because it is considered an auditing function. This is inherently insufficient because auditing is a post facto activity. What’s more, without a truly secure audit mechanism, the audit data may not be reliable. Thus reliance on computer-generated identification can cause erroneous accountability. The misunderstanding can occur because it is people who make decisions, yet it is hardware and software that are processing and recording activity.

Businesses require accountability at the level of the individual. In an environment such as the Internet that is fraught with malicious users and malicious software, it is vital to ensure that only an authorized individual’s decisions are reliably carried out by the software. Historically, businesses protected their data by keeping it in a centralized “fortress” and instituting strict access policies overseen by security administrators to permit access only to authorized individuals. Currently, the Internet does not have adequate electronic mechanisms to replicate these access control procedures, rendering it impossible to assign individual responsibility from the computer. Still, the only way to be sure of a user’s identity is to provide adequate hardware and software mechanisms as to assure an acceptable level of identification. Verifying the identity of an authorized individual is therefore the first issue.

Qualifying Identification

Most computer identification processes verify a user’s identity by asking for some secret, such as a password, which the computer has knowledge of and which only the user should know. This verification step is often referred to as “authentication” or authenticating the user ID. There are many different practices in place today for acquiring the user’s identification secret. Some of these processes are discernibly better at keeping the user’s secret from other users, administrators, or opponents on the network. Yet the typical user is not aware of the inherent risks involved in revealing the user secret, and many system administrators are not familiar with the unsecured authentication practices commonly used to log in to the Internet.

Accountability: Who Is That User?

Processing valuable information requires levels of accountability commensurate with the value of the information. Yet the perceived value of real accountability is often misunderstood because it is considered an auditing function. This is inherently insufficient because auditing is a post facto activity. What’s more, without a truly secure audit mechanism, the audit data may not be reliable. Thus reliance on computer-generated identification can cause erroneous accountability. The misunderstanding can occur because it is people who make decisions, yet it is hardware and software that are processing and recording activity.

Businesses require accountability at the level of the individual. In an environment such as the Internet that is fraught with malicious users and malicious software, it is vital to ensure that only an authorized individual’s decisions are reliably carried out by the software. Historically, businesses protected their data by keeping it in a centralized “fortress” and instituting strict access policies overseen by security administrators to permit access only to authorized individuals. Currently, the Internet does not have adequate electronic mechanisms to replicate these access control procedures, rendering it impossible to assign individual responsibility from the computer. Still, the only way to be sure of a user’s identity is to provide adequate hardware and software mechanisms as to assure an acceptable level of identification. Verifying the identity of an authorized individual is therefore the first issue.

Qualifying Identification

Most computer identification processes verify a user’s identity by asking for some secret, such as a password, which the computer has knowledge of and which only the user should know. This verification step is often referred to as “authentication” or authenticating the user ID. There are many different practices in place today for acquiring the user’s identification secret. Some of these processes are discernibly better at keeping the user’s secret from other users, administrators, or opponents on the network. Yet the typical user is not aware of the inherent risks involved in revealing the user secret, and many system administrators are not familiar with the unsecured authentication practices commonly used to log in to the Internet.

One acute example of unsecured identification and authentication is the TelNet session. In TelNet, passwords are sent across the wire “in the clear” with no cryptographic constraint. Without the ability to inspect what is actually being transmitted on the wire, the user is not frequently aware of the problem. Any opponent with a protocol analyzer or comparable software or intervening computers in the Internet would be able to capture the passwords, providing ample opportunity for the opponent to assume an authorized user’s identity and launch an attack.

Graded Authentication

In an interconnected environment, end-users typically have the opportunity to log in and access network resources from any location at any time. This ability exists even if the user does not always access network resources from remote locations using the same hardware, operating system, or protocols. Thus the variables underlying an actual authentication process may change for a given user from login to login. Recognizing this leads to the invaluable observation that not all authentications are equal. The quality of an end-user’s authentication as well as the inherent trust given to the end-user’s actual, nondisputable identity only diminishes as less secure
methods of authentication are applied in subsequent sessions.

The various authentication processes that exist today show the need for a graded quality of authentication. Ultimately, a graded authentication provides a more realistic picture of how “good” the original authentication was when performed, and gives an indication as to the trustworthiness of any subsequent login. Recognizing that there are observable grades of authentication, it becomes necessary to grade end-user authentication for the purpose of granting access. When there are levels of sensitivity associated with network information, these levels can correspond to the amount of trust in a graded authentication process. Certainly end-users who transmit login passwords over the network in a clear and decipherable manner should not be given the same grade for current or subsequently authenticated status as end-users who operate from secure equipment in an approved manner.

Although the term “graded authentication” is new, the mechanisms for implementing it are those of the familiar and mature technology for what is commonly known as mandatory access control (MAC). MAC associates a label with a user session in this case, the label is the grade of the authentication, and a corresponding label on information in the network indicates what is accessible with that authentication. In short, graded authentication corresponds to those factors which influence the verifiability of an end-user’s identity as that user comes onto the network.

**Cryptography Is No Magic Pill**

The ability to use strong encryption is essential to the success of the global information infrastructure. When implemented and managed by trusted computer systems, encryption is a known technology that has been demonstrated to work. Yet there are many weak cryptographic implementations where the intended protection can be easily compromised. For example, a weak cryptographic implementation might create a digitally correct authentication package, yet allow identification secrets to be “leaked” before, during, or after the process. An untrusted authentication undermines any further trust in the integrity of subsequent transactions and makes it impossible to tell what actions an individual actually took.

Malicious software can leak authentication secrets or cryptographic keys, thus subverting confidentiality and undermining the security of a user or system. Such leakage is especially devastating since users are likely to assume that their actions are “secure” because they are “protected” by encryption. Clearly, there must be a division between trusted and untrusted, where the reliable part of the system is controlled by trusted software. This is the essential quality of the Trusted Computing Boundary (TCB) in the operating system.

**Strength of Authenticity**

As long as weak authentication (such as passwords being transmitted in the clear or passwords that can be acquired) is used, all accountability for a given user is lost. No subsequent transaction data can be reliably attributed to the user. The grade of the authentication must reflect the overall confidence in the authenticity of the user’s identity not just the strength of the cryptography used.

**The Trusted Path: Acquiring the Application**

Having a fail-safe process to confirm the user’s identity is vital, especially in the business environment where valuable information is exchanged. However, there is more to network security than just identification and authentication. Many people, like our fictitious Emperor, believe that the Internet has clothes on and looks sharp. But they are ignoring the basic concept of precedence in dressing: underclothing comes before outerwear.

Obtaining user accountability the point of bullet-proof authentication extends beyond identification and authentication (I&A). If user accountability is to be maintained, we must understand where users get their application software and use this as a prerequisite to control. The previous discussion of identification and authentication during the login process brought us to the point of obtaining some level of assurance in knowing who was in the session. In this next step, where and how the users get their software has direct implication to the reliability of the software in carrying out the users’ intentions. Since the software will act with the user’s authority, it is important to know the path along which the software has traveled to the end-user. The persistent threats of injected malicious software such as Trojan Horses cannot be ignored.

**Trusted Path for Session Authentication**

Every business-related action executed on a computer should be attributable to that user at the end of a session. This implies trusted identification throughout the session. The need for individual accountability is equally great whether the activity involves the transfer of cash, the filing of a document
mechanism for adequate identification of the individual is well within the capability of current technology. However, assuring that the identification mechanism, as well as the trusted path and evaluated software, have been properly implemented is another matter. Vendors must cooperate in independent third-party evaluations.

Evaluation

Neither users nor administrators can judge what software does once it is running on the machine. All parties need to be able to trust the software they are running, not just take it on blind faith that the software vendor has done a good job. Providing the mechanism for adequate identification of the individual is well within the capability of current technology. However, assuring that the identification mechanism, as well as the trusted path and evaluated software, have been properly implemented is another matter. Vendors must cooperate in independent third-party evaluations.

Beyond the initial trusted session authentication is the step of maintaining session accountability. The software vendor has done a good job. Providing the software does once it is running on the machine. All parties need to be able to trust the software they are running, not just take it on blind faith that the software vendor has done a good job. Providing the mechanism for adequate identification of the individual is well within the capability of current technology. However, assuring that the identification mechanism, as well as the trusted path and evaluated software, have been properly implemented is another matter. Vendors must cooperate in independent third-party evaluations.

Beyond the initial trusted session authentication is the step of maintaining session accountability. The software vendor has done a good job. Providing the software does once it is running on the machine. All parties need to be able to trust the software they are running, not just take it on blind faith that the software vendor has done a good job. Providing the mechanism for adequate identification of the individual is well within the capability of current technology. However, assuring that the identification mechanism, as well as the trusted path and evaluated software, have been properly implemented is another matter. Vendors must cooperate in independent third-party evaluations.

Trusted Software Path for Transactions

You cannot hold a machine or a program responsible in a business transaction; only people can be held accountable for actions. For accountability to work, the computer user must remain reliably identified. With a fail-safe process to confirm the user’s identity, and with a trusted path through which we will obtain the software and deposit the final results, we can proceed to the third point of application transaction processing for Internet commerce: examination of the software. This is a necessary step since the software will act with the user’s authority. In this step, we scrutinize the available product for any inadequacies or malicious intent. For example, consider the consequences of the following situation: From a networked computer, a user authorizes a cash transfer from his company’s bank to another institution. The user types in $500 as the amount to be transferred. After verifying this is the amount displayed on the screen, the user sends the transaction. When the recipient receives the transaction, it indicates $5000 has been transferred.

This scenario demonstrates that without a trusted path for the transaction to travel from the user’s input to the transaction end-point, there is no way of knowing what is going to go out across the wire. Clearly, what the screen displays does not have to be the same as the transaction contents stored in the memory register. What the user needs is a certainty on the transaction contents. This requires a mechanism whereby the user can receive confirmation that the transaction contents are, in fact, what the user entered. This requirement dictates hardware support for a trusted path between the user and the content verification of the transaction. At the point where the user is ready to send the transaction, a hardware-enabled switch is activated, giving the user a trusted path to the trusted computing base. The transaction contents from the application software are read from an area in memory, and the trusted software displays the contents to the user from the trusted area. If the contents are not correct, the user has the option to abort the transaction. If the user validates the contents as correct, the transaction amounts are sealed from the trusted computing base, at which point they can be transmitted. (This is essentially the Class B3 level requirement.)

This is different from a bank teller using dedicated hardware and software in a specific application since it offers the flexibility to use untrusted software and software which has not been evaluated for the application. This is a significantly greater requirement than the session reliability of Class B2. It imposes a
higher level of difficulty to obtain since it requires special hardware and a trusted path to the TCB.

**Trusted Distribution**

To obtain real accountability, it is a prerequisite to know where and how sensitive applications, as well as information, have been stored. A trusted directory service is therefore required to perform commercial operations in the Internet environment. If application software is subject to subversion in any form (alteration, substitution, or elimination), end-user accountability is not real. Thus, the path along which a computer system allows for the introduction of software modules, such as Java applets, is important since substitution, or the ability to claim alteration, invalidates any real accountability.

Without knowledge of where the modules come from, whose modules they really are, and what they will actually do, there cannot be any evidence pointing back to the user; and thus the user is not responsible. If the application calls or accepts modules or substitutes modules from without, the results can hardly be attributed to the user. This requirement delineates a requirement for a trusted path along which software operates. This path starts at the user for the acquisition of application software and extends to the deposition of the final results.

This requirement imposes the need for authenticity credentials belonging to software and software modules, as well as the need for having an authenticated location for obtaining software. Recent occurrences, such as the take-over of the Department of Justice Web site, tend to confirm the reality of this need for authentic locations. Even trade magazine articles depict the need for authenticated applets coming from Web sites.

What you need in the machine is an authentication for the software (or data) you download. It should irrefutably say which vendor it came from. This requirement imposes on distributors the need for trusted storage area accessed by authorized individuals, as well as for producing a properly credentialed piece of software. To give users the ability to authenticate both locations and software requires a trusted directory service with a built-in public key infrastructure which users can rely upon. Such a directory service could be used to obtain authenticated access information for both software location and software authenticity. Without this type of infrastructure, running commercial applications on the Internet is not viable.

Clearly, the software and hardware involved in electronic commerce must be reliable, even in the face of malicious intent. When the software integrity is inviolable, accountability falls unquestionably on the user who performs the transaction, and businesses have due recourse in the event of error or loss. Thus, at the very minimum, obtaining accountability for a user’s actions requires two things:

1. A reliably identified user who can substantiate his or her identity (individual accountability)

2. Some form of isolated and protected software (independently evaluated) performing the authentication as well as maintaining the essential elements of accountability

The issues of legal liability and concerns for sufficient evidence are important. If the user can show that someone else could provide his or her computer identity, the user cannot be held accountable. Likewise, if malicious software could intervene somewhere along the transaction path from sender to receiver, the traceable responsibility back to the user is no longer valid, and true electronic commerce is not viable.

**Consumer Responsibility**

It is important that the community of customers, including individuals, managers, and policy-makers, understand the threats to the confidentiality and integrity of their information, as well as the limitations of most currently available countermeasures. One valuable tool is a clear understanding of the benefits of independent product evaluation, the appropriate choices of evaluation class for specific applications, and the ways in which evaluated products interact and interoperate. Industry has the technology to build any evaluation class, from the lower ones commonly available to the highest ones defined. But affordable, significantly improved commercial products will become widely available only in response to market forces when customers make this a significant purchase criteria.

Existing government standards offer some of this information, but they are not yet widely enough known or applied outside (or even inside) government to form a dominant marketing force to drive major security development for commercial products. This sort of information would be of use to system designers and integrators who would use it to select and configure products. It would also support customers who would use it to guide their decisions as to which systems should be allowed to process their sensitive data.
There Are No Quick Fixes

Although powerful security technology for distributed environments exists, failure to recognize the need for evaluated products and the quick fix allure in hope of some new, effortless solution continues to impede the market forces that would otherwise lead to the effective incorporation of real solutions into commercial off-the-shelf (COTS) products. Firewalls are a good example of the quick fix. Despite repeated demonstration of their ineffectiveness, organizations continue to put them up. They do not work against the hostile adversary, as evidenced by repeated break-ins.

Another in the quick fix category of solutions is the persistent belief in the "penetrate and patch" approach. This approach proposes that meaningful security can be provided against the growing hostile threat by having "experts" try to penetrate the security controls, and then patch the holes found. This is a fundamentally flawed myth, especially in the face of malicious software. The practical problem is that the defender needs to find essentially all the holes while the attacker only needs to find one. This is a seriously unbalanced game of wits in favor of the attacker. Instead, a sound basis for systematic security evaluation is essential.

Evaluation or Emphatic Assertion

In the government arena, the terms "product evaluation" and "assurance" have long been used in association with computer security to describe the results of technically based processes that assess security products' feature content and the level of quality or reliability of their construction. These processes compare products' security features, chosen by vendors to meet the needs of their users, with a list of fundamental computer or network security functions. They also assess the conditions of products' construction to evaluate the likelihood that the security features are correct and complete. Most major operating system vendors have committed to obtaining U.S. and European evaluations of network and operating system products. Technically-based product security evaluation by independent, objective third parties offers users significant value compared with simple vendor claims in terms of assurance of the quality of security features and their implementation. While the public at large, and computer and network users in particular, are largely unfamiliar with such formal processes, this is changing.

Conclusion

Security is a barrier to entering the "promised" empire of the Internet: electronic commerce. The Emperor has no clothes, and he still hasn't woken up to that fact. What's worse, his selected (but fraudulent) tailors are still hawking their ineffective wares. The careful will seek other tailors who are offering real clothes with instructions on how to wear them. These offerings include graded authentication, cryptography under TCB control, trusted path to user at workstation, trusted directory for distribution of information and software, and cooperating with independent evaluators. Novell has actively pursued development in all of these areas. The products we offer represent carefully planned steps along a path of systematic improvements in security for our customers.