Global Information Assurance Certification Paper

The Challenges of Centralized Identity and Access Management and an Overview of the eTrust™ Identity and Access Management Suite

John Lyssikatos
GSEC Practical, v1.4b, Option-1
April 06, 2004

Table of Contents

Abstract

The security management requirements of the modern day computing enterprise are daunting. The effort needed to manage user identities and resources across the enterprise while ensuring proper user access and protection of data is quickly becoming a protracted effort at best. This paper will discuss many of the challenges to centralized identity and access management in today's computing enterprises.

Additionally, an overview will be given of one vendor's solution to this problem as offered by the eTrust™ Identity and Access Management Suite created by Computer Associates®. The eTrust™ Identity and Access Management Suite is actually a combination of six of the products within the eTrust™ family. The actual products are as follows: eTrust™ Admin, eTrust™ Access Control, eTrust™ Web Access Control, eTrust™ Single Sign on, eTrust™ Directory, and eTrust™ Audit.[1]

Security Challenges

Centralized administration of user identities and company resources is quickly becoming the mantra, if not the mandate, of senior management within most organizations. A litany of factors are coming together to produce an environment where the challenges are simply too overwhelming for traditional methods of identity and access management. Listed below are various areas of identity and access management that system administrators, information security personnel, auditors and senior management are faced with on a daily basis:

Provide ubiquitous access to customers:

The dot.com boom may have gone bust but the layman's interest in the Internet did not. Whether it's requesting a stock quote, filling a prescription, booking a vacation, managing one's bank account, ordering the latest bestseller or participating in an online auction, customers are demanding to be able to access the services and procure the products that they want, when they want and from wherever they are. Oh, and did I mention that they want the transaction to be fast, secure, reliable and of course, with as little imposition on themselves as possible?

Provide secure and reliable access to vendors and business partners:

The client who purchases one hundred shares of the latest hot stock on margin from his online trading broker and also simultaneously shorted another hundred shares of an unknown company that he just got a tip from in a chat room, is probably unaware of the myriad of tasks that occur behind the scenes between numerous business partners, and the client most likely doesn't care, nor should he/she.

Here's a glimpse at the high level tasks involved in processing this customer's request:

[1] http://www3.ca.com/Files/Brochures/etrust_iam_brochure.pdf

1. Route the order from the web application to the brokerage company's workflow engine.
2. Verify the account information and standing.
3. Verify the requested stocks transferability status, which is done via a data feed from another business partner.
4. Route the request to the margin department.
5. Route the request to the purchase and sales department.
6. Route the request to the order desk.
7. Repeat some or all of these preceding tasks if the brokerage company routes their order through a clearing-house.
8. Route the order to the proper exchange.
9. Execute the trade.
10. Return the confirmation message from the exchange to the originating customer (either directly and via the clearing-house).
11. Handle any exceptions along the way and notify the customer if there is a problem in processing the request.
12. Send the customer a printed confirmation of the trade with the details of the transaction.

This listing is not meant to be a tutorial in trade processing but rather an illustration of the complexity of processing what, in the customer's mind, is a simple request. The details of the process may change from firm to firm, but the challenges are the same. Process a request from what is almost always an untrusted endpoint (who is really at the other end of this request and where is it coming from?).

The request process will probably pass from one or more distributed platforms to a mainframe or AS/400. Various data feeds are needed to provide all those quotes, charts, analyst reports and stock information in addition to actually processing the trade request. It's probable that some sort of middleware for messaging and queuing is also being used.

The session management and auditing requirements for such systems are extremely demanding. Organizations today, simply must be able to determine: who is accessing their corporate resources and what do they have access to? Meanwhile, customer's demand instant access to their data and generally don't want to hear about security concerns, at least not until something goes wrong.

Which brings us to non-repudiation. While cryptography is not a focus of this paper, it is implicitly tied with establishing user identity and when implemented properly, can be used to legally obligate a person to the conditions of a transaction.[2] If we recall our example of a customer's request to buy and sell some stock, it's not uncommon for one side of a transaction to try to either deny participating in the transaction altogether, or attempt to alter the conditions of the transaction when things don't go as hoped, "I didn't say buy, I said sell".

[2] http://www.yourwindow.to/information-security/gl_nonrepudiation.htm

Ultimately, these challenges, and the responsibility to meet them fall upon the organization providing the product and/or service and their affiliated partners and suppliers. Sensitive financial and personal customer information is being passed between several business partners and the customer. The legal system demands that the integrity and confidentiality of this transaction and its data be preserved. For instance, one provision of the Gramm-Leach-Bliley Act requires banks to protect customer privacy and prove it.[3]

The potential revenue from such arrangements between business partners and vendors are tremendous as are the consequences and damages to these firms if they fail to ensure that only authorized users and system requests are processed correctly. The marketplace can be most unforgiving to businesses that are unable to protect their customer's data and personal information.

Additionally, business partners need to be certain that orders received from another partner are legitimate. Did John Q. Public really just short 1,000,000 shares of stock ABC? Processing false orders can be just as damaging if not worse than mishandling a legitimate customer order or exposing their data.

Heterogeneous environments:

The days of a centralized computing facility with company associates connecting exclusively through dumb terminals are long gone. True, one can still find many dumb terminals (or at least terminal emulator programs) still reliably performing today, in specific roles, but the computing needs of even many small companies demands an amalgamation of information systems. Most corporations today have to contend with operating and integrating email, file and print services, web services, payroll and accounting systems, supply chain management systems, customer relationship management systems, human resources systems, intranets, as well as a variety of security systems such as firewalls, intrusion detection systems and auditing systems to name a few. Don't forget of course all of the networking devices that enable all of these systems to work together.

Even the realm of the desktop operating system can be challenging. Many companies will maintain multiple versions of the Microsoft® Windows operating system, which in of itself can present integration challenges. Additionally, graphics departments often use Macs while web application developers frequently perform their daily duties on some flavor of Unix workstation. Mobile computing has also complicated the mix with wireless laptops, PDAs, mobile phones and other mobile devices. I'm sure that the strategic vision for many IT departments may speak to standardizing on a particular platform but in reality, such goals are usually untenable.

[3] http://www.tripwire.com/files/literature/white_papers/GLB_OCC_White_Paper.pdf

Business requirements principally drive the makeup of a corporation's information technology and consequently most organizations will have to live with Java and .NET, IIS and Apache, and a variety of both databases and application servers. Additionally, with the advent of many open source products making their way into the enterprise, the problems of heterogeneity have gotten worse, not better.

User-ids:

Now for the really challenging part of identity management: it's most likely that each of these systems has it's own facility for creating and managing user-ids and defining the entitlements to its resources. These are, after all, systems that are made to stand on their own. So, now the typical user has a desktop (LAN-id), an email-id, a database-id, a mainframe-id (I'll get to legacy systems a little bit later), and depending on their responsibilities, may also have user-ids for the payroll systems, human resource systems, and supply chain systems. Others will also have access to security systems, facilities management systems, network management systems, telephony systems and the list goes on.

Do all of the various platforms in your company use a consistent naming convention in the creation of their user-ids? It's possible but I wouldn't bet on it. The speed of change in the modern world is almost blinding. Six years ago few companies, especially traditional "brick and mortar" companies, had any significant presence on the Internet, if any. Today, it's almost unthinkable not to have a high quality portal into your organization on the Internet, even if there is no intention to sell your product through the web.

The need to provide information about a company's products and services to customers and investors (existing or potential) is extremely important. For instance, I doubt that anyone can actually buy the GE90 jet engine through the General Electric Aircraft Engines website[4] but this page does provide valuable information for potential customers and investors.

I'm confident that some organizations have been able to implement a naming convention for all user-ids that is consistent across their enterprise. These organizations should be commended, as this is not an easy task. It requires defining and enforcing a naming convention across all enterprise platforms, not just at policy inception but indefinitely thereafter. This is not just a technical problem, but a political one as well.

On the technical side, the questions regarding user-id naming convention may be greater than initially thought.

- What are the minimum and maximum number of characters that a user-id can have? – Remember, you're establishing an enterprise-naming

[4] http://www.geae.com/engines/commercial/ge90/index.html

standard so this policy will need to be enforceable on all platforms. For instance:
    - Windows® 2000 permits logon names of up to 20 alphanumeric characters[5]
    - Solaris™ 7 permits login names of up to 8 alphanumeric characters[6]
- What types of characters are permitted? Are there are constraints?
    - Windows® permits logon names with any combination of upper and lower case alphanumeric characters except for "/\[ ] ;:|| = . + * ? < >[7]
    - Solaris™ 7 strictly requires only upper and lower case alphanumeric characters. Additionally, the first character must be a letter, and at least one character must be a lowercase letter[8]
- What about everyone's favorite, first initial of first name + last name? It's easy to remember but with the onset of the global economy and global, virtual teams within the enterprise, here are some questions to consider:
    - How will you handle associates with very long names that will probably exceed the limits on user-id length?
    - Some cultures have reverse naming conventions from the west, whereby last names precede first names. How will these be addressed? Will you honor their tradition and treat their last name as their first and their first name as their last?
    - Additionally, some people have such lengthy names that these associates will often choose to be referred to by their first name only, or with an abbreviation of their first and last names. Will you let the user decide on the abbreviated names? There can be political ramifications of permitting such users to choose their user-id. Invariably someone will complain and demand to customize their own user-id. Perhaps you will simply use the first x number of characters?
    - Still other cultures have traditions of honoring previous generations of their family by having four, five or even six or more names. Can administrators and policy writers in North America casually dismiss traditions of associates in these countries? Is there a rule that can be applied as to which names should be used?
    - How will hyphenated names be treated?
    - How will you treat duplicate names? Do you add an incrementing suffix to the duplicates names? Ex. jdoe1, jdoe2, jdoe3, etc.
    - What if the duplicate name fills up the user-id and prevents the addition of a numeric suffix? For example, if we had a limit of 10 characters, how would you handle John Associate and Joe Associate as both would have the user-id of jassociate?
    - How will you handle changes in an associate's name? Typically this is associated with a change in marital status. Human resources

[5] Komar, p.284
[6] Calkins, p.183
[7] Komar, p.284
[8] Calkins, p.183

may record and track an associate with one name while the associate continues to use the pre-existing user-ids. Ex. Jane Doe in the HR system is actually identified as Jane Smith (user-id = jsmith) in the corporate information systems.

- How will you handle associates who use their middle name in lieu of their first name? For instance, J. Quincy Public
- Does a user-id that provides an indication of both the associate and their department, make sense in your environment? There are some pros and cons with this approach.
    - Managers, administrators, security personnel, auditors or anyone else responsible for ensuring that only authorized personnel access the appropriate resources can easily identify users who are clearly out of their area of responsibility. For instance, if John Doe (irajdoe) worked in the IRA department, and he was accessing the payroll systems, his activity will probably be noticed more easily either in real time monitoring or via an audit of logged activity in the payroll system than if his user-id was jdoe. This is obviously a pro.
    - With a limited number of characters making up user-ids, (whether via a technical limitation or a practical one), including characters to identify the associate's affiliated department increases the likelihood of duplicate names over the first initial of first name + last name naming convention. For example: if these three individuals worked in the IRA department, John Gallagher, James Galante, and Jared Galioto, they would all by default get the same user-id of irajgal. As you can see, duplicate user-ids can easily be a problem.
    - Another drawback of this naming convention is when an associate changes departments. Perhaps within a period of five years our associate John Doe of the IRA department has moved onto the Margin department and after a two-year stint there, maybe he's even finagled his way into the payroll department that he was trying to break into only five years earlier. How will you handle the reassignment of an associate to another department? Either you will have to issue a new user-id and transfer the user's entitlements to all their resources appropriately (which can end up being a considerable amount of work and is subject to errors), or you can permit the associate to continue to function with their previous user-id and simply add any new entitlements required with the new position (another reason why many associates who have a name change frequently end up having a user-id that does not match their current name). But what about all those entitlements that the associate no longer needs? Hmmm, a good question, one that will be addressed when we look at the eTrust™ Identity and Access Management Suite later on.
- One reason in favor of not using the first letter of the first name + last name for user-ids is that these are probably the easiest for would be imposters to guess. Does your organization have a security policy that

prevents the user-id of the last person logged into a windows desktop to be displayed at login, in order to make it more difficult for unauthorized personnel to guess valid internal user-ids? If you've embraced the naming convention of first letter of the first name + last name, then this policy can be very easily defeated. It also has another drawback in that it prevents legitimate users from seeing whom the last person was who logged into their workstation. Besides, I would pose the question, who are these unauthorized people who are trying to login into workstations inside your organization? If you work in the corporate world, physical access to work areas are becoming increasingly controlled. If you're a sales clerk in a department store, then such a precaution makes more sense.

- How will you handle senior management people who ask for user-ids that do not conform to existing naming standards? When the CEO asks that his user-id be Bob, what do you say? Probably, yes sir. While I did briefly mention the fact that user-id naming standards can also be political, it's when we get to the next topic of password policies that the perks we give to senior management becomes problematic.

Password policies:

Dare I say anymore? If this topic doesn't spark a debate within your organization, nothing will. End users don't want any and the most paranoid security mavens will cry for three-factor authentication, which is fine for nuclear launch codes but not very practical to run a business, let alone satisfy customers. If I can take some literary license with Kipling's The Ballad of East and West, somewhere in between the twain shall meet[9], but where? That's the $64,000 question.

The challenges of establishing a standardized password policy across the various platforms in an organization's enterprise are far more difficult than those that were discussed regarding user-ids. The whole point of implementing passwords is to help ensure that the right people can access the data to which they are entitled to, nothing more and also nothing less. Yes, strictly speaking passwords are a function of authentication, but indirectly they enable the authorization process. You wouldn't think about proceeding with providing a user access to a resource without a high level of certainty as to the user's identity.

It's just like conducting business with a bank: you would not want security that is so strong that it becomes impossible for you to withdraw your money. Likewise, you probably wouldn't trust your money to a bank that just blindly accepted the identity claims of anyone who walked up to a teller and ignored any sort of verification of both the customer's credentials and their right to access the requested account, even if it was a known customer.

It wasn't too long ago in American history that incidents of a spouse emptying out the savings account of the other without their knowledge or permission were

[9] http://www.theotherpages.org/poems/kiplin01.html

unfortunately not uncommon. The bank may have conducted authentication (oh hello Mr./Mrs. Public), but in these cases, the authorization process was non-existent. Assumptions were made regarding one spouse's inferred authorization to access the account of their spouse.

Identity and access management systems of today need to protect organizations and the individuals that they serve from such breaches in authorization. Although this story of a bank account being emptied without authorization is essentially a social engineering attack, it is one, that in my opinion, could be well addressed with a combination of not only thorough centralized identity and access control management, but also consistently applying clear, simple security policies, and ensuring that the organization's associates are educated in these policies. It also involves auditing mechanisms and the cleaning up of no longer valid user-ids, profiles and entitlements. Hmmm, sounds like the beginning of defense in depth to me.

So, let's get back to where we started in this section on password policies. Understandably, most users do not want their password to be #zP3vT69*. Nor, can we permit their password to be "password" or even "qwerty". The initial example will undoubtedly be displayed on a post-it affixed to a monitor, or perhaps under a keyboard, and the latter passwords will be virtually instantly compromised. So what requirements do we need to define in creating an effective password policy?

Just as the various platforms in our heterogeneous computing environment have a variety of acceptable character strings and lengths for their user-ids, the rules regarding acceptable passwords for these individual systems are even more varied and difficult to standardize across platforms. Some of the typical parameters and rules applied to password policies across the different platforms an organization's information systems include the following:

- Varying minimum and maximum password lengths
- Varying constraints on the minimum strength or mandatory characters that must be present in a password
- Varying abilities to lock out accounts and whether these accounts can unlock themselves after a specified period of time
- Varying ability to define the length of password histories to be retained
- Varying abilities and definitions of what constitutes a strong password
- Varying constraints on which characters are not permitted in a password
- Varying rules on whether blank passwords are permitted
- Varying limits on the minimum and maximum age of a password
- Varying limits on whether grace logins are permitted and if so, the maximum number of grace logins permitted
- Varying limits on who can reset passwords
- Varying ability for an operating system to force a user to login – think Microsoft® Windows 9x where a user can bypass a login screen by pressing the escape key

- Varying ability for a system to permit a password to never expire
- Varying ability to define acceptable login methods
    - Windows® 2000 includes the ability to prohibit a user from performing a logon locally on a system as well as deny access to a system from the network[10]

So now we've talked about a multitude of parameters associated with password characteristics. One password practice that is gaining popularity that offers considerable strength against non brute force cracking, yet is relatively easy for users to remember is to use the first letter of each word in a phrase. For example, the phrase "April showers bring May flowers" becomes " Asb*Mf ". The asterisk is included for additional security.[11] Of course, you can always have some other conventions that can be easy to remember and strengthen your password acronyms even further.

Here's an example I created: " $fRcLmYe! " (Ignore the quotation marks). By consistently applying the following practices to all of my passwords, I can improve the security thereof even further:

1. Prepending the password with a $ (or any other special character I choose to consistently use)
2. Append a suffix appropriate for the phrase, depending on whether a statement or a question is being used for the passphrase. For instance, end all statements with an exclamation point, or even a period, and ending questions with a question mark.
3. Alternate between lower and upper case letters in the password (or vice-versa). I know, I know, it's a common ploy and easily guessed, by both hackers and password cracking tools. However, given that we're not talking about anything that can appear in a dictionary list, and the fact that even the basic application of using the first letter of each word in a phrase lends itself to secure passwords that are very tough to guess, these measures make it very unlikely that anyone will guess your password before your account is locked out.

If you're interested in trying to crack the above phrase, I'll leave its answer after the References section.

Some final and even heretical thoughts on passwords from Peter Tippett, the executive publisher of Information Security and the CTO of TruSecure Corp. Listed below are some quoted excerpts from an article called "Stronger Passwords Aren't" that Dr. Tippett wrote for Information Security magazine in June 2001.[12] I highly recommend that readers read the actual article for themselves. For the purposes of readability, the quoted excerpts from this article are presented in bullet point format.

---

[10] Komar, p.300
[11] http://www.biology.ualberta.ca/facilities/computing/index.php?Page=2076&Print=Yes
[12] http://infosecuritymag.techtarget.com/articles/june01/columns_executive_view.shtml

- In the real world, an eight-character mixed alphanumeric password is no more secure than a simple four-character password.
- A “strong” password is really no more secure than a “good enough” one.
- Passwords are usually hashed…and stored with corresponding user ids. Hashes are truly one-way functions.
- The reason we’re told to use strong password boils down to this: Someone might steal the password file -- or sniff the wire and capture the user ID/password hash pairs during logon – and run a password-cracking tool on it.
- By using random alphanumeric characters in lengthy strings, strong passwords supposedly thwart these so-called dictionary attacks. But there are at least three problems with this assumption.
    - Strong password policies only work for very small groups of people. In larger companies, they fail miserably.
    - With modern processing power, even strong passwords are no match for current password crackers.
    - Strong passwords are incredibly expensive…The second or third highest cost to help desks is related to resetting forgotten passwords.
- Many recommend augmenting passwords with another form factor, such as biometrics, smart cards, security tokens or digital certificates. But each of these solutions is expensive to deploy and maintain, especially for distributed organizations with heterogeneous platforms.
- For most organizations, we should recognize that 95 percent of our users could use simple (but not basic) passwords – good enough to keep a person (not a password cracker) from guessing it within five attempts while sitting at a keyboard. I’m talking about four or five characters, no names or initials, changed perhaps once a year. Practically speaking, this type of password is equivalent to our current strong passwords…Under this scenario, we could reserve the super-strong passwords for the 5 percent of system administrators who wield a lot of control over many accounts or devices.
- Everyone should make the password files mighty hard to steal. You should also introduce measures to mitigate sniffing, such as network segmentation and desktop automated inventory for sniffers and other tools.
- If the promised land is robust authentication, you can’t get there with passwords alone, no matter how “strong” they are.

As I mentioned, the above points are quoted excerpts from Dr. Tippett’s article that I cited. It breaks with many conventional wisdoms of password security but great ideas are often rejected at first as outlandish. If you don’t think that your organization doesn’t have a significant problem with users forgetting passwords and getting locked out of their systems, I would propose that you speak to your help desk manager. You’ll probably be surprised. If they’re not calling, I would start looking for post-its prominently displayed somewhere in the cubicle, or under a keyboard or even in a drawer.

Legacy systems:

This is another debate that has raged for sometime now, particularly with respect to the mainframe. I'm reminded of a quote from Mark Twain, "The reports of my death have been greatly exaggerated".[13] The dot com prognosticators who predicted the death of the mainframe were obviously wrong. Governments, financial institutions, large corporations and even many medium size corporations rely on the number crunching and data storage and access capabilities of the mainframe.

Additionally, these organizations have invested a tremendous amount of time and money into developing these platforms. The costs of moving off of them, in favor of a new technology, even if it was superior, are, for most organizations simply prohibitive. I don't know if anyone can provide any reliable statistics on the number of lines of COBOL code running today's businesses, but I believe I would be correct to guess that COBOL still reigns supreme as the principle computer language of today's business programs.

That said, organizations cannot ignore the tremendous benefits that distributed computing can bring to both their businesses and their customers. Clearly, the standard web architecture of a web server, an application server and some middleware connecting to various backend systems, has proven extremely powerful and valuable. Given the choice of using a GUI or a green screen, I think we can safely guess what most customers would choose.

Consequently, for those who must develop, administer, support and secure today's computing systems, the challenge of providing a reliable, responsive, and secure solution to customers, while crossing multiple tiers and being able to audit and track at a minimum, significant user actions, if not every event, is non trivial, to say the least. The use of a web portal that seamlessly connects customers to numerous applications and services, some of which are probably being delivered by a business partner or vendor, is becoming commonplace.

Administering user identities and controlling their access in such an environment can quickly become a nightmare and for most organizations, requires separate teams to manage these identities on their respective platforms. The temptation to alleviate this problem by using generic accounts when crossing from the originating platform to another can be very strong. It can also lead to serious financial and legal repercussions when this attempt to ease identity and access control administration burdens results in unauthorized disclosure of customer information, theft, fraud, damaged business reputation and relationships, and a variety of other undesirable actions.

[13] http://www.brainyquote.com/quotes/quotes/m/marktwain141773.html

Endpoints:

This problem was very briefly discussed earlier. Let's take a moment to look at this issue a little further. Typically, organizations will have three types of endpoints:

1) Internal users
2) Extranets – business partners and vendors
3) Customers

So that we don't get caught up in semantics, when I refer to the users as endpoints, I am including the computing devices with which they are connecting to an organization's information systems. The focus of this paper is the challenge of centrally managing user identities and controlling the resources to which they have access. This is not an exploration of how a zombie, or a worm, or any other type of malicious code can infect and propagate throughout a computer network. Although, I would submit that even those problems, can, to some degree, be alleviated through proper identity and access control management. Ultimately, it's users who are accessing an organization's resources and the devices with which they interact are simply tools to facilitate their desired actions. So what about these internal users?

Internal Users:

For obvious reasons, internal users are the easiest challenge to address since the organization has, presumably, total control over the hardware, significant control over any installed software (unless you have Windows® 9x installed) and to some extent, can influence employee actions through published security policies which the employees must acknowledge reading and that provide the organization with the option to dismiss employees for not complying with proper use policies. Some organizations will also conduct background checks as part of the employment process to help ensure that a prospective employee is not a convicted felon or otherwise nefarious sort. Include network and host intrusion detection systems, anti-virus software, firewalls, access control lists on routers, and organizations have a pretty good handle on controlling internal users.

That is not to say that an organization should presume that these endpoints are secure, which is why so many mitigating actions are taken to secure internal access points. Of course, there's always that pesky problem of consultants and vendors who connect their laptops to your internal network and who really knows where those laptops have been? Yes, a policy can be established, prohibiting any non-company maintained computing devices from being attached to the internal network without being first scanned and patched or updated (think virus definitions) as necessary by the desktop support group. A nice idea in theory, but difficult in practice to consistently enforce. Just ask anyone who was asked by a senior manager to provide a visiting VIP or sales rep Internet connectivity two minutes before the meeting is to commence. That said, internal users are still considered "trusted" endpoints.

Extranets:

The next class of untrusted endpoints is the organization's extranets, otherwise known as business partners, and possibly vendors or suppliers as well. These users are probably regarded as semi-trusted. While the organization does not have control over the hardware, software nor even employees at the other end of this relationship, if due diligence has been followed, the organization does have some understanding of the architecture, policies and procedures of their business partners. There is probably some legal agreement between the parties that define their responsibilities to each other as well as their potential recourse if the other party does not honor their obligations.

Additionally, both parties presumably have a common interest, make money. Since such relationships are to varying degrees symbiotic, depending on how attached at the hip these business partners are with each other, organizations hope that their business partners will follow the same due diligence in ensuring the security and reliability of their data and services as themselves. But users will be users, and this particular class of users probably has access to valuable resources within your organization.

In fact, they more than likely have some digital identity within your organization. Sure you may place them in a dedicated user group or container, or perhaps they even have their own domain or directory. Nonetheless, these are user identities that you'll have to manage. Oh, you delegate administration? That's nice, and probably a good thing, but if you're not watching over how your business partner is managing those identities you may be inviting some trouble.

Furthermore, how much do you really know about your business partner's employees? For that matter, how much do you really know about your business partner? You've outsourced some programming work to a friendly off shore consulting company that offered a great price and timetable for delivery. Perhaps you even have a history of many successfully delivered projects.

What do you really know about the internal controls in place to protect your data and resources? What is the employee turnover rate? What is the employee selection process? How well are these employees compensated relative to their peers? Does this company itself hire contractors to perform the work or even sub-contract the work to another party? Is your intellectual property flowing literally out the wire to another competitor or interested party?

We could go on and on of course down this line of reasoning but I think the point is clear: Even in the best of circumstances, an organization should take effective measures to ensure that only authorized users from a business partner are accessing only the resources to which they are permitted and only in accordance with the manner they are entitled. We wouldn't want someone who was only entitled to view pricing information to be able to update it now would we.

In the worst of circumstances, given the privileged level of access the employees of business partners can sometimes have, considerable damage could be done, perhaps even irreparable. Monies could be embezzled, inventories could be pilfered, back doors could be implemented in software, customer lists could be divulged to competitors, as well as intellectual property.

Additionally, malware could be introduced into the computing environment; customer information could be stolen for purposes of identity theft or simply extorting money from your organization (think credit card lists). Of course, these are all concerns for your own internal users as well, but generally speaking, these risks are greater for the user base of your business partners for all of the reasons previously stated.

For those that doubt that any company would let a business partner become integrated enough into their environment to inflect, intentionally or unintentionally, much of the damage that I have cited as being possible, I would offer these thoughts. Mergers and acquisitions are a constant in our world. Giant corporations acquire smaller companies and force these new acquisitions to use the services of sister companies. It is not uncommon for these "sister" companies to become heavily integrated into the newly acquired family. In these instances, it would be a mistake to believe that just because two companies share the same parent that they aren't in practice two separate companies with the same challenges any business partnership faces.

Despite these negative facts, we're still talking about two organizations that have agreed to do business together and so, on the surface, have a mutual interest to see the other partner succeed. Consequently, these users are semi-trusted.

Customers:

These are truly untrusted endpoints and unfortunately, from an information security perspective, a necessary evil. Unless your organization is one that deals strictly with other businesses, your revenues depend on being able to provide quality services and products to your retail customers. Yes, there are many businesses where considering your customers to be an untrusted endpoint is not applicable and perhaps even ludicrous. However, we're not discussing serving breakfast in a diner or cutting someone's lawn.

In the context of this paper, we're discussing the challenges of user identity management and access control to your organization's resources. Perhaps your organization is a financial institution that provides a version of your online banking and trading software that operates in a PDA and needs to be operable where ever a WiFi connection is available in the world. Maybe your organization is a payroll company with customers in every state and you must provide both an easy and secure means for both employers to enter payroll information and for their employees to view this data. In both these instances, organizations have a requirement to manage literally millions of user identities and ensure that the

customers are who they say they are and are only accessing that information to which they are entitled. There is one thing in their favor though; these organizations know something about their customers. The identities of these customers have been established and they in turn, have been provided user credentials (digital identity) during some form of initial customer processing.

Consider the challenge of a company that sells its product strictly through the Internet. Whether its books, music CDs, computers or clothing, the company's wares will be shipped to a customer, probably upon validation of a credit card number, to any address specified in the request, without ever having verified a user's identity nor their location. Talk about an exposure to the company!

In any of the aforementioned scenarios, we have users who demand to be able to securely access desired products and services from anywhere at which Internet connectivity is available. Maybe the customer is at a cyber café, finishes their latté, forgets to log off and someone else sits down, more than happy to continue this person's business. Perhaps the customer is using an airport kiosk that didn't clear out the customer's credentials and session information stored in a permanent cookie with an expiration of 2029 and protected with only base64 encoding. There could be a customer who decides to order the latest best seller while at the library and is completely unaware of the keystroke logging program that a hacker installed that's recorded the user's personal information and credit card information gathered during the order process. Needless to say, that customer is probably going to become apoplectic when his/her credit card statement arrives.

So does all this mean that we should immediately shut down the web server? Of course not. However, it does mean that organizations must take reasonable precautions. Err on the side of caution and simply assume that retail customer endpoints are insecure and should be considered untrusted. By implementing a centralized management of identities and access control, augmented with a thorough, regular audit mechanism, many of these risks can be mitigated. Of course there is a litany of other security tools necessary to assist in this effort, but without these components in place, you won't even be able to determine if a user is even permitted in your network, let alone whether that user's actions are authorized.

User provisioning:

Organizations have numerous information systems to which users need to be granted access. If you go to any conference and speak to colleagues involved in the process of getting new employees access to the systems, applications necessary to perform their duties, chances are that they're not going to tell you a pretty story. Perhaps they have some email workflow process that multicasts out a notice that Jane Q. Citizen has just been hired into the accounts payable department, identifies her manager and requests that the necessary user-ids be created. Instructions on the needed levels of access on the various systems are

vague, if they exist at all, other than to provide the same access as Suzy Q. Associate who works in the same department.

How do we know that Suzy Q. Associate has the appropriate level of access? Perhaps she has worked in four other departments and every time she changes departments, new entitlements are simply added on top of existing ones, without any review of which of her previous entitlements were still required? Is there a way to simplify not just the user-id creation process, but the entitlement management process as well?

The simply answer of course is through the use of roles, and it's a good solution. The difficulty arises when we look at the significant amount of labor involved in defining these roles and the challenge of keeping these roles current on all the organizations information systems. The entitlements for these roles change as well as the roster of users that should be assigned to them. Consequently, user entitlements can quickly become out of synch with those required for users to perform their assigned duties.

What about employees that have left the company? As you can imagine, immediately removing all access to the organization's resources of an employee that left is extremely important. It wouldn't take long for a former employee with privileged access to cause great havoc to an organization. Likewise, illegally downloading confidential company information could also prove very damaging. Consequently, possessing the ability to immediately revoke a user's access to all resources becomes one of the top priorities of any organization. Unfortunately, for many organizations, a facility to provide centralized identity and access management to all of its information systems simply doesn't exist.

Single Sign-On:

Every user wants to have this and most security people probably cringe. It provides tremendous ease of use for customers but also gives the keys to the kingdom, so to speak, to anyone who is successful in fraudulently breaking in with another user's id. Implementing such a solution in a homogeneous environment, such as the Microsoft® resources that leverage Active Directory™, is relatively painless. Implementing such a solution across disparate systems, particularly when in-house propriety systems are involved is not for the feint of heart. Nonetheless, whether your organization currently implements a single sign-on solution or not, this is a challenge that system administrators and security personnel will probably have to address sooner or later.

Auditing:

This activity is similar to exercise. No one likes to do it, but it usually results in improving your health and probably makes you admit things that you would rather ignore. Without auditing, an organization can never know what actions are being taken to secure the enterprise, nor where gaps exist that require further attention.

Consequently, auditors insist on being provided reports that identify items such as:

- How many users have been inactive for a specified period of time (30, 60, 90 days etc.)?
- How frequently are users forced to change their passwords?
- What resources can each user in the organization access, and types of access do they have (browse, create, update, delete, etc.)?
- What profiles have been inactive for a specified period of time?
- Are there any user-ids or profiles that have never been used?

Obviously to anyone who has undergone an audit, the list of questions is far more extensive than presented here. However, even with the few questions that have been listed above, I suspect that there are many system administrators who would admit that one reason audit's are so dreaded, besides the fact that you may already be doing the job of two or three people, is that administrators simply do not possess any means to perform the requested queries.

So where do we go from here? Let's take a look at one vendor's proposed solution to these challenges, the eTrust™ Identity and Access Management Suite by Computer Associates®.

CA's eTrust™ Identity and Access Management Suite

Disclaimer:

OK, let's start with the obligatory legal disclaimer: This overview is not an endorsement, nor recommendation of the eTrust™ Identity and Access Management product suite and should not be considered as such. Neither should the reader infer any negative critiques, judgments, findings or conclusions against this solution. This is simply an overview of one solution offered by Computer Associates® to address the problem of Identity and Access Management.

Any representation of features, descriptions and benefits of the eTrust™ Identity and Access Management Suite and its products listed hereafter are derived directly from product information sources from the Computer Associates® website.

Centralized identity and access management:

This product suite is a solution built on a modular design that enables organizations to either deploy individual components of the product suite or the complete solution. If the complete solution is chosen, organizations will be able to manage their user identities and assign access rights from a common interface.[14] This product suite also has the capability to manage disparate technologies with

[14] http://www3.ca.com/Files/Brochures/etrust_iam_brochure.pdf

the capability to address security for legacy systems, distributed computing environments and emerging web services.[15] Let's take a look at the individual components.

eTrust™ Admin:

This is a key component of the eTrust™ Identity and Access Management Suite.[16] I don't know if all roads ever did in fact lead to Rome during the Roman Empire, but within this product suite, they do lead to the Admin tool.

eTrust™ Admin provides businesses with the ability to fully automate the user provisioning process. Additionally, user accounts can be automatically created, modified and deleted on multiple, heterogeneous systems or applications based on user roles. Furthermore, eTrust™ Admin can integrate with human resource systems to achieve completely automated user account management.[17]

eTrust™ Admin uses role-based administration to help ensure consistent application of security policies across the enterprise. Instead of defining an individual's needs to resources, eTrust™ Admin bases user assignments by job function.[18]

eTrust™ Admin reduces administrative workloads through the following features:[19]

- automated account creation – interface with a human resources system[20]
- delegated web-based administration – create subsets of administrators with limited functionality[21]
- self-service administration – users may update personal information and change passwords[22]
- self-service password reset – includes the ability to define a challenge/response web interface[23]

eTrust™ Admin is built upon the eTrust™ Directory. This is an X.500 directory that can scale from small focused user departments to large-scale global enterprises.[24]

eTrust™ Admin supports most platforms and applications out of the box. It can interface to any LDAP-compliant directory or SQL-capable database system.[25]

---

[15] http://www3.ca.com/Files/Brochures/etrust_iam_brochure.pdf
[16] http://www3.ca.com/Solutions/Overview.asp?ID=155&TYPE=S
[17] http://www3.ca.com/Solutions/Overview.asp?ID=155&TYPE=S
[18] http://www3.ca.com/Solutions/Overview.asp?ID=155&TYPE=S
[19] http://www3.ca.com/Solutions/Overview.asp?ID=155&TYPE=S
[20] http://www3.ca.com/Solutions/Overview.asp?ID=155&TYPE=S
[21] http://www3.ca.com/Files/FactSheet/eTrustAdmin2_FDB.pdf
[22] http://www3.ca.com/Files/FactSheet/eTrustAdmin2_FDB.pdf
[23] http://www3.ca.com/Files/FactSheet/eTrustAdmin2_FDB.pdf
[24] http://www3.ca.com/Files/FactSheet/eTrustAdmin2_FDB.pdf
[25] http://www3.ca.com/Solutions/Overview.asp?ID=155&TYPE=S

Bottom line: eTrust™ Admin provides role/policy based user provisioning that simplifies administration, reduces administrative costs and enhances security.[26] eTrust™ Admin supports the following environments:[27]

Active Directory (Windows™ 2000)	Lotus Notes/Domino
AS/400	MS SQL Server
CleverPath™ Porta	Multiple UNIX platforms, NIS, NIS+
eTrust™ Access Control	Novell NDS and Bindaries
eTrust™ CA-ACF2® Security for z/OS and OS/390	NSK Safeguard
eTrust™ CA-Top Secret® Security for z/OS and OS/390	Open VMS
eTrust™ PKI	Oracle, DB2 and UDB
eTrust™ Single Sign-On	PeopleSoft HRMS
eTrust™ Web Access Control	Relational Databases
Exchange (5.5 and 2000)	RSA SecurID
IBM RACF	SAP R/3
LDAP v3 Directories	Windows NT domains
Linux (Red Hat, SuSE, and OS/390)	

eTrust™ Access Control:

eTrust™ Access Control takes the baton, so to speak, from eTrust™ Admin. After a user has been provisioned, or assigned to the appropriate roles, Access Control, through the use of policies, controls whether a user can access specific systems, what they can do within them and when they are allowed to access these systems. Policies can be created and managed for the enterprise or customized to meet the security requirements of a specific application.[28]

Distinctive features:

- Role-based security – Easy to implement security by using functional profiles that facilitate adding users to pre-defined groups with pre-defined access privileges[29]
- Fine-grained resource protection – All system resources including data files, applications, devices, processes/daemons, and audit files can be secured[30]
- True super-user control – Kernel level access control technology controls all actions including privileged accounts such as root in UNIX and administrators in Windows NT/2000[31]

[26] http://www3.ca.com/Files/Brochures/etrust_iam_brochure.pdf
[27] http://www3.ca.com/Files/DataSheets/etrust_admin_pd.pdf
[28] http://www3.ca.com/Solutions/Overview.asp?ID=154&TYPE=S
[29] http://www3.ca.com/Files/FactSheet/etrust_access_control_fdb.pdf
[30] http://www3.ca.com/Files/FactSheet/etrust_access_control_fdb.pdf
[31] http://www3.ca.com/Files/FactSheet/etrust_access_control_fdb.pdf

- Strong self-protection – Prevents hackers with administrator's access from circumventing or shutting down the eTrust™ Access Control security engine.[32]
- Comprehensive Network Control – Firewall-like security features control both inbound and outbound ports, especially TCP connections.[33]
- Enhanced security with dual control – A security sensitive option, if utilized, requires policy changes to be confirmed by a second security manager.[34]
- Reliable auditing – Tracks original user names from the initial authentication to create secure and useful audit trails with full integrity. Logs can be routed to multiple locations to reduce risks of unauthorized tampering as well as providing a centralized audit overview across different systems.[35]
- Open authentication – Supports many authentication methods including operating system passwords, smart cards, digital certificates, token and one-time passwords.[36]
- Extensive user account management – The Policy Model Database (PMDB) feature enables fast additions, changes and revocations to users and groups across different platforms, including synchronization with native operating system settings.[37]
- Integrated mainframe password synchronization – Top Secret and ACF-2 user databases can be shared by eTrust™ Access Control PMDB hierarchy.[38]
- Strong defense mechanism with STOP (Stack Overflow Protection) and Denial of Trojan Horse – STOP prevents hackers from using stack overflow exploits. eTrust™ Access Control can also deny the unauthorized access activated by Trojan Horse infected programs.[39]
- Platform support – AT&T, Digital Unix, HP-UX, IBM-AIX, Linux, SGI Irix, NCR MP-RAS, SCO UnixWare, Siemens Sinix, Sun Solaris and Windows NT/2000.[40]

Bottom line: eTrust™ Access Control controls:[41]

- What specific systems, applications and files users can access
- What users can do with these resources
- When users are allowed access these resources

eTrust™ Web Access Control:

You don't have to be a security expert nor a rocket scientist to realize that web security is a crucial issue to both customers and businesses. eTrust™ Web

[32] http://www3.ca.com/Files/FactSheet/etrust_access_control_fdb.pdf
[33] http://www3.ca.com/Files/FactSheet/etrust_access_control_fdb.pdf
[34] http://www3.ca.com/Files/FactSheet/etrust_access_control_fdb.pdf
[35] http://www3.ca.com/Files/FactSheet/etrust_access_control_fdb.pdf
[36] http://www3.ca.com/Files/FactSheet/etrust_access_control_fdb.pdf
[37] http://www3.ca.com/Files/FactSheet/etrust_access_control_fdb.pdf
[38] http://www3.ca.com/Files/FactSheet/etrust_access_control_fdb.pdf
[39] http://www3.ca.com/Files/FactSheet/etrust_access_control_fdb.pdf
[40] http://www3.ca.com/Files/FactSheet/etrust_access_control_fdb.pdf
[41] http://www3.ca.com/Files/Brochures/etrust_iam_brochure.pdf

Access Control positions itself as being able to secure web resources, proactively prevent intrusions, deliver secure single sign-on across internal and external websites and simplify system access for end users.[42] That's a tall order.

Let's take a look at some of the product's features:

- Online content and service security – eTrust™ Web Access Control acts as an authentication and authorization gateway for URLs and web applications.[43] Access to employee portals, partner extranets and web-based supply chain management systems are secured.[44]
- Versatile single sign-on – Through its user portal page, eTrust™ Web Access Control provides easy single sign-on capabilities to any form-based external web logins, as well as internal web servers.[45] Using JavaScript, automatic authentication is performed to any external form-based websites or web applications based on authenticated user IDs and stored passwords. Additionally, internal web servers can automatically share authenticated credentials across different web agents.[46]
- Reduced management costs and overhead – Centralized management and reporting across large numbers of heterogeneous servers.[47]
- Flexible authentication – Multiple authentication methods to meet business requirements to include: PKI, LDAP, mainframe, biometrics, token and passwords.[48]
- Self-registration – Easy to use self-registration function for entry-level account creation.[49]
- Embedded directory repository – Built in directory database with an open LDAP interface for synchronizing with an organization's existing user repository.[50]
- APIs – Various authentication and authorization APIs for identification, validation and regulation of user access. This feature enables the repository to build personalized, secure websites with superior access control.[51]

Supported environments:[52]

- Policy Server: Windows 2000
- Policy Manager: Windows 2000
- Web Agent: Microsoft IIS, Apache Sun iPlanet
- Application Server Agent: CleverPath™ Portal, BEA Weblogic, IBM WebSphere

---

[42] http://www3.ca.com/Files/Brochures/ewac_pd3.pdf
[43] http://www3.ca.com/Files/Brochures/ewac_pd3.pdf
[44] http://www3.ca.com/Files/FactSheet/ewac_fdb.pdf
[45] http://www3.ca.com/Files/Brochures/ewac_pd3.pdf
[46] http://www3.ca.com/Files/FactSheet/ewac_fdb.pdf
[47] http://www3.ca.com/Files/FactSheet/ewac_fdb.pdf
[48] http://www3.ca.com/Files/Brochures/ewac_pd3.pdf
[49] http://www3.ca.com/Files/Brochures/ewac_pd3.pdf
[50] http://www3.ca.com/Files/Brochures/ewac_pd3.pdf
[51] http://www3.ca.com/Files/Brochures/ewac_pd3.pdf
[52] http://www3.ca.com/Files/Brochures/ewac_pd3.pdf

Bottom line: eTrust™ Web Access Control provides the following benefits:[53]

- Provides secure access to employee portals and protects partner extranets and web-based supply-chain management systems.
- Provides dynamic personalization and seamless security. User will only see authorized web resources.
- Self-registration reduces administrative overhead.
- Able to integrate with eTrust™ CA-ACF2® Security and eTrust™ CA-Top Secret® and use either of these platforms as a trusted user repository.

eTrust™ Single Sign-On:

eTrust™ Single Sign-On provides seamless user authentication across the enterprise. It can log users into the mainframe, middleware or web applications from a single user authentication.[54]

eTrust™ Single Sign-On is not a password synchronization solution. Rather, it manages both a primary and a secondary authentication. Primary authentication verifies the identity of a user opening an eTrust™ SSO session. Secondary authentication is the process of supplying authentication credentials to the applications the user is accessing. eTrust™ SSO manages a unique user-id and password per application for each user.[55] It is through this automated login process that eTrust™ SSO is able to seamlessly provide users access to email, databases, web, mainframe and ERP applications.[56]

A variety of user authentication methods are supported. These include: biometrics, digital certificates, security tokens, LDAP or passwords.[57] Additionally, it is possible to use different authentication methods for designated parts of the user population.[58]

eTrust™ SSO employs a directory-based architecture. It enables management of roaming sessions and controlling access to shared workstations. eTrust™ SSO manages and enforces password policies, and strengthens application security through proactive generation of long, complex passwords that users no longer need to remember.[59]

eTrust™ SSO does not require that any changes be made to the applications to which it is managing access.[60] There are two ways by which eTrust™ SSO can log into applications: login dialogs (which are done via Tcl) and APIs.[61]

---

[53] http://www3.ca.com/Files/Brochures/ewac_pd3.pdf
[54] http://www3.ca.com/Solutions/Overview.asp?ID=166&TYPE=S
[55] http://www3.ca.com/Files/FAQs/etrust_sso_faq.pdf
[56] http://www3.ca.com/Files/DataSheets/etrust_sso.pdf
[57] http://www3.ca.com/Files/FAQs/etrust_sso_faq.pdf
[58] http://www3.ca.com/Files/FAQs/etrust_sso_faq.pdf
[59] http://www3.ca.com/Solutions/Overview.asp?ID=166&TYPE=S
[60] http://www3.ca.com/Files/FAQs/etrust_sso_faq.pdf
[61] http://www3.ca.com/Files/FAQs/etrust_sso_faq.pdf

eTrust™ SSO handles password expirations in the following manner:[62]

- Proactively change passwords before they expire on the application
- Generate new application passwords that the user does not know
- Through exception handling of messages from the target application

eTrust™ SSO encrypts all communications between applications whenever possible. For those applications that don't support encrypted communications, such as Telnet, one-time passwords can be used.[63]

eTrust™ SSO audit capabilities include capturing virtually all user login activity. This activity includes any access to the Policy Server, requests for application lists and failed login attempts. These logs can be used by the eTrust™ Audit tool for consolidated viewing of all login activity across the enterprise.[64]

Client software is needed when users wish to use eTrust™ SSO to access mainframe applications or client/server systems. This software only runs on Windows 98, NT, 2000 and XP. Client software is not required for access that is limited to web applications.[65]

eTrust™ SSO supports the following server and web server platforms:[66]

- UNIX – IBM AIX, HP-UX, Sun Solaris
- Windows – NT, 2000 and 2003 Server
- Microsoft IIS
- Apache
- Netscape web server

Bottom line: eTrust™ SSO enhances overall security by automating access to all authorized Web services and enterprise wide applications through a single login.[67] Application security is strengthened by using long, complex passwords that users no longer need to remember.[68]

eTrust™ Directory*:*

eTrust™ Directory is the backbone of the eTrust™ Identity and Access Management Suite.[69] Essentially, this is a component that stays behind the scenes. It is utilized by all of the other products in this suite to access and manage their respective required information. Most administrators will probably never have to concern themselves with the details of the directory, but for those who are curious or who are responsible for developing integration and security

[62] http://www3.ca.com/Files/FAQs/etrust_sso_faq.pdf
[63] http://www3.ca.com/Files/FAQs/etrust_sso_faq.pdf
[64] http://www3.ca.com/Files/FAQs/etrust_sso_faq.pdf
[65] http://www3.ca.com/Files/FAQs/etrust_sso_faq.pdf
[66] http://www3.ca.com/Files/FAQs/etrust_sso_faq.pdf
[67] http://www3.ca.com/Files/Brochures/etrust_iam_brochure.pdf
[68] http://www3.ca.com/Solutions/Overview.asp?ID=166&TYPE=S
[69] http://www3.ca.com/Solutions/ProductFamily.asp?ID=4839

capabilities of this suite beyond what was provided out of the box, then a much deeper understanding of this directory is required.

Here are some quick facts regarding eTrust™ Directory:[70]

- Customer proven capability to support 20,000,000+ entries & 1000 searches per second
- Provides a standards-compliant platform for managing complex distributed information
- An X.500 (DAP) directory that is also fully LDAP V3 compliant
- Supported environments:[71]
    - Solaris
    - Windows NT/2000/XP/.NET
    - Red Hat Linux
- Current version is V4.0
- V4.0 is certified to successfully interoperate with SAP

Listed below are some of the typical uses of eTrust™ Directory:[72]

- Consolidating and linking together legacy systems
- PKI: Storing and managing certificates
- Storing security profiles
- Integrating all of the directories in an enterprise
- Personnel and resource listing
- A repository for name, password and profile information for Radius servers
- Traditional “white pages/yellow pages”

eTrust™ Directory supports all LDAP-enabled clients from Microsoft, Novell, Sun-Netscape, Lotus and clients constructed from publicly available LDAP toolkits. Additionally, the directory supports any schema type that is specific to particular LDAP-enabled applications, such as ISP, DEN, CTI/IVR, Postal, Security, HR, catalog services, document management, government and financial services.[73]

eTrust™ Directory uses an embedded RDBMS.[74] It also has noteworthy performance claim: eTrust™ Directory’s patented ability to index every field (attribute) of every entry allows complex searches to retrieve any element of data within a maximum of 2 hard disk hits, delivering sub-second responses on multi-million entry databases.[75] Now I don’t pretend to be a hardware engineer, but that claim sounds impressive to me.

[70] http://www3.ca.com/Solutions/Collateral.asp?CID=33042&ID=160
[71] http://www3.ca.com/Files/DataSheets/eTrust_directory_pd.pdf
[72] http://www3.ca.com/Solutions/Collateral.asp?CID=33199&ID=160
[73] http://www3.ca.com/Files/WhitePapers/etrustdirectory_wp.pdf
[74] http://www3.ca.com/Solutions/Collateral.asp?CID=33199&ID=160
[75] http://www3.ca.com/Solutions/Collateral.asp?CID=33199&ID=160

eTrust™ Audit:

Now let's take a brief look at the last component of this product suite. We've all heard the saying, "The job isn't finished until the paperwork is done". This is where the paperwork will get done and both administrators, and organizations for that matter, can get a report card on the effectiveness of their Identity and Access Management practices.

Distinctive Functionalities:[76]

- Cross-platform event management – Collects audit log data from:
  - Windows NT/2000/XP
  - UNIX/Linux
  - OS/390
  - Security appliances – Checkpoint Firewall-1, Cisco PIX and Router
  - RDBMS – Oracle, MS SQL Server, MS Access
  - Web servers – Netscape, Apache
  - Other eTrust™ solutions
  - Systems not natively supported – via SNMP messages or via API calls
- Support for custom pattern recognition – Provides the ability to define the criteria that eTrust™ Audit will use to recognize event patterns as well as actions to take (if so defined) if a match is made. Several examples of predefined patterns recognition configurations are included with the product.
- Versatile filtering – Enables administrators to define critical events that should be retained and processed. This eliminates events that are of little or no importance.
- Near real-time alert management – Critical events can be filtered, logged and sent to security personnel in near real time.
- Centralized policy management – Your organization's central auditing policy is defined in eTrust™ Audit. The audit tool will then remotely distribute the rules to the clients from one central host.
- Central audit log data repository – Audit log data is collected from all defined organizational sources and subsequently stored in a central repository.
- Reporting capability – Numerous reporting and graph functions are included with eTrust™ Audit. Additional reporting capabilities can be added using Crystal Reports, or any other SQL-based reporting tool. There is an HTML format available for reports.
- GUI tools – Enables system management as well as the viewing and filtering of audit information.

Bottom line: eTrust™ Audit provides the following benefits:[77]

- Collects enterprise wide security and system audit files
- Filters collected information for consolidated viewing and reporting
- Automatically triggers appropriate actions upon detecting suspicious system activities

[76] http://www3.ca.com/Files/DataSheets/etrust_audit_pd.pdf
[77] http://www3.ca.com/Files/DataSheets/etrust_audit_pd.pdf

- Enables true cross platform event management

So we've almost finished our journey. We've discussed at some length the challenges of implementing a centralized identity and access management solution in the enterprise. We've also taken a high level look at the solution that Computer Associates® offers to this challenge. Before we conclude, I've listed some references of success stories with the various products described in the eTrust™ Identity and Access Management Suite.

eTrust™ Identity and Access Management Success Stories

Another Disclaimer:

This final section before the conclusion is simply an opportunity to provide some references from customer's who are satisfied with their implementation of one or more products from the eTrust™ Identity and Access Management Suite. Once again, this is not an endorsement, nor a criticism.

It is only prudent, for any organization considering a vendor's product to ask for customer references. We want to know; who else is using this? Therefore, I am listing a number of URLs along with an accompanying short blurb that describes the problem that each customer was trying to solve. Those interested in learning more about these success stories with the eTrust™ Identity and Access Management Suite as well as an endorsement, can follow the hyperlinks provided.

Success Story #1:

Brigham Young University Puts Its Faith in eTrust™ Security[78]

- Challenge: Improve System Security, Reliability and Performance in a Changing Environment
- Products used: eTrust™ Admin, eTrust™ Access Control, eTrust™ Audit
- URL: http://www3.ca.com/Files/SuccessStory/byu_etrust.pdf

Success Story #2:

Médiapost Adopts eTrust™ Admin and eTrust™ Single Sign-On to Reinforce Security of Critical Data[79]

- Challenge: Create centralized administration of existing directories and streamline the management of passwords through a single identification or single sign-on.
- Products used: eTrust™ Admin, eTrust™ Single Sign-On
- URL: http://www3.ca.com/Files/SuccessStory/mediapost_adoptetrust.pdf

[78] http://www3.ca.com/Files/SuccessStory/byu_etrust.pdf
[79] http://www3.ca.com/Files/SuccessStory/mediapost_adoptetrust.pdf

Success Story #3:

eTrust™ Directory Enables SECOM Trust.Net to Supply High-Level Security Infrastructure for the eMarketplace[80]

- Challenge: Select a directory to be the nucleus to support the PKI service needs for Japan's first certified IDENTRUS Express Partner.
- Product used: eTrust™ Directory
- URL: http://www3.ca.com/Files/SuccessStory/secom_ss.pdf

Endorsement:

The American Hospital Association has provided CA with an exclusive endorsement for technologies to enable compliance efforts with the HIPAA Security Rule.[81]

- Endorsed Technologies include:
  - eTrust™ Admin
  - eTrust™ Access Control
  - eTrust™ Web Access Control
  - eTrust™ Single Sign-On
  - eTrust™ Directory
  - eTrust™ Audit
- URL: http://www3.ca.com/Files/Brochures/partner_healthcare_aha_ads.pdf

Conclusion

Life's not fair. If you haven't learned that fact yet, you may want to skip this conclusion. Users, whether they're internal to your organization, employees of your business partners, or customers, especially customers, want what they want, when they want it, how they want it, and it always needs to work. Now, that might not have been the most grammatically suave sentence you've ever read, but I bet that phrase rings true.

Just ask an email administrator. Talk about a thankless job! I don't recall ever hearing anyone say to any email administrator, "Hey Sue, great job with that email system. I've been getting a couple of hundred emails a day for over a year and not a single glitch, keep up the good work." Watch how fast Sue's phone lights up when the email goes down.

Think about your car for a moment: you place the car in drive and push the gas, you go forward, push the gas pedal down further, you go faster; push the brake and you stop (hopefully). Each of these actions requires a very complex symphony of actions to occur between the majority of the mechanical and electrical systems of your car. Nonetheless, we expect them to happen without flaw, every time we use them. Hmmm, sounds like your average computer user, doesn't it?

[80] http://www3.ca.com/Files/SuccessStory/secom_ss.pdf
[81] http://www3.ca.com/Files/Brochures/partner_healthcare_aha_ads.pdf

The computing demands of customers, businesses and users will continue to increase in every dimension. People will always want what they want, when they want it, and how they want it, but now they are also demanding better, faster, cheaper, and in the area of electronic communications, not just more secure, but secure, period.

Those organizations that can consistently provide easy, secure, reliable, ubiquitous access to their customers will reap the greatest financial rewards. Organizations that can meet the myriad of identity and access management challenges to provide such a class of service to their customers will enjoy the victor's spoils.

Presumably, if you are reading this, you're a member of the Information Security community, and if you're not, why are you reading this? Ours is a profession much like Sue our email administrator, in that no one ever thanks us for securing their identities, transactions, data, personal information or even their money, but beware of their wrath if we ever get it wrong. That's simply the cost of admission.

If you're old enough to remember the television police series, "Hill Street Blues", I'd like to end with the same parting words that Sgt. Phil Esterhaus would use to end each roll call, "And hey – let's be careful out there".[82]

References

1. Computer Associates®, "eTrust™ Identity and Access Management Suite" 2003. URL: http://www3.ca.com/Files/Brochures/etrust_iam_brochure.pdf (6 April 2004). Page-6
2. Risk Associates, "Non-Repudiation". URL: http://www.yourwindow.to/information-security/gl_nonrepudiation.htm (6 April 2004)
3. Tripwire®, "Legislation Affecting Bank Security". URL: http://www.tripwire.com/files/literature/white_papers/GLB_OCC_White_Paper.pdf (6 April 2004). page-2
4. © General Electric Company, "The GE90 Engine Family". URL: http://www.geae.com/engines/commercial/ge90/index.html (6 April 2004)
5. Brian Komar. MCSE Training Guide (70-240): Windows 2000 Accelerated Exam. United States of America: New Riders Publishing, 2001. 284
6. Bill Calkins. Solaris 7 Administrator Certification Training Guide: Part I and II. United States of America: New Riders Publishing. 183
7. Brian Komar. MCSE Training Guide (70-240): Windows 2000 Accelerated Exam. United States of America: New Riders Publishing, 2001. 284
8. Bill Calkins. Solaris 7 Administrator Certification Training Guide: Part I and II. United States of America: New Riders Publishing. 183
9. Rudyard Kipling, "The Ballad of East and West". URL: http://www.theotherpages.org/poems/kiplin01.html (6 April 2004)

[82] http://www.nostalgiacentral.com/tv/cops/hillstreet.htm

10. Brian Komar. MCSE Training Guide (70-240): Windows 2000 Accelerated Exam. United States of America: New Riders Publishing, 2001. 300
11. University of Alberta, Department of Biological Sciences, "Choosing a Good Password". URL: http://www.biology.ualberta.ca/facilities/computing/index.php?Page=2076&Print=Yes (6 April 2004)
12. Peter Tippett, "STRONGER PASSWORDS AREN'T", June 2001. URL: http://infosecuritymag.techtarget.com/articles/june01/columns_executive_view.shtml (6 April 2004)
13. Mark Twain, "The Reports of my death have been greatly exaggerated". URL: http://www.brainyquote.com/quotes/quotes/m/marktwain141773.html (6 April 2004)
14. Computer Associates®, "eTrust™ Identity and Access Management Suite" 2003. URL: http://www3.ca.com/Files/Brochures/etrust_iam_brochure.pdf (6 April 2004). Page-6
15. Computer Associates®, "eTrust™ Identity and Access Management Suite" 2003. URL: http://www3.ca.com/Files/Brochures/etrust_iam_brochure.pdf (6 April 2004). Page-7
16. Computer Associates®, "eTrust Admin Identity Provisioning For an On-Demand Environment", URL: http://www3.ca.com/Solutions/Overview.asp?ID=155&TYPE=S (6 April 2004)
17. Computer Associates®, "eTrust Admin Identity Provisioning For an On-Demand Environment", URL: http://www3.ca.com/Solutions/Overview.asp?ID=155&TYPE=S (6 April 2004)
18. Computer Associates®, "eTrust Admin Identity Provisioning For an On-Demand Environment", URL: http://www3.ca.com/Solutions/Overview.asp?ID=155&TYPE=S (6 April 2004)
19. Computer Associates®, "eTrust Admin Identity Provisioning For an On-Demand Environment", URL: http://www3.ca.com/Solutions/Overview.asp?ID=155&TYPE=S (6 April 2004)
20. Computer Associates®, "eTrust Admin Identity Provisioning For an On-Demand Environment", URL: http://www3.ca.com/Solutions/Overview.asp?ID=155&TYPE=S (6 April 2004)
21. Computer Associates®, "eTrust Admin Features, Descriptions and Benefits". URL: http://www3.ca.com/Files/FactSheet/eTrustAdmin2_FDB.pdf (6 April 2004). Page-1
22. Computer Associates®, "eTrust Admin Features, Descriptions and Benefits". URL: http://www3.ca.com/Files/FactSheet/eTrustAdmin2_FDB.pdf (6 April 2004). Pg 1-2
23. Computer Associates®, "eTrust Admin Features, Descriptions and Benefits". URL: http://www3.ca.com/Files/FactSheet/eTrustAdmin2_FDB.pdf (6 April 2004). Page-2
24. Computer Associates®, "eTrust Admin Features, Descriptions and Benefits". URL: http://www3.ca.com/Files/FactSheet/eTrustAdmin2_FDB.pdf (6 April 2004). Page-1
25. Computer Associates®, "eTrust Admin Identity Provisioning For an On-Demand Environment", URL: http://www3.ca.com/Solutions/Overview.asp?ID=155&TYPE=S (6 April 2004)
26. Computer Associates®, "eTrust™ Identity and Access Management Suite" 2003. URL: http://www3.ca.com/Files/Brochures/etrust_iam_brochure.pdf (6 April 2004). Page-6

27. Computer Associates®, “eTrust™ Admin Comprehensive Identity Provisioning for an On-Demand Environment”, URL: http://www3.ca.com/Files/DataSheets/etrust_admin_pd.pdf (6 April 2004). Page-2
28. Computer Associates®, “eTrust Access Control Regulating Access to Critical Business Assets”, URL: http://www3.ca.com/Solutions/Overview.asp?ID=154&TYPE=S (6 April 2004)
29. Computer Associates®, “eTrust Access Control – Features, Descriptions and Benefits Version 5.1”, URL: http://www3.ca.com/Files/FactSheet/etrust_access_control_fdb.pdf (6 April 2004). Page-1
30. Computer Associates®, “eTrust Access Control – Features, Descriptions and Benefits Version 5.1”, URL: http://www3.ca.com/Files/FactSheet/etrust_access_control_fdb.pdf (6 April 2004). Page-1
31. Computer Associates®, “eTrust Access Control – Features, Descriptions and Benefits Version 5.1”, URL: http://www3.ca.com/Files/FactSheet/etrust_access_control_fdb.pdf (6 April 2004). Page-1
32. Computer Associates®, “eTrust Access Control – Features, Descriptions and Benefits Version 5.1”, URL: http://www3.ca.com/Files/FactSheet/etrust_access_control_fdb.pdf (6 April 2004). Page-1
33. Computer Associates®, “eTrust Access Control – Features, Descriptions and Benefits Version 5.1”, URL: http://www3.ca.com/Files/FactSheet/etrust_access_control_fdb.pdf (6 April 2004). Page-2
34. Computer Associates®, “eTrust Access Control – Features, Descriptions and Benefits Version 5.1”, URL: http://www3.ca.com/Files/FactSheet/etrust_access_control_fdb.pdf (6 April 2004). Page-2
35. Computer Associates®, “eTrust Access Control – Features, Descriptions and Benefits Version 5.1”, URL: http://www3.ca.com/Files/FactSheet/etrust_access_control_fdb.pdf (6 April 2004). Page-2
36. Computer Associates®, “eTrust Access Control – Features, Descriptions and Benefits Version 5.1”, URL: http://www3.ca.com/Files/FactSheet/etrust_access_control_fdb.pdf (6 April 2004). Page-2
37. Computer Associates®, “eTrust Access Control – Features, Descriptions and Benefits Version 5.1”, URL: http://www3.ca.com/Files/FactSheet/etrust_access_control_fdb.pdf (6 April 2004). Page-3
38. Computer Associates®, “eTrust Access Control – Features, Descriptions and Benefits Version 5.1”, URL: http://www3.ca.com/Files/FactSheet/etrust_access_control_fdb.pdf (6 April 2004). Page-4

39. Computer Associates®, “eTrust Access Control – Features, Descriptions and Benefits Version 5.1”, URL: http://www3.ca.com/Files/FactSheet/etrust_access_control_fdb.pdf (6 April 2004). Page-4
40. Computer Associates®, “eTrust Access Control – Features, Descriptions and Benefits Version 5.1”, URL: http://www3.ca.com/Files/FactSheet/etrust_access_control_fdb.pdf (6 April 2004). Page-4
41. Computer Associates®, “eTrust™ Identity and Access Management Suite” 2003. URL: http://www3.ca.com/Files/Brochures/etrust_iam_brochure.pdf (6 April 2004). Page-6
42. Computer Associates®, “eTrust™ Web Access Control”, URL: http://www3.ca.com/Files/Brochures/ewac_pd3.pdf (6 April 2004). Page-1
43. Computer Associates®, “eTrust™ Web Access Control”, URL: http://www3.ca.com/Files/Brochures/ewac_pd3.pdf (6 April 2004). Page-1
44. Computer Associates®, “eTrust™ Web Access Control Features, Descriptions and Benefits”, URL: http://www3.ca.com/Files/FactSheet/ewac_fdb.pdf (6 April 2004). Page-1
45. Computer Associates®, “eTrust™ Web Access Control”, URL: http://www3.ca.com/Files/Brochures/ewac_pd3.pdf (6 April 2004). Page-2
46. Computer Associates®, “eTrust™ Web Access Control Features, Descriptions and Benefits”, URL: http://www3.ca.com/Files/FactSheet/ewac_fdb.pdf (6 April 2004). Page-1
47. Computer Associates®, “eTrust™ Web Access Control Features, Descriptions and Benefits”, URL: http://www3.ca.com/Files/FactSheet/ewac_fdb.pdf (6 April 2004). Page-1
48. Computer Associates®, “eTrust™ Web Access Control”, URL: http://www3.ca.com/Files/Brochures/ewac_pd3.pdf (6 April 2004). Page-2
49. Computer Associates®, “eTrust™ Web Access Control”, URL: http://www3.ca.com/Files/Brochures/ewac_pd3.pdf (6 April 2004). Page-2
50. Computer Associates®, “eTrust™ Web Access Control”, URL: http://www3.ca.com/Files/Brochures/ewac_pd3.pdf (6 April 2004). Page-2
51. Computer Associates®, “eTrust™ Web Access Control”, URL: http://www3.ca.com/Files/Brochures/ewac_pd3.pdf (6 April 2004). Page-2
52. Computer Associates®, “eTrust™ Web Access Control”, URL: http://www3.ca.com/Files/Brochures/ewac_pd3.pdf (6 April 2004). Page-2
53. Computer Associates®, “eTrust™ Web Access Control”, URL: http://www3.ca.com/Files/Brochures/ewac_pd3.pdf (6 April 2004). Page-1
54. Computer Associates®, “eTrust Single Sign-On”, URL: http://www3.ca.com/Solutions/Overview.asp?ID=166&TYPE=S (6 April 2004)
55. Computer Associates®, “eTrust™ Single Sign-On Frequently Asked Questions”, URL: http://www3.ca.com/Files/FAQs/etrust_sso_faq.pdf (6 April 2004). Pages 1-2
56. Computer Associates®, “eTrust Single Sign-On Managing eBusiness Security”, URL: http://www3.ca.com/Files/DataSheets/etrust_sso.pdf (6 April 2004). Page-2
57. Computer Associates®, “eTrust™ Single Sign-On Frequently Asked Questions”, URL: http://www3.ca.com/Files/FAQs/etrust_sso_faq.pdf (6 April 2004). Page-2

58. Computer Associates®, “eTrust™ Single Sign-On Frequently Asked Questions”, URL: http://www3.ca.com/Files/FAQs/etrust_sso_faq.pdf (6 April 2004). Page-3
59. Computer Associates®, “eTrust Single Sign-On”, URL: http://www3.ca.com/Solutions/Overview.asp?ID=166&TYPE=S (6 April 2004)
60. Computer Associates®, “eTrust™ Single Sign-On Frequently Asked Questions”, URL: http://www3.ca.com/Files/FAQs/etrust_sso_faq.pdf (6 April 2004). Page-3
61. Computer Associates®, “eTrust™ Single Sign-On Frequently Asked Questions”, URL: http://www3.ca.com/Files/FAQs/etrust_sso_faq.pdf (6 April 2004). Page-3
62. Computer Associates®, “eTrust™ Single Sign-On Frequently Asked Questions”, URL: http://www3.ca.com/Files/FAQs/etrust_sso_faq.pdf (6 April 2004). Page-3
63. Computer Associates®, “eTrust™ Single Sign-On Frequently Asked Questions”, URL: http://www3.ca.com/Files/FAQs/etrust_sso_faq.pdf (6 April 2004). Page-5
64. Computer Associates®, “eTrust™ Single Sign-On Frequently Asked Questions”, URL: http://www3.ca.com/Files/FAQs/etrust_sso_faq.pdf (6 April 2004). Page-5
65. Computer Associates®, “eTrust™ Single Sign-On Frequently Asked Questions”, URL: http://www3.ca.com/Files/FAQs/etrust_sso_faq.pdf (6 April 2004). Page-4
66. Computer Associates®, “eTrust™ Single Sign-On Frequently Asked Questions”, URL: http://www3.ca.com/Files/FAQs/etrust_sso_faq.pdf (6 April 2004). Page-4
67. Computer Associates®, “eTrust™ Identity and Access Management Suite” 2003. URL: http://www3.ca.com/Files/Brochures/etrust_iam_brochure.pdf (6 April 2004). Page-6
68. Computer Associates®, “eTrust Single Sign-On”, URL: http://www3.ca.com/Solutions/Overview.asp?ID=166&TYPE=S (6 April 2004)
69. Computer Associates®, “eTrust Identity and Access Management Suite Security That Protects and Enables”, URL: http://www3.ca.com/Solutions/ProductFamily.asp?ID=4839 (6 April 2004)
70. Computer Associates®, “eTrust Directory Quick Facts”, URL: http://www3.ca.com/Solutions/Collateral.asp?CID=33042&ID=160 (6 April 2004)
71. Computer Associates®, “eTrust™ Directory Managing eBusiness Security”, URL: http://www3.ca.com/Files/DataSheets/eTrust_directory_pd.pdf (6 April 2004). Page-2
72. Computer Associates®, “eTrust Directory FAQ v3.6”, URL: http://www3.ca.com/Solutions/Collateral.asp?CID=33199&ID=160 (6 April 2004). Page-2
73. Computer Associates®, “eTrust Directory Meeting the Needs of Global Infrastructures”, URL: http://www3.ca.com/Files/WhitePapers/etrustdirectory_wp.pdf (6 April 2004). Page-5
74. Computer Associates®, “eTrust Directory FAQ v3.6”, URL: http://www3.ca.com/Solutions/Collateral.asp?CID=33199&ID=160 (6 April 2004). Page-2
75. Computer Associates®, “eTrust Directory FAQ v3.6”, URL: http://www3.ca.com/Solutions/Collateral.asp?CID=33199&ID=160 (6 April 2004). Page-2
76. Computer Associates®, “eTrust™ Audit Managing eBusiness Security”, URL: http://www3.ca.com/Files/DataSheets/etrust_audit_pd.pdf (6 April 2004). Pages 1-2
77. Computer Associates®, “eTrust™ Audit Managing eBusiness Security”, URL: http://www3.ca.com/Files/DataSheets/etrust_audit_pd.pdf (6 April 2004). Page-1

78. Computer Associates®, “Success with CA Brigham Young University Puts Its Faith in eTrust™ Security”, URL: http://www3.ca.com/Files/SuccessStory/byu_etrust.pdf (6 April 2004). Page-1
79. Computer Associates®, “Success with CA Médiapost Adopts eTrust™ Admin and eTrust™ Single Sign-On to Reinforce Security of Critical Data”, URL: http://www3.ca.com/Files/SuccessStory/mediapost_adoptetrust.pdf (6 April 2004). Page-1
80. Computer Associates®, “Success with CA eTrust™ Directory Enables SECOM Trust.Net to Supply High-Level Security Infrastructure for the eMarketplace”, URL: http://www3.ca.com/Files/SuccessStory/secom_ss.pdf (6 April 2004). Page-1
81. Computer Associates®, “Partner in Health Care American Hospital Association”, URL: http://www3.ca.com/Files/Brochures/partner_healthcare_aha_ads.pdf (6 April 2004)
82. Nostalgia Central, “Hill Street Blues”, URL: http://www.nostalgiacentral.com/tv/cops/hillstreet.htm (6 April 2004)

Appendix-A

Phrase from which the $fRcLmYe! password was derived:

Friends, Romans, Countrymen, lend me your ears!