

MODERN NETWORK ACCESS CONTROL: LAYERED DEFENSE SECURITY STRATEGY

Copyright, 2006. [Guy Huntington, AuthenticationWorld.com](http://GuyHuntington.AuthenticationWorld.com)

This briefing is designed for senior managers wanting to know how to create a network access control strategy that will withstand modern attacks.

INTRODUCTION

The last several years has seen a major shift in how enterprises conduct business. Today, it is quite common to have customers, business partners, vendors and employees accessing information and applications deep within the enterprise. As a result, the enterprise firewall is no longer the defining bastion between the enterprise and the rest of the world.

In parallel to this, has been a change in enterprise attack vectors. Mostly gone are the days of hackers who simply want to prove they can bet your defenses. Ominously, organized crime has arrived on the global and local scene. They bring with them hundreds of thousands computer savvy criminals.

The first sign of this as the emergence of phishing attacks. By creating an enterprise look a like site and then sending out emails to unsuspecting users with a link in the email to the site, criminals have been raking in the money by capturing uids, passwords, credit card numbers and other identity information.

More worrisome has been the development over the last two years of botnets, rootkits and Trojan attacks. By using computer worms criminal gangs have been able to easily infect tens of millions of computers around the planet and essentially take control of them. They infected computers become known as “bots” and the network of bots controlled by organized crime as “botnets”.

The botnets are used to conduct organized crime money making efforts. These include:

- Capturing credit card on password information and auctioning them on line
- Threatening denial of service attacks on enterprises unless they pay a ransom

One gang in Holland was recently captured that ran a [botnet of 1.5 million computers](#).

Even more worrisome is the development of targeted attacks on enterprises. Rather than send out millions of emails with links to phishing sites organized crime is getting sophisticated. Instead they infect a MS Office attachment with malicious software (known as “malware”) and then send in a few emails to enterprise employees. The emails all look legitimate as does the document attachment. The emails and the

MODERN NETWORK ACCESS CONTROL: LAYERED DEFENSE SECURITY STRATEGY

attachments fly in underneath existing firewall and anti-virus protection. The employee clicks on the attachment and the malware deploys itself behind the enterprise firewall (this is known as a Trojan attack).

The malware is often a rootkit. This software deploys itself in the network software kernel. The rootkit then begins to capture ids, passwords and other sensitive enterprise information. It then sends this out through the firewall undetected. The enterprise is at high risk. It is very hard to detect as malware software evolves and it is very hard to remove. [Security experts are very worried about this development.](#)

To add more gloom, recently computer security specialists have admitted defeat against battling botnets. [Their prediction is that it will take at least one and more likely two years](#) to prepare new defenses able to withstand botnet attacks.

Another enterprise attack pattern is also emerging at cheaper price points. This is the use of hardware keyboard loggers. These small devices simply plug in between the keyboard and the computer. They don't install any software on the computer, so they will remain undetected by the enterprise firewalls and anti-virus software. They capture all information entered in via the keyboard. The criminal simply unplugs the small device, takes it home, and then downloads all the information.

The price point for this attack is \$60 and these devices are legally available all over the internet. It takes about 10 seconds to install. It's so easy that a child can do it. During the past year in the US, several students have been caught in different schools including [Houston](#), [Palm Beach](#) and [Boston](#) using the keyboard logger to download their teacher's id and passwords. One had spent two years changing marks for friends so they could get into university.

Organized crime also uses these. In [2005 in the UK](#), a group of criminals hired some janitors to install hardware keyboard loggers on a bank's computers. They obtained the uids and passwords. They were caught when they were transferring portions of 220 million pounds out of the bank.

What are your chances of your enterprise coming under such attacks over the next one to two years? They're very high, since local and global organized crime will be targeting enterprises, institutions and government agencies, all of whom are generally unprepared for such attacks.

What is the answer?

THERE IS NO MAGIC BULLET FOR THIS. There is no one hardware or software system which will defend the enterprise. The firewall and anti-virus manufacturers are often late in getting product changes out for documented attacks. [In fact it was recently reported](#) that for one documented attack four months ago only four anti-virus products had made the changes to detect and prevent the attack.

MODERN NETWORK ACCESS CONTROL: LAYERED DEFENSE SECURITY STRATEGY

The only answer is to have a network access control layered defense security strategy.

NETWORK ACCESS CONTROL: LAYERED DEFENSE SECURITY STRATEGY



YOU NEED A LAYERED DEFENSE!

The picture above is of a fort used during the middle ages to protect the kingdom against enemy attackers. Toward the top left hand of the picture you will see there are two sets of drawbridges to access the main part of the fort which is surrounded on all sides by moats and a river.

MODERN NETWORK ACCESS CONTROL: LAYERED DEFENSE SECURITY STRATEGY

Then there are the main outer-walls.



This assumed that the fort would be attacked and that the attackers would make it through the outer layers. Finally there was a last set of walls and defenses before accessing the inner keep.

How does this apply to modern enterprises?

The arms race in attack patterns means that:

1. Reliance upon the outer defenses of the firewall and anti-virus software to thwart most attacks is no longer valid. This is analogous to the drawbridges and the moats in the picture above. While it may act as a deterrent and keep out the lowlife attackers who are not very smart, it's not going to stop modern criminals from swimming across the moat and entering your enterprise (refer to the earlier references in this paper to confirm this).
2. Attacks must be thwarted as early as possible. Like the fort that had two drawbridges, you should be using a series of network protection in addition to your existing firewalls and anti-virus.
3. The fort above had narrow, heavily fortified entrances to screen visitors, thus preventing a surprise attack internally. You need to screen enterprise users better to ensure they are who they say they are. Remember the adage that 80% of attacks come internally in an enterprise.
4. You need a series of inner walls to thwart more sophisticated attackers. In the fort above, the designers used a series of walls to slow down attackers allowing them to be killed by the fort defenders. You need to construct a series of electronic

MODERN NETWORK ACCESS CONTROL: LAYERED DEFENSE SECURITY STRATEGY

walls that either slow down or prevent attackers from breaching towards the heart of the enterprise.

5. The fort used a series of guns to surround the inner keep. You need to have your best weapons for high risk networks, applications and information.
6. The fort kept an accurate watch list of who entered the fort and when they left the fort. Your enterprise needs to adopt an end to end user session audit trail that can quickly show where a security breach occurred and remedy it.

NINE LAYERS OF NETWORK ACCESS CONTROL DEFENSE

FIRST LAYER OF DEFENSE: IDENTITY REGISTRATION

When an employee comes to work for you, what kind of identity check did you do on them? Was there any criminal record check? Did you check out their education credentials? Do you do any kind of criminal or education background check on contractors and consultants working for you? What kind of identity check do you apply to customers who will be using your systems?

As the enterprise risk rises for applications and information systems your customers will be using, so to must the initial identity registration check increase. This layer of first line defense is usually poorly thought out in most enterprises, especially beyond employees. Are you checking your janitors, project contractors or temps?

Like the watch guard at the entrance to the fort, do more rigorous background checks before letting workers into the enterprise.

SECOND LAYER OF DEFENSE: USER TRAINING

Does your enterprise do any kind of annual training for all users of your systems about email, phishing and rootkit attacks? Are you strongly warning them about the danger of clicking on any links in an email document? This kind of basic training, while it might be ignored, put's some of the enterprise defense on the shoulders of its users. A 2-3 minute online flash presentation can be put together cheaply. It may result in your enterprise being able to avoid an enterprise breach at the firewall.

THIRD LAYER OF DEFENSE: DEVICE SECURITY CHECK

When a user tries to log on to your enterprise systems, is there a device check done? Is the software and hardware platform checked out and ensured that all available patches are in place? If not, before the device can even reach your network, is it placed in a quarantine area where patches can be recommended to be installed? If you're not doing this, using a device like from [Caymas](#), then you're enterprise is open to unexpected forms of attack.

FOURTH LAYER OF DEFENSE: INITIAL IDENTITY AUTHENTICATION

Your users, if you're going to require password authentication (which is the weakest form of authentication) should enter in their id and password using a keyboardless entry.

Companies like [RSA](#) and [Bharosa](#) provide excellent tools allowing you to minimize the risk of keyboard hardware and software attacks.

DO NOT USE KEYBOARDS FOR PASSWORD ENTRY...IT IS TOO RISKY TO BE CAPTURED. Do not trust password authentication for medium and high risk enterprise applications (read the paper "[Why your use of id and password is likely a joke](#)").

Further, if the user is coming in via a wireless device are they given more restricted access privileges than if they are logging on from inside the enterprise? If not, then you should be rethinking your enterprise security strategy. Wireless device authentication methods are relatively easily breached. Therefore, limit your enterprise risk by either restricting access to low risk applications or, requiring stronger authentication from the user's wireless device in order to access higher risk networks, applications and information.

FIFTH LAYER OF DEFENSE: QUICK PROVISIONING AND DE-PROVISIONING

When a user no longer requires access to your enterprise, an application, building, room, network, etc., how long does it take until they are de-provisioned? Many enterprises have very weak to poor provisioning and de-provisioning processes. In today's age, this puts the enterprise at greater risk, since a user who is gone may still have access to the enterprise. Put in place the infrastructure to quickly add, adjust or remove someone from having physical or electronic access to your enterprise

SIXTH LAYER OF DEFENSE: STRONGER AUTHENTICATION

As the enterprise risk rises for networks, applications and information access, so too must the layer of authentication strength. The financial system, payroll and payables are all higher risk. So too are users who hold super-user privileges like senior network administrators.

For all of the medium and higher risk applications, your enterprise should be using a graded series of stronger authentication. For instance, low to medium risk might be addressed by the user providing their id, password and a digital certificate.

Medium risk should be addressed by the user providing things like a secureID token along with their id and a password.

Medium to high risk should be addressed by the user providing something like a smart card, a secure id token, a biometric and a second unique password.

MODERN NETWORK ACCESS CONTROL: LAYERED DEFENSE SECURITY STRATEGY

Can your existing security and identity sign on systems support this? Do you have budgets for this? All of this requires senior management support to successfully implement.

SEVENTH LAYER OF DEFENSE: RE-IMAGING NETWORK OPERATING SYSTEMS

Are you prepared for a successful rootkit attack against your enterprise? Currently, Microsoft is recommending that the best way to recover is to re-image all desktops and servers affected! This could bring your IT department to a halt. Are you prepared for this?

Don't rely upon the firewall and the vendors. While they will assure you of their defensive abilities, the chance of an attack getting underneath the firewall is currently a lot higher than they would let you believe. If you are the unlucky enterprise who gets hit by a rootkit attack before the firewall vendors figure it out, then you had better be prepared to deal with it and fully recover, quickly and at low a cost as is possible.

EIGHTH LAYER OF DEFENSE: TRANSACTION AUTHENTICATION

The emergence of numerous attack vectors on an enterprise means that enterprise must assume that criminals will successfully penetrate their outer layers of defense i.e. the firewall, the authentication systems and even stronger authentication. The answer to this is to deploy transaction authentication.

In transaction authentication, software watches the following:

- IP address being used by the user
- Geo-location of the user
- Time of day the event is occurring
- Historical user pattern
- Computer hardware the user is using

If any of these criteria are different than expected, even with a successful authentication, the transaction authentication software will start alarm bells ringing in the enterprise.

This may result in:

- The user being asked all sorts of personal questions to verify it is really them
- Security or business managers being paged in real time
- The event, process or transaction refused

All enterprises should be using this type of software to protect high risk applications like payables and other sensitive applications. [RSA](#) and [Bharosa](#) are recommended vendors.

NINTH LAYER OF DEFENSE: ENTERPRISE REAL TIME AUDITS

The final layer of defense is the ability to quickly go back in minutes, hours, days, weeks or months to find out every network, application, information resource, type of device used, building and room the identity used at a specific point in time. All too often, the audit data is very hard to interpret from an application audit trail and worse, hard to integrate with other audit data from other applications.

Get a team organized on trying to provide an end to end user audit that is quickly available, easy to access and use. This will help you find out where problems and breaches occurred and then prepare remedial action.

CONCLUSION

The arms race is currently favoring criminals who want to attack your enterprise. They have a large talent pool to draw upon, a wide variety of tools and many an unsuspecting enterprise to go up against. You don't want to be that enterprise!

Admit reality and decide you need a layered network access control defense. Start with the outer moats and construct your drawbridges and defenses to slow down and thwart the unsophisticated attackers. Then construct an increasing set of defenses to weed out inside criminals and minimize the damage when the more sophisticated criminals break through the moat. Slow them down using stronger authentication and stop them from stealing the enterprise crown jewels by using defenses like transaction authentication.

With this in place you will sleep better at night knowing that the enterprise is well defended at all layers. While battles may be lost along the outer walls over the next two years, the war will be won by your enterprise having a layered defense preventing the criminals from walking away with their loot.

ABOUT THE AUTHOR:

Guy Huntington, President of Huntington Ventures Ltd, has many years of experience leading large, complex, Fortune 500 identity projects. His work has included leading Boeing's single sign on, Capital One's single sign on, Capital One's Sarbanes-Oxley provisioning project and Kaiser Permanente's web single sign on review.

He maintains a website at www.authenticationworld.com . He also maintains an authentication blog available off his website. He can be reached at guy.huntington@authenticationworld.com or by phone at 604-921-6797.