

**BATTLING THE BOTNETS AND ROOTKITS:  
A LAYERED IDENTITY STRATEGY USING  
ENTRUST AND SUN IDENTITY MANAGER**

**A WHITE PAPER**

**Author:**

**Guy Huntington**

**President**

**Huntington Ventures Ltd.**

**“The Business of Identity Management”**

**Date: April 21, 2006**

**BATTLING THE BOTNETS AND ROOTKITS: A LAYERED IDENTITY STRATEGY USING ENTRUST AND SUN IDENTITY MANAGER**

The emergence of organized crime using sophisticated malware attacks (keyboard logging, phishing, botnets, rootkit attacks, Trojan Horse, etc.) is quickly highlighting the weaknesses of individuals and enterprise security systems. For example, in [March 2006](#), Russian organized crime used rootkit software. This places malicious code at the heart of the Microsoft operating system. The code was installed when a user visited certain sex websites. It then watched for when a user entered uid and password information for banks, dating, social websites and email. As the data was entered, in seconds, the rootkit software then began passing the information back to a Russian web server. Over four day's time 90,000 pieces of user information from 6,500 companies was sent before the server was shut down.

Organized crime now sells millions of uids, passwords, social security and credit card numbers in eBay type auctions. For example a web mob named Shadowcrew: [“In the past two years, the Shadowcrew's 4,000 members, according to the U.S. Secret Service, ran a worldwide marketplace in which 1.5 million credit card numbers, 18 million e-mail accounts, and scores of identification documents—everything from passports to driver's licenses to student IDs—were offered to the highest bidder.”](#)

As well, the code for writing these types of attacks has become modularized. This allows the criminal to effectively order a piece of code that performs specialized functions. Further, the code can be checked before purchase by the criminal to ensure it will bypass the enterprise's existing intrusion detection systems. [Code is being offered at \\$25 per 10,000 hijacked computers it infects.](#)

The increase in phishing attacks (where the user is directed to a fictitious site resembling the enterprise web site and then entering in personal identity information) as well as keyboard logging attacks by both hardware and software devices is also part of the organized crime toolkits. [McAfee in April 2006](#) stated that the increase in Windows based stealth components was 2,300% from 2001 to 2005.

The bottom line? You need to have an enterprise security strategy that keeps one step ahead of the game. You don't want to face lawsuits from your employees or customers for not protecting their personal identity data. Nor do you want to have impostors successfully logging on to your systems and perpetrating crimes against your enterprise. Finally, you definitely don't want to be in the media explaining why your security was breached.

The existing intrusion detection systems, even the best ones, are insufficient on their own to preventing all types of attacks. The result is that enterprises need to adopt a multi-layered identity security strategy that adapts to these types of attacks and mitigates enterprise and user risk. This paper examines the strategic framework for such a strategy.

## **Battling the Botnets and Rootkits: A Layered Identity Strategy**

### **FIRST LEVEL OF DEFENCE: IDENTITY VALIDATION**

Do you really know the identities physically and electronically entering your enterprise? How do you know? Has there been any background check done on them? A criminal check? Presentation of a passport? A driver's license?

All of these ways of validating an identity have different degrees of trust one can put against them. There are new types of identities you should also be thinking about; for example...janitors.

In [2005 in the UK](#), janitors installed hardware keyboard loggers on user's keyboards in a bank. This led to an attempted theft of \$200 million pounds. Even if the computers are turned off when the janitors are in late at night cleaning, it means that they are now easily attackable by using janitors to install the device.

Even if you use a stronger type of identification, such as a passport, these too can be easily fraudulently obtained in many third world countries. Therefore, while identity validation is the first step in a layered identity strategy, your level of trust and reliance upon these mechanisms should be relatively low unless a full background check is conducted by the police.

As part of the strategy, determine all types of identities who are currently working physically or electronically in your enterprise. Then assign them the level of identity validation you think is acceptable to the enterprise relative to their risk.

## **Battling the Botnets and Rootkits: A Layered Identity Strategy**

### **SECOND LEVEL OF DEFENCE: PROVISIONING**

The next layer of defence concerns providing what applications, assets and system access a user is entitled to AND EQUALLY quickly removing this access when their job changes or they're left the enterprise. Current best practice is to use a provisioning tool, such as Sun Identity Manager, that automatically provisions and deprovisions the user with workflow approvals as required.

The benefit from this is that enterprise security is strengthened by:

- Quickly reacting to status changes in workers
- Removing access to workers who no longer need access
- Eliminating existing workflow business process holes for providing application and asset access

The same tools also provide regulatory reporting. This is important for Sarbanes-Oxley, Patriot Act and other national, international and state level regulatory reports.

Implementing these systems can be time consuming and expensive depending on your enterprise. It assumes that there are:

- Authoritative sources for different identity types
  - Not always the case for contractors,, temps, consultants, business partners, outsourced third parties, etc.
- Good business processes already in place
  - Often there aren't thereby requiring significant effort, time and politics to re-engineer

Provisioning people who are coming into your enterprise from third parties is now becoming common. This requires the implementation of:

- Legal contracts with third party outlining:
  - Validation of the identities taken by the third party
  - Identity information to be supplied by the third party to your enterprise
  - Provisioning standards to be established and maintained by the third party for their identities
    - So you have a high degree of confidence that when a third party identity undergoes a role change or leaves the enterprise, you will be automatically notified
  - Authentication standards to be used by the third party
  - Authorization information, if any, to be provided by the third party
- Implementation of federated identities for provisioning as well as for authentication

## **Battling the Botnets and Rootkits: A Layered Identity Strategy**

### **THIRD LEVEL OF DEFENCE: LOW RISK AUTHENTICATION**

Your next layer of identity defence is to have a set of authentication mechanisms for low risk applications, documents and network access. The use of uid and password entered in by keyboard is no longer best practice on its own. The use of hardware keyboard loggers means that even the most sophisticated intrusion detection system won't pick this up. Further rootkit attacks means that anyone entering in data via a keyboard is possibly open to attack.

You therefore have two general choices:

- Continue to use the keyboard
- Use keyboard less authentication

#### **Continue to Use the Keyboard**

The continued use of the keyboard for entering in passwords is fraught with high level risk. If you decide to continue down this path you must strongly consider the following options:

##### *Second and Third Factor Authentication Mechanisms*

The financial industry has learned over the last three to four years that one of the best methods if using a keyboard and mitigating risk of attack, is to use software that provides additional authentication information in real time and detects an attack in progress.

Today this software is available commercially from several vendors such as [Entrust](#). It monitors:

- Physical configuration of the user's computer

The person who has successfully stolen a password and then logs on as the user may be picked up in real time if they log in from a different computer.

As organized crime adapts the modern attack tools, non-financial enterprises such as medium sized businesses, universities and local government all become potential targets. Good applications for using this software are for managers and clerks of sensitive areas of enterprises such as payroll, payables, human resources and user data. There is however privacy concerns that need to be addressed when using this type of software. Users in Canada and Europe will need to be told that their home computers will be monitored for hardware and their IP addresses when they use them to log on to enterprise systems.

## **Battling the Botnets and Rootkits: A Layered Identity Strategy**

### **Use Keyboard-less Authentication**

Vendors like [Entrust](#) make several types of authentication mechanisms that are very robust and don't use a keyboard to enter in data. Entrust Identity Guard provides a series of mutual authentication mechanisms to mitigate the risk from Phishing, Trojan Horse and man in the middle attacks by using:

- images selected by the user
- viewing of serial numbers known only to the enterprise and the user
- SMS or cell phone calls to confirm identity

### **Recommendation:**

My recommendation is to use something like [Entrust's Identity Guard](#). This hardens up your general first level authentication. Should the password be obtained, Entrust's Identity Guard has various additional ways of confirming the identity is who they purport to be. This effectively minimizes the risk from litigation from your users that best efforts were not taken to protect their identity data.

### **Federated Identities Authentication**

The occurrence of federated identities within enterprises is now becoming common. As referred to in the prior Provisioning section of this paper, a number of contractual decisions need to be made. Once this has been agreed upon the next challenges are managing the federated identities.

Modern identity vendors such as [Entrust](#) provide identity federation as part of their access toolkit. Based on the contractual and enterprise risk decisions you make, you must then configure the toolkit to allow for:

- Trusted authentication to take place
  - This usually means accepting the third party's sign on mechanism and letting their users into your enterprise
- Additional authentication and authorization as required
  - Asking the user for more authentication and/or authorization information

### FOURTH LEVEL DEFENCE: MULTI-FACTOR AUTHENTICATION

Many types of documents, applications and some networks will be higher risk to the enterprise. For the identity to successfully access these, a stronger authentication and authorization information should be provided. Best practice is to use multi-factor authentication.

There are a number of authentication mechanisms available for use:

- Digital certificates
- Security tokens
- Smartcards
- Biometrics

#### **Digital Certificates:**

Digital certificates offer the ability to provide proof that the user is trusted by a third party i.e. the Certificate Authority. Over the last three years, digital certificate management costs have decreased making these a viable authentication mechanism in many enterprises.

#### **Security Tokens:**

Security tokens usually contain changing authentication digits which only the host server will be able to match to. Security tokens have higher operating costs than other techniques associated with issuing and maintaining them as they are often lost and require replacement.

#### **Smartcards:**

Smartcards are plastic credit card sized cards that can contain a variety of digital authentication mechanisms on it. These can include digital certificates, changing authentication numbers and biometric data. They are rapidly gaining in wide use acceptance.

## **Battling the Botnets and Rootkits: A Layered Identity Strategy**

### **Biometrics:**

A wide range of biometric devices are available and being implemented in passports, cell phones, etc. Some types of biometrics are easily foiled e.g. some type of finger scan cards. Others have high false error rates. Further, biometrics can change as a person ages. Their deployment cost is decreasing but still requires hardware to detect the biometric.

### **Recommendation:**

Use a combination of the above technologies to ascertain the identity of the user. For example, if a user who's successfully logged in using a keyboard-less uid and password, tried to access a sensitive application you might require them to provide an additional password coupled with a digital certificate and/or a biometric.

The use of different combinations can be used to:

- Target smaller groups of higher risk users
- Keep implementation and maintenance costs down
- Ensure the identity is who they say they are

For highly sensitive applications, many enterprises set time limits after which the user is forced to re-authenticate. For example, a user named Jane who's accessing the Payables system for large customers may be required to re-authenticate every 15 minutes.

The use of these strategies can also be applied to document management. For example, Adobe's Livecycle provides document authentication. Therefore, if a document is low risk, there will be no authentication required. Medium risk documents may require the user to use their keyboardless uid and password to open. High risk documents may require multi-factor authentication to open.

## **Battling the Botnets and Rootkits: A Layered Identity Strategy**

### **FIFTH LEVEL OF DEFENCE: AUTHORIZATION**

The implementation of an enterprise identity management infrastructure is critical to helping provide authorization. Modern enterprise architecture uses levels of authorization from the enterprise level before even allowing the user access to the application.

Therefore, when a user successfully logs on, they are automatically granted certain privileges based on attributes in the enterprise directory. Thus a user named Guy will be shown the employee portal page because one of his attributes is employee and not contractor. The contractor will see a different portal page when they log on.

The next step is to use attributes that automatically dynamically assign the user to groups. Thus a user named Guy may automatically be given access to several different HR applications because his department attribute is HR. Other employees or contractors will never even be allowed access to the applications.

The final step is the authorization information that is used to grant application specific access. Thus a user named Guy may be successfully granted access to the enterprise's Human Resource Management System (HRMS) but only be allowed low level access since he is a HR clerk.

Managing authorization in large enterprises can be extremely challenging. Many role based access projects fail because of the:

- Number of roles required
- Internal political challenges in getting approval for role definitions
- Maintenance of roles in a fast changing environment

#### **Recommendation:**

- Go for the low hanging authorization fruit first
  - High level enterprise groups
- Next focus role based access control in areas where the number of roles is well defined, changes slowly and is well maintained
- Avoid enterprise wide role based access control projects

A number of the main identity product vendors such as Entrust provide the ability to the enterprise to effectively manage the use of groups. Use of these types of tools can quickly help an enterprise achieve quick sustainable wins in providing some degree of enterprise authorization.

## **Battling the Botnets and Rootkits: A Layered Identity Strategy**

### **SIXTH LEVEL OF DEFENCE: AUDIT**

If an attack is successful then audit files are the historical trace back through time to see what happened. The author strongly recommends use of an identity management product like Entrust to provide an end to end trace of a user's session. Without this, you are forced to access many different independent audit files to begin reconstruction of what a user did during a session.

Make sure that you keep good audit records for long periods of time. This will enable good analysis done and reconstruct the path of the crime.

Products such as Adobe LiveCycle also need to be taken in consideration in audit. For higher risk documents, you can create an audit file showing the entire use of the document through its life-cycle. When this is combined with the identity vendor's audit file, it provides an end to end usage from when the user began their session, the applications they touched and what they did with sensitive documents.

## **Battling the Botnets and Rootkits: A Layered Identity Strategy**

### **CONCLUSION:**

Today's digital world is becoming an arms race as attackers increase their sophistication in attack vectors. Further, the likely targets are no longer the defence and financial sectors. Mid-sized enterprises, educational institutions and local government are now also high quality targets for local or international organized crime.

In addition to your existing intrusion detection systems, you need to create architecture of layered identities. This must include:

- Validation
- Provisioning
- Low risk authentication
- Multi-factor authentication
- Authorization
- Auditing

Modern identity tools from vendors such as Entrust provide the overall framework for managing this throughout the enterprise. By using Identity Guard and Sun Identity Manager you can provide effective second and third level authentication with stronger keyboard-less authentication. This provides you with a strong underlying platform to provide your second and third levels of identity defence.

It offers enterprises the ability to meet privacy compliance regulations and demonstrate they are making best efforts to protect user identity data. Further, it better protects the enterprise from attacks by impostors who have successfully obtained the user's uid and password.

You also need to consider integrating products like Adobe LiveCycle into your enterprise to protect your documentation. This should also be integrated with the identity vendors like Entrust to provide a seamless way of managing identities and security policies from one central place. Additionally, the documents of higher risk should use identity authentication.

This layered identity structure mitigates risks from modern day attacks. It provides enterprises with cost effective ways of applying more expensive risk management solutions to only those users who are high risk.

## **Battling the Botnets and Rootkits: A Layered Identity Strategy**

### **ABOUT THE AUTHOR:**

Guy Huntington is an independent identity management consultant. He has been the lead consultant on several large Fortune 500 projects including Boeing's global single sign on, Capital One's single sign on, Capital One's Sarbanes-Oxley provisioning and Kaiser Permanente's web single sign on review.

Guy is happy to assist you with developing a layered identity strategy. He can be reached at 604-921-6797, [guy.huntington@hvl.net](mailto:guy.huntington@hvl.net) or [www.hvl.net](http://www.hvl.net).