

IDENTITY MANAGEMENT - A KEY PART OF A UTILITY CYBER AND PHYSICAL DEFENSE

A SUBMISSION TO THE UTC CYBER-SECURITY WORKGROUP

Author:

G. Huntington

President

Huntington Ventures Ltd. – “The Business of Identity Management”

Date: February 24, 2009

Table of Contents

Identity Management - a Key Part of a Utility Cyber and Physical Defense	1
Introduction	3
What is Identity Management?	3
Perimeter Defense	4
Perimeter Authentication Strength	4
Who Gets Access to Your Systems, Buildings and Apps?.....	5
Physical Master Building Key Issuance, Tracking and Recovery.....	6
Central Security Ops Command Console.....	7
Web Services.....	8
Federation.....	9
SCADA and Identity Management	10
Regulatory and Audit Reporting.....	11
Conclusion	12
About the Author	12

Introduction

A modern defence against cyber-security and physical attacks against a utility involves having many layers of defence. From the physical and electronic perimeters of SCADA and IT through to applications, HMI's and RTU are using stronger levels of authentication and encrypted communications where risk warrants it. Additionally, having quick processes to quickly remove an identity from physical and logical security access when the identity is terminated reduces the risk of insider attacks. Finally, having a central security ops command console combining SCADA, IT and physical security is also vital to determining early on if an attack is in progress.

This paper will outline why identity management is critical to utility cyber and physical defense layers. It will show for each of the security layers the key part identity management plays and how it interacts with other utility infrastructure.

What is Identity Management?

It is the business processes, technology and people that provide for:

- Provisioning – how identities are created, have role changes and are terminated as well as which access rights (physical and logical) are assigned to them as well as what assets are also assigned and recovered
- Access Control – identity management applies to web and non-web based access control using enterprise security policies applied based on enterprise risk. Note that access control also applies to app to app and system to system interactions (since these too are all identities)
- Identity Management – ability for users (workers or customers) to do self-serve on their identities, provide identity search and do on-line org charts dynamically created
- Web Services – ability to use XML between app to app interactions
- Federation – ability to build trust between different enterprise business units or between one or more enterprises. This allows users to not have to re-authenticate as often when they are going from one enterprise to another where contractual trust has already been agreed upon
- Regulatory reporting – the provisioning system can easily generate “attestation” reports for managers to easily and quickly verify what workers are still reporting to them and what their access rights are. These are then aggregated and can easily be reported to regulatory agencies
- Audit Reports – the provisioning and the access system can quickly provide auditors or forensic security people with a record of which identities access a system or app at a specific time

Perimeter Defense

On the SCADA and IT systems there is usually these types of perimeter defences:

- Anti-virus
- Firewalls
- Intrusion Detection
- Intrusion Prevention
- Web Security (e.g. Finjan)
- DMZ
- Physical access controls requiring authentication
- Logical access controls requiring authentication

Identity management has a role to play at the perimeter. The SCADA and Enterprise identity management systems should be reporting to a central security command console the following data and trends:

- Failed authentications both physical and logical
- Number of authentications per second and per minute
- Number of authorizations per second and per minute
- Door entries per minute per facility per location in the facility

These are all early warning signs of potential attacks. For example, when the number of authentication attempts dramatically rises, it could be a denial of service attack. Unusual door entries at a specific time might be matched to subsequent unusual network logins from the same physical area.

Perimeter Authentication Strength

Different logical and physical areas of the perimeter will have different risks. For low risk areas, the identity management system will enforce uid and passwords or presentation of a security badge. Medium risk areas might use things like one-time password tokens, smart cards, biometrics or combinations thereof. High risk areas will use multiple authentication methods.

Identity management provides an enterprise framework to apply and enforce different authentication methods and centrally report this on a continual basis. This is a significant advantage to each app, RTU etc, applying their own authentication and tracking it locally.

Who Gets Access to Your Systems, Buildings and Apps?

Human Resources is normally authoritative for the identities of employees and often students. They may or may not be authoritative for contractors, consultants and third parties. Often Purchasing and Finance might be involved. For suppliers it is often Purchasing and Facilities.

So what happens in most enterprises is that emails and paper or electronic forms are criss-crossing the enterprise to let people know that an identity is here and needs certain access rights. Especially with contractors and suppliers, these processes often are slow or breakdown, especially when it comes to letting systems, apps and facility physical security people know that an identity has been terminated.

These processes often provide significant attack vectors. For instance, a contractor may be coming on to your site. The end date isn't put on the form or email. The badging person then applies a year to the badge. The contractor who has left after one month's time with their security badge has eleven more months of access until someone notices.

Identity management is a process. Therefore, no technology is going to solve this problem on its own. A key component of an identity management system is to have an enterprise identity management committee that first of all determines the processes for each identity type: creation, modification, extension and termination.

Then agreed upon identity triggers are agreed. These are points in the process where the identity is legally contracted and the identity has been created in an authoritative source. At this point then identity management technology can appear.

Workflows for the identity can be electronically done giving them automatic, semi-automatic or manual approvals for system, application and physical badging. The provisioning component of identity management can provide for different workflow paths; electronically divert the request after a pre-determined period of time when no approval has been given, etc.

The combination of the identity business processes with the provisioning service provides for much greater overall enterprise security. When an identity is created, the identity's badge can be waiting for them at the front desk and their computer, apps and system access can all be waiting for them.

When a role change occurs, the identity management system can quickly pick this up and enforce changes to apps, systems and security badges. Normally, in most enterprises, role changes are not well tracked resulting in security creep (i.e. the person inherits more and more access rights without losing any).

When an identity is terminated, within minutes the provisioning system can quickly remove all access.

Physical Master Building Key Issuance, Tracking and Recovery

Many enterprises have master building keys that are lost or not returned. In one instance at a utility, they found a person walking around their main generation station. The person had been one of the builders and years later came back to have a look around using their master building key they still possessed.

These keys are critical to security since they allow a person to often bypass electronic physical access controls. Identity management systems can assist in this area.

The building keys and master keys should all be placed in the central IT asset management system (e.g. Remedy). When an identity is created, the provisioning system might automatically request a certain type of key for the identity based on their role. Exception processes require management approval using the identity provisioning workflow engine. The key administrator might receive the request from the identity management system and close off say the Remedy ticket after issuing the key.

When an identity undergoes a role change, the provisioning service would check to see if the key needs to be upgraded or recovered. It would then send the identity's current manager this request if the key is to be recovered. The ticket remains open until the manager recovers the key. Escalation to security and senior management personnel can be automatically done by the provisioning service at pre-determined points of time.

When an identity is being involuntary terminated, the identity management system can instantly provide the identity's current manager and/or HR with a list of assets the identity has in their possession. They can use this to recover the keys and then close the ticket.

Central Security Ops Command Console

All utilities have SCADA command centres. They usually have separate IT security ops centres which are frequently separated from the physical command centres. In today's age, where there are numerous different attack vectors, it makes sense to have an enterprise security ops command centre monitoring the security for SCADA, IT and physical security on the same consoles.

Identity management has a role to play here. It is the source of some of the critical information flowing to the consoles. As mentioned earlier in this paper, it should provide things like:

- Failed authentications both physical and logical
- Number of authentications per second and per minute
- Number of authorizations per second and per minute
- Door entries per minute per facility per location in the facility

Web Services

Many enterprises are just considering the use of web services internally, especially in Purchasing and within IT. However, web services are prone to attacks if not properly planned for.

Most web services use XML (eXtensible Mark-up Language). This allows for rapid integration between different enterprises using different applications (such as Purchasing who might want their key suppliers to automatically be able to query the inventory management system and provide just in time delivery of widgets). However, XML through a firewall significantly increases enterprise risk.

For example, a document that has a buffer overload attack will hopefully be stopped by your firewall. However, the same document as an XML attachment will pass through the same firewall.

To mitigate this risk, enterprises deploy XML Firewall/Gateway servers. These are essentially the policy enforcement point or enterprise sentries. The policies for the web service are held in the identity management system.

This provides the enterprise with a scalable solution for one web service to thousands of web services. It reduces risk of cyber-attack from this new way of doing business internally or externally.

Federation

Identity federation is the ability to build trust electronically between two or more different enterprises. This often results in the user not having to re-authenticate or as often when they cross out of their enterprise to another.

Federation poorly done can enable a possible attacker a way into your networks. Properly thought through, federation can enable an easier user experience in your enterprise.

SCADA and Identity Management

Many SCADA operators are rightfully scared of IT. IT changes things quickly and their systems are not always available. Therefore, creating an interface between IT and SCADA is not desirable from a security or process perspective.

However, in today's emerging world of IP based SCADA networks, out-sourcing, digital cert management for SCADA assets, using stronger authentication, CIP regulatory reporting and having central command consoles requires some form of identity management within the SCADA system.

I am currently working on a target architecture that would provide for an independent identity management system within SCADA and DCS. It would interface via an internal DMZ with the enterprise identity management system.

I am very interested in providing the working group with a white paper addressing this to seek comments, criticisms and suggestions.

Regulatory and Audit Reporting

As other industries have found when under regulatory reporting requirements, the identity management system can significantly lower reporting costs and personnel time required. All access control reports (using the attestation features previously described in Provisioning), can be quickly and automatically formatted to CIP reports.

This means the end of spreadsheets and isolated databases to figure out who had access to what asset or system or application or facility yesterday, last week, and last month, last quarter or last year.

Internal auditors will love the capability of being able to see that higher risk areas have stronger authentication. They can also see how segregation of duties is enforced both logically and physically.

Forensic analysis can be quickly done to determine what physical and logical access an identity had over a specific time period.

Conclusion

Identity management should become one of the key security cornerstones in your enterprise. It provides a framework to help mitigate risk of cyber, physical or combined attacks. It allows the utility to grow and adjust its security architecture over time as new threats emerge.

About the Author

Guy Huntington, President, Huntington Ventures Ltd., has lead and rescued many large Fortune 500 identity projects including Boeing, Capital One and Kaiser Permanente. He has also lead Toronto Hydro's identity project and been instrumental in developing their security architecture. Guy can be reached at guy@hvl.net, www.authenticationworld.com or cell at 604-861-6804.