

Risk and Trust

Author: Guy Huntington, President, Huntington Ventures Ltd.

Date: October 20, 2010

Table of Contents

Risk and Trust.....	1
Executive Summary.....	2
It's All about Risk.....	2
Today's Enterprises.....	3
You Need to Start With Risk.....	3
Trust Chart	4
Business Need.....	5
Now You Can Begin Your Business Case and Decide Which Vendor to Buy.....	5
It's Getting More Complicated!	6
Summary	7
About the Author	7

Executive Summary

In many enterprises I have been in, I'm usually asked "What's the best authentication method to use?" or "What do I recommend?" The reality is both of these questions are wrong. The purpose of this paper is to illustrate for the reader:

- Why this is so
- Explain a risk framework
- Frame the discussion about significant sea changes in the internet that are rapidly approaching

It's All about Risk

What is authentication? It's a way of measuring trust about a person trying to gain entry. In the medieval days, trust was a soldier by a door who asked "Who goes there" and using his knowledge of the person (his memory, his five senses and his instructions on who to allow or deny) allowed them entry or not.

As time progressed, identities that were traveling from one place to another were often given tokens to present at the other end. There was something that the two parties had agreed upon in advance to establish trust. So if I showed up at your door presenting you with a special piece of cloth, gold, etc. you would examine it and, if it looked the one you had agreed to, you granted me entrance.

In other cases, the two parties would agree on a secret password. The knowledge of this was very limited to only the two parties and to whomever they told the secret to. Thus, when I arrived at your door and told you the secret password that you agreed upon, you granted me access.

The three examples above are of something you are, something you have and something you know. They are all ways of measuring trust.

As life got more complicated there was a growing trend of people masquerading as another. For example, people in the past who were carrying tokens might have been murdered en route and their tokens used by the murderer to gain entrance to the castle. Thus people learnt the hard way that there are degrees of trust.

This led to parties agreeing to use combinations of three methods. So, when you show up at the castle gate and present the stolen token but don't know the password, then you are lead to the dungeon instead of the king or queen.

The point I am making is that the degree of trust required is dependent upon the degree of risk. For example, the ruler might have open gates to their outer walls of the castle, allowing trades people in to conduct their trade while having stronger degrees of authentication for different doors leading into the inner walls and sanctuaries of the castle. The rulers decide that the risk for the outer layers is very low while the inner sanctuaries have higher degrees of risk. Based on this, the rulers then use different authentication methods e.g. a token to gain entrance beyond the outer walls, a token and a password

for the next door and finally only allowing someone in to the inner sanctuary who the rule can see and recognize before granting them access.

Today's Enterprises

Modern enterprises have identities passing through their electronic and physical walls all the time. However, I have frequently found that, unlike kings and queens of old who would have done their risk assessment and constructed the castle accordingly to risk (i.e. having moats out front, drawbridges and then tougher levels of access to the inner sanctuary), most enterprises have the moat out front (their DMZ, firewalls and physical access controls to the buildings) and then use a uniform unique identifier and a password to allow access internally and...that's normally about it. Common exceptions to this statement are financial and military enterprises which often have more different layers of authentication (like RSA tokens and smart cards).

Whenever I see reliance upon the uid and password, the first image that comes to my mind is the enterprise as a giant mash mellow that's just been toasted over a campfire. The outside is a little hard but when you push in through it, underneath it's all soft and gooey.

Then I normally laugh inside myself when someone in these enterprises asks me what "other" authentication method should they use? The question is laughable since they are letting the tail wag the dog. In this case, the tail is the measure of trust. The dog is the enterprise risk. I laugh since how can one measure trust without first deciding on the risk? All too often, the question is a result of some authentication sales person trying to sell their method of measuring trust.

You Need to Start With Risk

Before leaping to measuring trust, the first requirement is to establish risk. This is the hard part, since it involves getting management to agree to do a top to bottom enterprise risk assessment for logical and physical access. This means pulling people together across the enterprise to look at all networks, applications and physical areas within the enterprise and then evaluating it for risk.

Risk itself is variable and can be defined several ways. For example there is business risk, intellectual risk and physical risk as just some examples. Each area and app needs to be rated (often this is a critical, high, medium and low rating). In today's complex digital world, the risk rating needs to go into the enterprise content as well. For example, the formula for Coke is extremely valuable or the contract details for an upcoming merger are high risk and thus need stronger measures of trust to be accessed.

What the enterprise needs is a risk framework such that new knowledge, information, applications and new physical access areas can be inserted into the enterprise risk framework up front as they are created. This framework is more than IT security or physical security. It needs business unit involvement to help categorize the risk as it evolves.

The process of doing an enterprise risk assessment can take much time. Therefore, while this is going on, one of the first things to do is to identify risk areas rated critical and begin with them, as the next two sections of this paper illustrates.

Trust Chart

The security gurus need to construct an enterprise “trust chart”. This is a table where methods of trust are rated from lowest to highest measures of trust. This requires some knowledge on means of authentication.

For example, at the bottom of the chart, you’ll likely have uid and password. This is easily obtainable through social exploits, by hardware keyboard loggers, etc. such that no matter how “strong” the password is, it is easily obtainable. Above this you’ll have one time passwords, smart cards, many different biometrics and then combinations of these i.e. multi-factor authentication using combinations of something you know, something you have and something you are.

I also want to point out here that biometrics are NOT A SECRET. Therefore, many enterprises are increasingly relying upon biometrics as if it was a secret. **This is wrong.** A biometric is something you are and is not a secret. If the biometric or the database upon which it is stored is stolen, then the biometric is useless. Further, the individual for whom it is stolen is now at greater risk and possibly inconvenienced for the rest of their life when the biometric is required.

The trust chart must also take into account new methods of authentication that will be developed. To address this, I normally get my clients to assign numerical values to these authentication methods: The higher the degree of trust, the higher the numerical value (usually on a scale of 1-100).

Then when the network, application or door entrance is required, the security sign-on software managing this is coded to accept a value. For example, let’s say that the identity is trying to access a medium risk area electronically and the value assigned to this is say 50. The person might present a smartcard and a password, whose combined score is 50 or more and would be granted access.

This allows new authentication methods to be adopted by the central security team without having to recode the access management software. So if a new form of biometric is introduced plus a password in the future, then the access control software doesn’t need to be changed.

The chart is then normally rated for critical, high, medium and low trusts. For example, low might be 20, medium might be 50, high might be 70 and critical 85.

Business Need

The next step is to then match up the enterprise risk assessment against the trust chart. This then matches critical risk to critical trust etc. HOWEVER, THIS IS NOT ENOUGH! The security teams needs to meet with the business and determine user acceptance of the trust authentication method being used. In many cases, they will not agree with the trust. Why?

Take a financial institution that has applications that can trade hundreds of millions of dollars. This will be rated critical. However, the business owners might not want the trader to have to spend time doing their authentication for a critical trust. Seconds are an eternity in trading. Instead they may simply want a proximity badge to gain access to the app. In situations like this, then compensating measures are normally introduced. For example, the financial institution might put the apps in a special trading area where there is lots of additional physical security taken as well as using software to monitor all trades the trader makes.

Therefore, all medium, high and critically rated risk business owners need to be consulted on the trust method being proposed to be used. If there is disagreement, then compensatory mechanisms must be found while using lower levels of trust for authentication.

Now You Can Begin Your Business Case and Decide Which Vendor to Buy

Once the risk assessment is underway and the trust chart agreed upon is the time to then begin doing business cases for implementation. Critical and high risk should be done first.

A different level of expenditure will often be allocated for protecting critical and high risk areas than for medium and low risk areas. The process I have described takes the enterprise out of silly discussions about using smart cards and tokens for most people. Instead the business discussion is focussed on risk assessment and containment.

Now you are ready to drop into what I call “vendor land” and determine which methods will work for your enterprise for a given level of risk. Obviously the management of the measure of trust must also be taken into consideration.

Things like smart cards and tokens are more expensive to manage than passwords. There are also false positives and negatives associated with different forms of biometrics. All of this must be factored into the business case.

It's Getting More Complicated!

Bob Blakely, of the Burton Group, wrote a paper "[The Emerging Architecture of Identity Management Version: 1.0, Apr 16, 2010](#)" and Craig Burton, of the Burtonian, wrote a paper in August 2010 "[The Advent of the Internet Application Platform](#)" that that I highly recommend readers of this paper get their hands on and read.

Bob's paper talks about the future of identity management moving from a push to a pull model. He sees the evolution of the business model to one where there are data clouds and information is coming into and out of the enterprise by being "pulled" rather than pushed and prescribes the beginning of new identity architecture to deal with this.

Craig's paper talks about the evolution of the internet and postulates the evolution of a new Burtonian layer called "Logical Endpoint" with a "purpose based web" and a "dynamic application protocol platform for the Internet". He uses [Kynetx](#) as an example. Things like mashups are also good examples of where Craig sees data being used from a variety of sources.

All of this requires risk assessment and trust frameworks that are not really in existence yet. What this means to the enterprise is that a significant sea shift is underway.

Enterprises that have risk assessment frameworks in place for logical, physical **and content**, and have trust charts and integrated enterprise identity management, access control and content management systems are in the best position to take advantages of the new opportunities that these two papers predict. Those that don't will fall significantly behind just as when the web hit industries 15 years ago.

This means that enterprises need to get their butts into gear now and lay the risk frameworks in place. This must include data classification since the data can become used in mashups, data clouds, etc and there will be system to system interaction requiring trust to be established as well as audit and billing rights.

Summary

Over my 13 years in the industry, I have watched the evolution of LDAP directories, SSO, provisioning and content management. What I see coming is an even greater change when internet application programming languages and data clouds come into being. All of this introduces new risk and requires different levels of trust measurement and recording.

The impact this will make on identity management and access control is very significant. To illustrate this, I finally suggest that readers also read [NIST's "WORKING DRAFT - A SURVEY OF ACCESS CONTROL MODELS"](#) published in 2009. It sees the evolution of access lists (ACLs) to Role Based Access Control (RBAC) to Access Based Control (ABAC) to Policy Based Control (PBAC) to Risk Adaptive Based Control (RADAC).

In the end, as we construct data clouds and programmable internet application, it requires risk based access. This needs to evolve quickly. I believe that the commercial pressures of licensing content will force this into being sooner rather than later.

About the Author

Guy Huntington has been in the identity industry for the last 13 years. He has rescued several large Fortune 500 identity projects and written numerous white papers on identity (<http://www.authenticationworld.com/papers.html>). Guy can be reached at guy@hvl.net or 1- 604-861-6804.