
It's All About Authentication

**An information security white paper to help focus resources
where they produce the best results.**

March 2005

**Author: Doug Graham, CISSP
Senior Director
Blue Ridge Networks®, Inc.**

It's All About Authentication

Author: Doug Graham, CISSP

**Originally published March 15, 2003, SANS Institute.
Updated March, 2005**

Table of Contents

Abstract.....	3
Five Layer Security Model	4
Authentication	4
Authorization	6
Encryption	7
Integrity	7
Audit.....	8
Summarizing the definitions.....	8
Summary.....	9

Blue Ridge Networks is a registered trademark of Blue Ridge Networks, Inc. Other names used herein may be trademarks of their respective owners.

Abstract

Information security professionals who seek to reduce vulnerabilities in their organizations are presented with an overwhelming number of options that cover the entire information security landscape. With the dichotomy of ever-increasing organizational demands, and fewer and fewer resources – both financial and human to meet those demands, where in the information security arena do you invest to maximize the return on your investment?

This paper simplifies and categorizes some of the core fundamentals of electronic security controls and mechanisms, and concludes that authentication may be the single most important aspect in information security. It further challenges the validity of other security controls that may be adopted by organizations prior to implementing a strong and robust authentication system.

A Five Layer Security Model

Let's begin by attempting to slice security into five different layers as seen below in Figure 1.



Figure 1: Security Pyramid

It may be argued that physical security is a component missing from this model. However, this paper intends to focus on electronic security controls and countermeasures. Two points do need to be mentioned:

1. a robust physical security model is essential to build a strong foundation for electronic security
2. some of the major components of physical security include authentication, authorization, and audit controls.

Authentication

The SANS (SysAdmin, Audit, Network, Security) Institute defines authentication as “....the process of confirming the correctness of the claimed identity.”¹

Basically, authentication is the process where an entity proves who or what it says it is. In many cases it is technically accurate to separate identification and authentication into two separate processes. However, for the purpose of this paper, we will count both identification and authentication as a single layer.

There are actually two types of identities that come into play in the security arena.

1. An entity's actual identity defines who or what the entity really is
2. An entity's electronic identity is the identity of the entity that actually produces the data.

A person may have more than one electronic identity. For instance, an individual has a work identity (usually defined as name@company.com), a home or non-working identity (name@mylocalisp.com), and several different identities on different messaging platforms such as AOL, ICQ etc. People try to avoid mixing up identities by not sending work-related email from my personal accounts and not sending personal email from work accounts. Digitally signing these emails in effect binds a digital

¹ SANS Institute. “SANS Glossary of Terms Used in Security and Intrusion Detection.” May 2003.

identity to the data it produces, logging into an email server, with a password, One Time Password (OTP) or smartcard is binding a real identity to an electronic identity.

Various authentication methods are available. These are by broad definition.

1. Something you have (possession factor). Examples include credit cards, proximity badges, USB smart cards, etc.
2. Something you know (a knowledge factor). Examples include passwords, PINs, social security numbers, etc.
3. Something you are (a biometric factor). Examples include fingerprints, retinal patterns, voice patterns, etc.

Possession-based authentication is clearly subject to theft or use by an unauthorized individual if what you possess is lost or stolen. In almost all practical cases, a secondary factor is combined with this such as a signature.

In their book Secure Electronic Commerce, Ford and Baum define the major threats to password or knowledge based systems as:

- a) External Disclosure²
- b) Guessing³
- c) Communications Eavesdropping⁴
- d) Replay⁵
- e) Host compromise⁶

In other words, passwords can be shared, guessed, sniffed from the wire, captured, and re-used or stolen from a compromised end user machine.

According to Defending Your Digital Assets by Nichols, Ryan & Ryan; "Biometric products are often said to have the highest levels of security."⁷ However, biometric authentication is still somewhat in its infancy and its usability, acceptability, and practicality are still questionable. Nichols, Ryan & Ryan further comment that biometrics "have enjoyed serious use by law enforcement and DoD agencies."⁸ In these applications the relatively high acquisition costs for this technology may be less important than in commercial applications where the cost is often viewed as too high when balanced against the risk.

Limitations in each of these methods have encouraged the industry to combine factors to provide two-factor authentication. Two-factor authentication is generally accepted as stronger authentication because it is more robust than any single factor. Combining a knowledge factor with a possession factor is a common solution in the marketplace today. We see this in everyday use at ATM machines. The ATM card is the possession factor; its associated PIN is the knowledge factor.

Public key technology is often seen as the *new breed* of authentication. People commonly refer to certificate-based authentication when describing authentication derived from such technology. In

² Ford, Warwick & Baum, Michael S. Secure Electronic Commerce. Upper Saddle River: Prentice Hall, Inc, 1997, page 127.

³ Ford & Baum, page 128.

⁴ Ford & Baum, page 129.

⁵ Ford & Baum, page 129.

⁶ Ford & Baum, page 129.

⁷ Nichols, Randall K, Ryan, Daniel J & Ryan Julie J.C.H. Defending Your Digital Assets. New York: McGraw-Hill 2000. Page 361.

⁸ Nichols, Ryan, & Ryan page 358.

reality, what they really refer to is the user being able to carry out a cryptographic function with a private key component that may be verified by a corresponding public key (SSL authentication is an example). The private key in this case is the user's possession factor and this is often combined with a knowledge factor in the form of a password that is used to electronically unlock access to that key.

Security professionals should be prepared to question the validity of this authentication model in scenarios where the user's private information is simply stored on a hard drive and protected by a password. Clearly there is a knowledge factor involved, but is there really a possession factor involved? It all depends on whether we are willing to accept that the physical machine can be labeled as a possession factor, and if the credentials on that machine are truly non-exportable or cannot be copied. Storing the user's private keys on a smartcard or other removable media device would once again allow us to claim true two-factor authentication. In this scenario the user truly would have to have possession of a physical factor and knowledge of the password to unlock it.

Choosing the appropriate authentication scheme can be difficult and the funds allocated to implementation should be related to the value of the assets it protects. However, it is important to understand the **resultant** effect of a poor authentication choice on the other layers defined within the Security Model.

Authorization

SearchSecurity.com defines authorization as, "...the process of giving someone permission to do or have something."⁹

The key point to address here, is the reference to the word "someone." We should also understand that authorization may extend to processes, or objects in addition to users so it may be appropriate to slightly change this definition to something more like "the process of giving an entity permission to do something."

To assign permissions to an entity, we obviously have to know who or what that entity is. No matter how robust or fine grained the authorization model may be, it could be logically challenged if there is no real proof that the entity is in fact who it claims to be. Naturally, we can draw the conclusion that an authorization scheme can only be as robust as the underlying authentication scheme that proved the authenticity of the entity subject or object in the authorization scheme.

RFC 2989, Network Access AAA Evaluation Criteria defines authorization as, "The act of determining if a particular right, such as access to some resource, can be granted to the presenter of a particular credential."¹⁰

Clearly there needs to be some assurance that the presenter has the associated rights to obtain that credential. Looking back at our explanation of identity and authentication, if we seek to authorize access to a resource based on a user's identity (his credential), we need to ensure that that user is properly authenticated to the credential. It could be argued that the presenter of the credential should authenticate the resource he is accessing to complete the chain of trust for the transaction. This method is usually referred to as mutual or bi-lateral authentication.

Imagine the impact of legitimately granting "Joe" access to data he may not be cleared for simply because he claims to be "Paul," or the impact of "Joe" posting sensitive data to the wrong database by mistake.

⁹ SearchSecurity.com. "Definitions, powered by whatis.com – Authorization". 21 July 2001.
URL: http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci211622,00.html

¹⁰ RFC 2989. "Network Access AAA Evaluation Criteria". Nov 2000. URL: <http://www.ietf.org/rfc/rfc2989.txt>

Encryption

RSA Laboratories defines encryption as, "...the transformation of data into a form that is as close to impossible as possible to read without the appropriate knowledge ...Its purpose is to ensure privacy by keeping information hidden from anyone for whom it is not intended, even those who have access to the encrypted data."¹¹

If we break down encryption in the context of this definition we can conclude that we want to keep data private from everyone except the intended recipient.

How do we achieve this privacy?

It seems that two essential components in keeping this data secret are authorization and authentication. Since the definition above once again references an entity by using the word "anyone," we can conclude that before we allow that entity to view or decrypt data we must be able to ensure that they are who they indicate they are. We must also check that they are authorized to view that data.

Encryption is almost always accomplished by choosing and using some form of "secret key." The essential component in choosing or generating this key is the assurance that the only other entity possessing this secret key is the intended recipient of the encrypted data. Since a modern cryptographic algorithm has many checks and balances built in, we make the assumption that if the key is kept private and the algorithm is secure, we have this assurance. Let's consider how that secret key is generated or distributed.

If we assume some sort of out of band delivery mechanism where we physically give a copy of the key to the recipient before initiating communications, we still have an authentication check. In a face to face meeting we would naturally make sure we recognize the person (if we know them), or check some kind of identification to ensure the person is the intended recipient. In short, we authenticate that person prior to distributing the key.

In the electronic world, we typically try to distribute keys in-band. It is impractical to manually distribute secret encryption keys to everyone with whom we intend to communicate. Authentication in this digital world is more important than in the physical as the likelihood that the secret key could be intercepted is significantly higher.

Once again we can tie this back to the practical SSL example using "certificate based authentication." Without a robust authentication scheme in place, it could be argued that encryption may only allow us to have a private conversation with a stranger.

Integrity

The American National Standard T1.523-2001 defines data integrity as, "[The] condition existing when data is unchanged from its source and has not been accidentally or maliciously modified, altered, or destroyed."¹²

¹¹ RSA Laboratories. "RSA Laboratories' Frequently Asked Questions About Today's Cryptography, Version 4.1" 2000. URL: <http://www.rsasecurity.com/rsalabs/faq/1-2.html>

¹² American National Standard T1.523-2001. "Telecom Glossary 2000." 28 Feb 2001. URL: http://www.atis.org/tg2k/_data_integrity.html

Although the definition above does not directly reference an entity, integrity has a direct tie with authentication. Typically integrity is seen as a component of encryption which we have previously explained as having a strong dependency on authentication.

We assume that if data has maintained its integrity, it has not been altered, modified, or destroyed accidentally or maliciously. The threats to data integrity clearly link to unauthorized entities having the ability to conduct operations on that data. We protect integrity of data through careful authorization and encryption where appropriate. Both these measures have a strong dependency on authentication as previously discussed within this document.

Audit

Sandi Smith, CPA, wrote a paper entitled "Leaving a Digital Audit Trail" in a technology magazine published by the American Institute of Certified Public Accountants and defined an audit trail as, "...a form of electronic evidence that can be used to trace transactions to verify their validity and accuracy."¹³

There is a lot of good advice that can be gleaned from the financial community and applied to information security. Accountants have been involved in electronic audits for many years and have defined and documented what constitutes evidence of transactions. Perhaps this is best illustrated by the phrase, "Without information security controls, an electronic transaction is worth the paper it is not written on." In other words, it's worthless.

Breaking down the definition above leads us to some interesting conclusions. Verifying the validity of a transaction closely maps to ensuring that it was created and executed by an authorized individual. Clearly in the digital world, if we wish to tie an event to an individual, it is important that we properly tie the individual to their digital identity. Authentication assumes this responsibility.

As laws are being created to enforce issues such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA), audit trails are becoming more and more important. In fact, audit trails will become significant pieces of evidence in enforcing these acts. To make these audited trails admissible and credible in a court of law, we must be able to prove that events can be strongly tied back to the entity causing an event. As an example, in the healthcare arena HIPAA mandates that access to Private Health Information is properly audited. We need to understand who accesses patient records along with creating a timestamp of when this was done. If this audit trail can only be followed back to a weak password or PIN, it is difficult to prove that the access was from an authorized user and not from someone who simply had knowledge of the user's password. A strong authentication scheme is a pre-cursor to proving who accessed the confidential information.

Summarizing the definitions

Summarizing the definitions and analyzing them proves that each layer of the security model is dependant on the "who" factor. Clearly we can claim that unless we have positively and reliably authenticated the source of the end entity then the upper levels of the security pyramid become fundamentally flawed. The figure below illustrates that without a strong authentication foundation, the security pyramid is compromised.

¹³ Smith, Sandi, CPA. "Leaving a Digital Audit Trail" 2001. URL: <http://www.toptentechs.com/issues/Issue9/>



The security pyramid is all built on "who."

Summary

Organizations must carefully consider authentication schemes and evaluate whether their chosen methods provide a firm base on which they can build the additional requirements for their security controls. Just as a house built on a weak foundation will crumble, an authorization, encryption, integrity, or audit scheme built on a weak foundation may also crumble when it comes down to a forensic evaluation after an incident has occurred.

Risk analysis studies should not only consider the impact of an unauthenticated user accessing the data, but also the impact of not being able to enforce the "upper layer" security controls required to complete the suite of services required for security.

We should constantly look downward in the model depicted above as well as our own organizations and we should challenge vendors on how their given products for encryption, authorization, etc. rely on and embrace strong authentication models.

Wise men build houses on rock, not sand.

About the Author

Doug Graham has been involved with information and physical security for over a decade. He has worked for companies in Europe and the United States and is currently responsible for the managed services division at Blue Ridge Networks. Prior to his appointment at Blue Ridge Networks, Doug was a Senior Systems Engineer at RSA Security and Director of Systems Engineering at Ubizen. Doug has also gathered some experience in the physical security sector as Director of Sales Engineering at Object Video. Doug studied electronics and avionics at the No. 1 Radio School of the Royal Air Force in the United Kingdom and is a Certified Information Systems Security Professional (CISSP).

Blue Ridge Networks, Inc.
14120 Parke Long Court
Suite 103
Chantilly, Virginia 20151

(P) 703/631.0700
(F) 703/631.9588

www.blueridgenetworks.com