It’s All About Authentication

Doug Graham

March 15 2003

GSEC Option 1, Version 1.4b

Table of Contents

Abstract

Information security professionals, seeking to reduce vulnerabilities in their organizations, are presented with an ever-increasing variety of options that range over several subsets of the information security landscape. Given the rapidly decreasing financial resources available for IT infrastructure and a mandate from management to maximize a return on investment for security technologies, in what specific area of the information security landscape should an investment be made?

This paper categorizes and then simplifies some of the core fundamentals of electronic security controls and mechanisms and concludes that authentication is the single most important aspect in information security. It also 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

We will begin by categorizing security into five different layers as seen below in Figure 1.

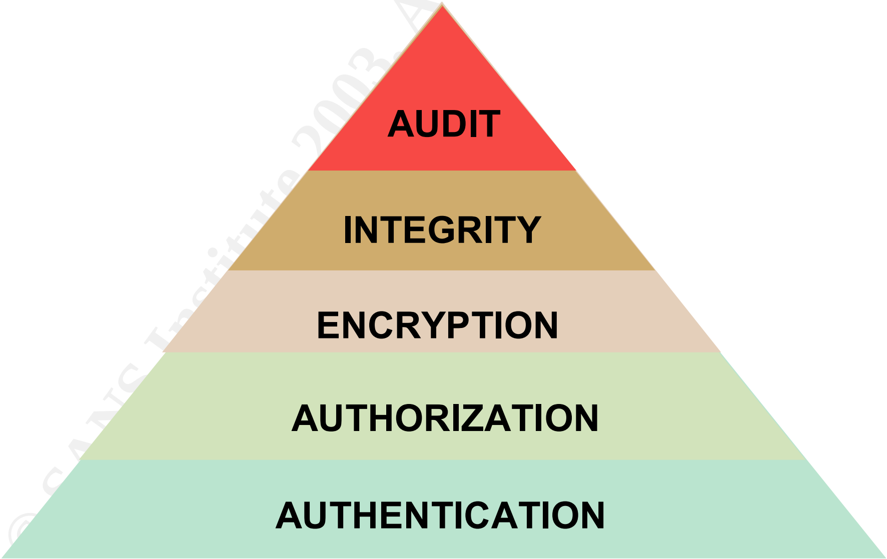


Figure 1: Security Pyramid

It may be argued that physical security is a component missing from this model; this paper focuses on electronic security controls and countermeasures. An in-depth discussion of physical security is outside the scope of this paper, and thus, will not be included. The author assumes recognition on the part of the reader of the two following fundamental axioms. A robust physical security model is essential to build a strong foundation for electronic security and some of the major components of physical security include authentication, authorization and audit controls.

Authentication

The SANS institute defines authentication as "….the process of confirming the correctness of the claimed identity." [1]

At its most basic level, authentication is the process where an entity provides proof that it is who it is claiming to be. 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.

The definition of identity must be established prior to discussing the authentication of an identity. It should be noted that there are actually two types of identities relating to security as we are addressing it here.

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

In other words, a real person may have more than one electronic identity. For example, I have my working identity (usually defined as name@company.com), my home or non-working identity (name@mylocalisp.com), and several different identities on different messaging platforms such as AOL, ICQ etc. It is vital to keep those identities separate at all times by only sending work related email from my work account and personal email from my personal account. Digitally signing these emails in effect binds my digital identity to the data it produces. Logging in to my email server, with a password, SecurID or smartcard is binding my real identity to my electronic identity.

Three primary authentication methods are available to the security professional. By broad definition, these are:

1. Something you have (possession factor). Examples include credit cards, proximity badges, 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 lost or stolen. In almost all practical cases a secondary factor is combined with this such as a signature.

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

a) External disclosure [2]
b) Guessing [3]
c) Communications eavesdropping [4]
d) Replay [5]
e) Host compromise [6]

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* authored 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 use-ability, acceptability and practicality are still being put to the test. Nichols, Ryan & Ryan also state 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 of a decision making factor than in the private sector where the expenditure of each dollar is becoming more frequently scrutinized.

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 "strong authentication" because two factors are more robust than any single factor. Combining a knowledge factor with a possession factor is the most common solution in the marketplace today. We see this in every day use at ATM machines (the combination of an ATM card as the possession factor and its associated PIN as a knowledge factor).

In many applications, public key technology is often seen as the "new breed" of authentication. Certificate-based authentication is often referred to but in reality the authentication is derived from the user having the ability 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 of this). 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 key is simply stored on the hard drive of their machine and protected by a password. Clearly there is a knowledge factor involved, but is there really a possession factor involved? It all depends 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 passphrase to unlock it.

Choosing the appropriate authentication scheme can be difficult, and the funds allocated for implementation should be related to the value of the assets it protects, however it is important to understand the “knock on” 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]

They key point to address here, is the reference to the word “someone” in the definition above. 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, or “someone”, 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. Furthermore it could be argued that the presenter of the credential should authenticate the resource he is in fact accessing to complete the chain of trust for the transaction. This 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.

Encryption

RSA Laboratories define 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 the definition given above we can very easily conclude that we want to keep data private from everyone except the intended recipient.

How do we achieve this?

It seems that two essential components in keeping this data secret are authorization and authentication. Since the definition above once again references an entity (with the word anyone) we can conclude that before we allow that entity to view or decrypt the information we must be able to ensure that they are who they claim to be. We must also confirm that they are authorized to view that data.

In almost every case, encryption is achieved by choosing and using some form of "secret key". The essential component is 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, then we have this assurance. But 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 intended 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 they were known to us) 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 of course impractical to manually distribute secret encryption keys to everyone we intend to securely communicate with. Authentication in this world is even more important 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 T1.523-2001defines 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]

Although the definition above does not directly reference an entity, integrity has a direct link to authentication. Typically, integrity is seen as a component of encryption. Encryption, to be useful, requires a strong dependency on authentication.

We assume that if the data has maintained its integrity, it has not been altered, modified or destroyed accidentally or maliciously. The threats to data integrity can be clearly linked 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.

Audit

A Certified Public Accountant named Sandi Smith authored a paper entitled "Leaving a Digital Audit Trail" in a technology magazine published by the American Institute of Certified Public Accountants. It defined an audit trail as:

"………a form of electronic evidence that can be used to trace transactions to verify their validity and accuracy" [13]

The information security profession can take a lot of good advice from the financial community, especially those well versed in electronic audits. Accountants have been conducting audits for many years, and have well defined and documented requirements for evidence of transactions. Perhaps this is best illustrated by the phrase;

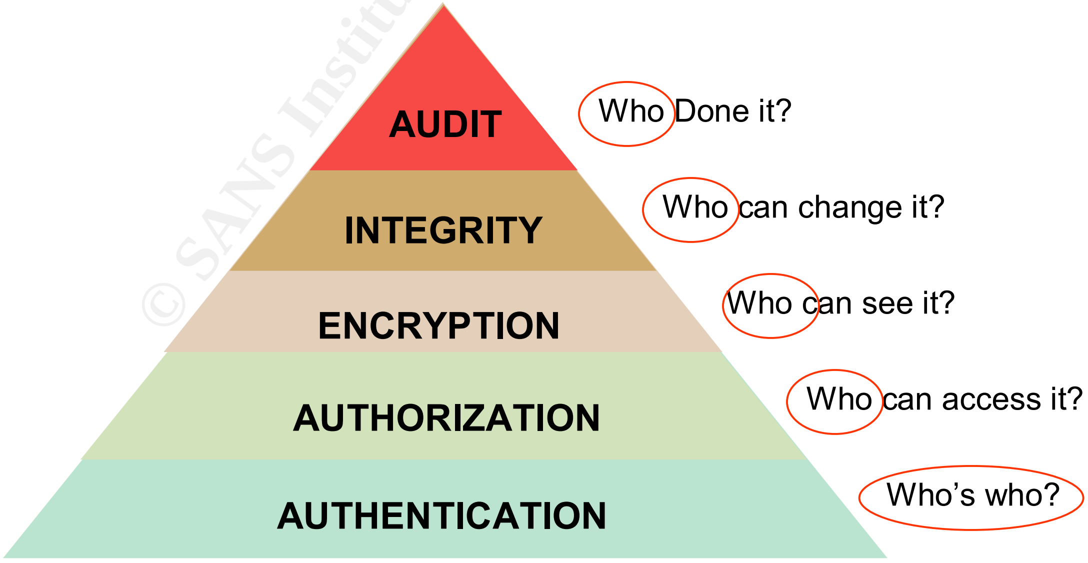
Without information security controls, an electronic transaction is worth the paper it is not written on. (In other words, it's worthless)

Analyzing the above definition 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. This is the fundamental task of authentication.

As laws are being created to address issues such as patient privacy (HIPAA act) or privacy within banking (Gramm Leach Bliley), audit trails are becoming more and more important. In fact, audit trails will become significant pieces of evidence in the enforcement of these new regulations. To make these audited trails admissible and credible in a court of law we must be able to prove that the events logged can be strongly tied back to the entity causing the event to produce the log. As an example, if we attempted to determine who accessed a medical patient's record on a given date, and could only tie an audit event back to a shared secret such as a password or PIN. Could we really say that a certain individual must have accessed if the authorization to do so was only determined after authentication by a weak, easily compromised password scheme?

Summarizing the definitions

Summarizing the definitions and breaking them down to simplicity proves that each layer of the security model is dependant on the factor of "who". Clearly we could claim that unless we have positively and reliably authenticated the source of the end entity, then the "upper levels" of the security model become fundamentally flawed. The figure below illustrates this.



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 be looking downwards in the model depicted above and challenging vendors how their given products for encryption, authorization etc. rely on and embrace strong authentication models.

Would a wise man build a house on a rock, or on sand?

Notes:

[1] SANS Institute
[2] Ford & Baum, p.127
[3] Ford & Baum, p.128
[4] Ford & Baum, p.129
[5] Ford & Baum, p.129
[6] Ford & Baum, p.129
[7] Nichols, Ryan & Ryan, p.361
[8] Nichols, Ryan & Ryan, p.358
[9] SearchSecurity.com – Authorization
[10] RFC 2989, p.2 section 1.2
[11] RSA Laboratories section 1.2
[12] American National Standard T1.523-2001
[13] Smith

References:

SANS Institute. "SANS Glossary of Terms Used in Security and Intrusion Detection". May 2003. URL: http://www.sans.org/resources/glossary.php

Ford, Warwick & Baum, Michael S. Secure Electronic Commerce. Upper Saddle River: Prentice Hall, Inc, 1997, 127 – 128.

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

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

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

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

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

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