VSC IT Definition of Secure
Approved by Security Policy Steering Committee: 9/5/06
Revised:
Reviewed: 9/5/2013

I. Definition

Information is said to be secure if is protected against disclosure to unauthorized individuals, cannot be altered by unauthorized individuals and is available when required.

Supporting Discussion

I. Introduction

In this document we provide a definition of the term "secure" as it is to be used in other VSC policy documents. We elaborate on this general statement by also providing an operational definition of "secure." The operational definition can be used to objectively verify when information is being stored or being transmitted in a secure manner.

II. Purpose

The purpose of this document is to define the term "secure" as it is used in the context of VSC security policy documents. This definition is intended to be sufficiently precise so that statements such as "the data shall be stored securely" have a clearly defined meaning, and so that the truth of such statements can be objectively verified.

It is not the intent of this document to set security policy or to impose any specific requirements on how information must be handled, transmitted, or stored. Such requirements are specified by other security policy documents. It is not even the intent of this document to describe a security standard toward which other security policies must strive. In many cases handling data securely, in the sense we define it here, is too expensive or too inconvenient to be feasible. However, security policy documents must enumerate the exceptions in those cases using language such as, for example, "the data shall be stored securely EXCEPT THAT back up copies may be discarded without first being wiped." In this way the authors of policy documents are forced to make explicit any potential weaknesses in the policy that were introduced for the sake of practicality.

III. Scope

Our definition is concerned only with the security of information. Our definition is not intended to apply to the security of physical objects, except indirectly where such physical objects are used to store or transmit information, nor is this definition intended to apply to the personal security of individuals.

There are three aspects of information security that our definition is intended to cover:

Confidentiality: Information that is secure should not be readable by unauthorized individuals.

Integrity: Information that is secure should not be modifiable by unauthorized individuals.

Availability: Information that is secure should be available to authorized individuals when it is needed.

IV. Operational Definition of "Secure"

To make the definition specified in the beginning of this document more precise, and to provide a way to objectively verify when information is being handled in a secure manner, we offer the following operational definition of "secure." Our operational definition is expressed in terms of attack models. *Information is said to be "secure" if it is protected from unauthorized reading or writing by attackers with specific capabilities, as detailed below.* We define two different attack models: one for attacks against information as it is being transmitted and another for attacks against information as it is stored.

Attacks Against Data Transmission Media

We adopt the standard Dolev-Yao (D-Y) attack model from the security literature. Such an attacker has the following capabilities. In all cases, the D-Y attacker is not an authorized user.

- Able to observe all data flowing across any media.
- Able to modify any data as it flows across any media.
- Able to record and then later replay any transmission on any media without necessarily being able to understand the transmission.
- Able to indefinitely block or delay any transmission on any media.
- Able to participate in any communication protocol as a legitimate user.

However, the D-Y attacker is not able to do the following:

- Not able to defeat any cryptographic technology.
- Not able to view or modify the data stored in any data storage device.
- Not able to observe or influence any computations done on the data before it enters the transmission media or after it leaves the transmission media.
- Not able to indefinitely block or delay any transmission on any media without detection.

Generally speaking, defeating the D-Y attacker requires using encrypted, authenticated data transmission protocols that resist replay attacks. Network protocols such as SSL/TLS

defeat the D-Y attacker on a single network connection (although not necessarily on multiple related connections).

We extend this attack model to include various non-traditional and non-electronic media. For example we assume a D-Y attacker can listen to all phone conversations *while simultaneously* monitoring network traffic. We assume a D-Y attacker can read all information stored in sealed envelopes and sent through the US postal system[1]. We assume a D-Y attacker can overhear all verbal communications.

Attacks Against Data Storage Devices

Information that is not physically secure is at risk. Information stored in locked containers that can be easily carried is not secure regardless of the quality of the locks being used. To be considered secure a data storage device must either be monitored by an authorized person or in a physically locked space that can't be carried away, or the data must be encrypted according to best practices.

We now define the capabilities of a "data storage" (D-S) attacker.

- Able to take advantage of any known security vulnerability.
- Able to read and remember all publicly exposed information.
- Able to defeat weak passwords[2].
- Able to find all physically hidden information.
- Able to work infinitely fast.
- Knows all VSC procedures and work flows. Knows every detail of the operation of every software package. Knows the configuration details of all VSC computer systems.
- Can read data in any format.

However, the D-S attacker is not able to do the following.

- Defeat any encryption or authentication technology without knowing appropriate passwords, etc.
- Take any action while being watched.
- Trick any user into revealing sensitive or security related information or trick any user into violating established security policies and protocols[3].

---

[1] A sealed envelope does not provide the equivalent confidentiality protection that encryption does because, unlike a high quality encryption algorithm, the seal is easily "broken."

[2] The precise definition of "weak password" is left to another policy document.

[3] Here we assume that the user community is educated in how to avoid being tricked in this way.

- Find previously undocumented and unknown vulnerabilities in existing computer systems.
- Defeat any physical locks.

For example, a D-S attacker can enter any unlocked office and immediately read and later remember all documents left out on the desk. The attacker would also immediately know any hidden information in the room, such as passwords stuck under a keyboard or stored in unlocked desk drawers or filing cabinets. The attacker could sit down at the office computer and, perhaps using the hidden information obtained earlier, immediately operate all software on the machine with the skill level of an expert. The attacker could do all of these things instantaneously, even if the authorized user of the office stepped out for only a few moments.