A NEWLY CLARIFIED FOURTH STATE OF DATA

By Prem Sobel, CTO MerlinCryption LLC

Current discussions regarding encryption typically define three states of data: **Data-at-Rest**, **Data-in-Motion**, or **Data-in-Use**. However, to more accurately describe encryption solutions, a new definition is required: **Data-in-Change** [Ref-1]**.**

The current literature is muddled and definitions are nebulous regarding **Data-in-Use**. This broad-brush deficiency not only makes it difficult for security providers to effectively identify conditions for protection, but more critically, confuses the actual margin of risk for the user. It is important to explicate the existing data state, **Data-in-Use**, and distinguish it from a new "state of data" introduced in this paper, **Data-in-Change**.

First, this paper reviews the definition of data. Next, it will introduce two new ways to look at the behavior of data: data on a **Static Axis** and data on a **Dynamic Axis.** And finally, it will introduce a clarified distinction of **Data-in-Use** and the newly defined state of data, **Data-in-Change**.

Data Definition: Back to Basics

Data is **information** containing a linear (one dimensional) sequence of:

- *bits* (base 2),
- *numbers* (in any base), or
- *symbols* (from any alphabet).

There can be multiple interpretations for the same information. The exact same linear sequence of *bits* (base 2) or *numbers* (in any base) or *symbols* (in an alphabet), can simultaneously *mean* more than one thing (to different computer programs or users).

A linear sequence of *information* is called a ***file*** or ***message***. Information is a mathematical concept [Ref-2 and Ref-3]. In a file or message, the *meaning of the data* resides in the interpretation. *The actual structure of the data is typically nonlinear (a tree for example) and is implicit, or implied, by the computer program or user, as a function of the interpretation.*

512-348-SAFE
PO Box 341133 | Austin, TX 78734
www.MerlinCryption.com

Static Axis: Data with Unchanging Content

Data-at-Rest *is data stored on "permanent" storage media, such as a disk, CD, flash, or piece of paper.*

The relationship of the data to the storage media is either simple or complex. A simple relationship of data to its storage media treats the whole storage media as one message or file. The complex relationship of data to its storage media treats the whole storage media as multiple messages or files. With multiple files or messages, the information in those files or messages have a temporal and/or structural relationship imposed by the computing device or the user.

The *permanence* of the data (over time) is still subject to energy "noise" which, if it appears, can unintentionally (by a computer or a user) destroy some or all of the contents of the file or message. Energy "noise" can be electrical, magnetic, thermal, mechanical, or other (like spilling soda on the system unit). The contents are unchanged as long as excessive or cumulative noise energy *is not* in effect. The types of energy required to change the data is determined by the type of media storing the data. The storage media may or may not be associated with, or accessible by, one or more computing machines or users.

The fact that the storage media is physically moving in space relative to other physical objects does not alter the status of the file or message as being in "a state" of **Data-at-Rest**.

Three examples of **Data-at-Rest** are: a file on a laptop (or other information system) carried by a person from one location to another, or transported by a delivery service, or stored on a file-server.

Data-in-Motion *is data with unchanging contents in the form of an intentional communication with a defined data protocol.*

The data is in the form of a file or message, which is traveling between two or more computing devices or users. Conceptually, **Data-in-Motion** is a transient file or message between two or more computing devices or users, which is always saved or discarded when the "use" is completed. Examples of **Data-in-Motion** are: a file or message on a communications channel such as FTP, email, chat message, or telephone (digitized text, voice, or video).

Any permanent storage media (such as a CD or hard drive) that is physically transported (and is not connected to a computer, is turned off, or not being accessed) is **Data-at-Rest**, *not* **Data-in-Motion**. Permanent storage media is accessed through an interface and a communications protocol in the states of **Data-in-Motion**, **Data-in-Use**, or **Data-in-Change**. A *Communications Protocol* is a system of digital message formats and rules for exchanging those messages in or between computing systems and in telecommunications [ref 4].

Encrypt Data with Unchanging Content

Data with unchanging content, **Data-at-Rest** or **Data-in-Motion**, can be directly encrypted. Even if the data is being transported, no user or computing device is accessing it for "use." Neither **Data-at-Rest** nor **Data-in-Motion** are at an **End-Point**, and as a result, the data does not need to be decrypted when in these two states.

End-Point

Data-in-Use *and* ***Data-in-Change*** *at some moment in time, reside at an* ***End-Point****. An* ***End Point*** *is a user or decision-making computing device (HW) and/or program (SW) that accesses only, or changes and saves the data.*

Dynamic Axis: Data with Temporary Duration or Changing Content

Data-in-Use: *Data with Temporary Duration in Time*

The current definition for ***Data-in-Use*** *requires clarification and delineation.* **Data-in-Use** is data that is accessed by a computer or user for temporary use, and is only needed for a finite duration in time. Practical examples of **Data-in-Use** are: opening, viewing, and reading a document or file; viewing a database query result; or viewing search results.

Data-in-Use can always be encrypted up until it reaches its **End-Point** (user or computing device and/or computer program). The **End-Point** makes a decision to change or not to change its "state" based on the content of the data. For example, if the **End-Point** (the user or computing device or program) does not change its state, the data received in the **Data-in-Use** state was already known, inapplicable, or of no consequence.

Data-in-Change
A Newly Clarified 4th State of Data

Data-in-Change: *Data with Changing Content*

It is critical to distinguish between the states of **Data-in-Use** and **Data-in-Change** when securing data. **Data-in-Change** is data that is being created for the first time, altered totally or partially, destroyed, deleted, added to, or modified in any way. **Data-in-Change** resides at an **End-Point**.

The changed data will be saved to a storage medium or communicated by a defined protocol. This may happen multiple times.

This new distinction between **Data-in-Change** and **Data-in-Use** is necessary because improved solutions to Data Loss Prevention (DLP) are needed. Specifically, **Data-in-Change** implies that at some point in time (after a decision by a computer or user is made), storage media needs to be altered to record the *change*. **Data-in-Use** is different: by this revised definition, *storage media is never altered* in the **Data-in-Use** state.

Changing Data Is Vulnerable

We must assume the changing data is vulnerable in its unencrypted state (no matter how short in duration or restricted in its exposure to being copied) at an **End-Point**.

Data-in-Change State Compared to Other States of Data

Data State	Viability	Representation	Changed	End Point
Data-at-Rest	Permanent	State of matter	No	No
Data-in-Motion	Transient	State of energy and/or matter	No	No
Data-in-Use	Transient	State of energy and/or matter	No	Yes
Data-in-Change	Transient	State of energy and/or matter	Yes	Yes

Data States and Risk

Unencrypted data is at risk in each of the four states of data: **Data-at-Rest**, **Data-in-Motion**, the newly clarified **Data-in-Use**, and the newly clarified and defined, **Data-in-Change**.

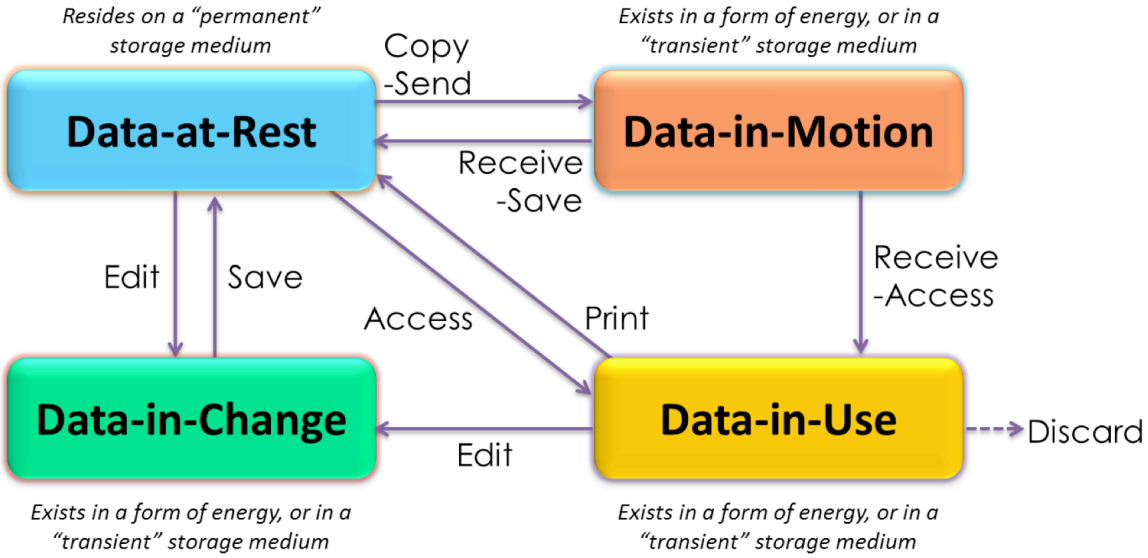
Permanent Storage Medium

A "permanent" storage medium is one which will *not* lose its data if power or energy is unavailable (hard drive, CD, flash, or even paper). When this "permanent" storage is in a virtualized or cloud environment, there are additional risks and encryption should be considered up to the End Point.

Transient Storage Medium

Data in a "transient" storage medium (such as RAM) is in a form (and states of energy and matter) that will be lost if power or energy is unavailable to sustain it.

This applies to both the **Static Axis** and **Dynamic Axis**.



Unencrypted Data Is Vulnerable In All Four States

"Deleting" data is the result of sending a command to a storage medium device. The "deleted" data is still available unless it has been "shredded" (overwritten multiple times before it is deleted).

Data in a transient storage medium is still at risk while power is on. It needs to be "scrubbed" (overwritten) to eliminate the security risk, before the process that owns it, terminates.

Some editing software creates temporary files in an intermediate state, **Data-at-Rest**, which is vulnerable. It is also possible that the data may be exposed on a storage medium acting as a cache for virtual memory in the **Data-in-Use** and **Data-in-Change** states.

MerlinCryption©

Protect Your Privates

A software technology company in Austin TX, MerlinCryption LLC develops invincible data security solutions that combine powerfully robust encryption products with surprising affordability and functional ease.

The encryption distinctly differentiates from standard encryption in key structure. A discrete key approach eliminates PKI expense and introduces scalable key size from 2000 bits to 2 gigabytes in length. MerlinCryption is the first to develop the stealthy CryptoFile™ encryption process. An advanced, yet simple embedded Key-in-a-File technique, leverages invulnerability with a user-designated key and variable key length MerlinCryption's original Password-in-a-File solution introduces scalable passwords, up to 65,535 bytes in length, releasing the strongest encryption available for consumer, enterprise, and OEM use. Underpinned by a proprietary algorithm, the encryption is not based on mathematical technique and not subject to statistical analysis. These significant breakthroughs establish a new paradigm for the data security industry.

Leading edge MerlinCryption technology secures data-at-rest and data-in-motion, and pioneers innovative products to protect data-in-use and data-in-change. The unprecedented encryption protects file, email, instant messaging, password, and broadcast data as it is created, viewed, edited, shared, stored and moved around the Internet and around the world. Experience how MerlinCryption architecture is changing the way the world protects data.

REFERENCES

[Ref-1]
http://groups.google.com/group/jstree/browse_thread/thread/2c7132b6400736c0
http://help.sap.com/saphelp_nw70/helpdata/EN/44/588168ce8c08fae10000000a422035/content.htm
http://www.trendsparency.net/tag/healthcare-reform/
http://www.ittestpapers.com/sap-bw-interview-questions---part-a.html?page=8

[Ref-2]
Shannon, C.E.;
"A Mathematical Theory of Communication";
Bell System Technical Journal, 27, pp. 379–423 & 623–656, July & October, 1948

[Ref-3]
Claude E. Shannon, Warren Weaver;
"The Mathematical Theory of Communication.";
University of Illinois Press, 1949. ISBN 0-252-72548-4

[Ref-4]
"Communications Protocol.";
http://en.wikipedia.org/wiki/Communications_protocol

ABOUT PREM SOBEL

Published by Prem Sobel, Chief Technology Officer, MerlinCryption LLC. Graduating with honors with a B.S.E.E. Electrical Engineering from Pratt Institute, and M.S.E.E. Electrical Engineering from California Institute of Technology, Mr. Sobel holds four patents in CPU Architecture.

Prem.Sobel@merlincryption.com

P.O. Box 341133 | Austin, Texas 78734
www.MerlinCryption.com
512-348-SAFE