Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Managing Secure Data Delivery: A Data Roundhouse Model

Managing data securely in today's corporate enterprise is no mean feat. What once entailed simple permissions controlling access to information locked within glasshouses or stored within data warehouses now means also controlling transport as it replicates around the worldwide web or bounces back and forth between business-to-business end-points. Data, once stationary, is now energized, always in route to its next destination. Managing this data securely with the same expectations once placed on its static predecessor ...

Copyright SANS Institute
Author Retains Full Rights

AD
Investigate Insider Threats
Protect your company against corporate IP Theft
Learn More
SpectorSoft

Managing Secure Data Delivery: A Data Roundhouse Model

By Jim Farmer
GSEC Version 1.2f (amended August 31, 2001)

Managing data securely in today's corporate enterprise is no mean feat. What once entailed simple permissions controlling access to information locked within glasshouses or stored within data warehouses now means also controlling transport as it replicates around the worldwide web or bounces back and forth between business-to-business end-points. Data, once stationary, is now energized, always in route to its next destination. Managing this data securely with the same expectations once placed on its static predecessor is presenting a new challenge to the security professional that needs to be addressed quickly.

Revving up the dynamics of data delivery is a host of inventive technologies that have exploded into the marketplace. The primary focus of these inventions is on speed, and their mantra is efficiency. If not completely forgotten in the excitement, basic security requirements are typically applied only as an afterthought, as band-aids on an unexpected bump in the process. Offering encryption as an add-on module is a good example of band-aid security. Adequate security administration and management are even less likely to be included in the newly developed product lines. The expectation is that good security and easy management will be in the next release.

Waiting for delivery technologies to mature is not acceptable when good security is needed today. Risk factors are increasing faster than the technologies, especially in the open Internet model. And unforeseen risks within the global management of data delivery are being over looked due to new complexities. Exacerbating the situation even more, old cracks in the existing delivery structures are widening from increased pressures to "make things happen."

Today the only available design solutions that address security concerns are those drawn out by policy. However, these are safeguards on paper only. Too quickly, either the day-to-day operators forget that these paper limitations are in place, or else, exuberant engineers who've been given a new delivery mechanism become overly resourceful and go beyond the bounds comfortable for security. These are reasons for urgency. And there are others. For example, even the existing, older channels of delivery add to the risk. These entrenched technologies remain available and in operation long past their expected use; they are dinosaurs always waiting for the last service to be upgraded or removed to a new platform. As another example, very often in today's information technology environment security risks increase because sensitive data can be delivered piggyback through delivery mechanisms designed for less secure traffic--if a pathway is open to a destination, it will undoubtedly be used to deliver information unplanned for and with a higher risk to the corporation that that which was intended.

To address the compounding security issues, a centralized method founded on good security policy is needed to manage the numerous security factors in data delivery. In fact, bringing the policy management of all the data delivery functions together may lead eventually to a better long-term solution. Bringing the management under one roof equates to building a data "roundhouse". The analogy of a traditional roundhouse, where railroad engineers manage and

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

redirect the delivery of millions of tons of payload, reinforces the most important goal in the data delivery process: manage data securely from the start and secure it throughout its delivery all the way to its destination.

In the case presented here, and for any sound security implementation, policy is still the foundation that must define the process. Writing the goal of secure data delivery as a security policy is simple:

- *Establish and ensure the appropriate level of security for data throughout its delivery*

Defining the levels of security for data delivery is based on the standard security blocks: identification/authentication, authorization, data integrity, privacy or confidentiality and non-repudiation. These are defined in detail in any security primer and should be accepted as a business standard, especially since technologies must adhere to their attributes. Other levels of security can be less definitive if they make sense within a corporation.

Applying the actual appropriate level of security to data delivery is more difficult, but with the help of data owners and risk models the definitive levels for protecting data are not impossible to set. Appropriate levels of security may vary between companies. There are also laws and contracts that can set the expected level of security. These should not be forgotten. Whether this means there are agreements between corporations or regulations defined by government, the importance for managing to these definitions is the same as if set by company policy.

Once necessary levels of security can be established, the follow-up task remaining is to ensure that security really is in place. For this, the roundhouse concept becomes useful. Using centralized reviews of the basic elements involved with respect to secure data delivery will give the best assurance to everyone concerned that policy is being met.

In the roundhouse model, the data delivery process has three basic elements:

1. Payload
2. Destination
3. Transport

Keeping up with these three elements separately and distinctly simplifies the overall management process so that any identified level of security can be evaluated with some confidence.

“Payload” refers to the information being delivered. Using “Payload” to describe the data flowing through the network breaks away from some current concepts about data. How to handle a payload does not mean the same as how to handle the data in a database. Static data can already meet the privacy, integrity or non-repudiation needs, so the answer to the question how to handle the payload can result in a different solution.

By definition, the second element “Destination” asks, where is the payload headed at anytime during transit. This means that destination has a flexible character taking any number of different

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

forms--an endpoint, hub, staging point, or a next hop down the line. It can even be defined as another site or as an arena of differing responsibilities. Destination can also refer to a legal entity, as for example, a business partner. But regardless of form, each of these destinations can be identified, rated, inventoried, and evaluated in terms of security. And since one destination can become nested within another, it is also important to not forget the enclosed destination's attributes as well. Generally speaking, the purpose for including destination in this model is to reinforce the importance for security to be evaluated all the way to the end of the track.

The last element, referred to in this model as "Transport," is the most likely to have a technical definition, but it is often the hardest to confirm. Transport here refers to the data delivery protocols and other mechanisms. It is the engine behind the delivery process. Transport is easily quantified in security terms. Adequate privacy, integrity and non-repudiation can normally be proved mathematically. But its appropriate use in the security realm may not be clear-cut. Default configurations, changes in upgrades, a myriad number of patches, and a host of options, all make transport difficult to police. Only good review processes can meet the demand here.

Taken together, payload, destination, and transport form a single functioning process for data delivery. Analyzing them at first separately and than as a whole is the purpose behind applying the model.

Each of these three features or elements in the model has various factors to consider and each of them must be analyzed with respect to the security policy's mandate to establish an appropriate level of security. In general, there are only two processes that actually need to addressed for each element in the model:

1. Establish a standard with respect to security requirements
2. Inventory the exceptions to standards

The development of standards and the determination of their exceptions work hand-in-hand toward establishing a basic understanding of the security picture for any transport environment. Constructing these standards and exceptions inventories for each element--Payload, Transport, and Destination--is the first step in the security process behind sound data deliver.

Payload

Establishing the appropriate level of security for any data delivery payload means answering the question, how must the data be handled? A first step to help answer this is creating a requirements document that explains security levels for payloads. An overly simplified example of "Payload Requirements" and their respective security levels is:

Payload Requirements

Security Level	Types of Payload
Non-repudiation*	Transaction data
Privacy*	Secret Classification, Medical History, and Credit History data
Integrity	Production and System data
None	Public data

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

*Includes Id/Authentication and Authorization

An inventory of other payloads establishes the security requirement for specific payloads that are exceptions to the established standards. These can be found by checking existing batch files, MQ Series scripts, NDM records, etc.

Individual Payload Inventory [Exceptions to the Requirement Doc]

Payload	Acceptable Security Level	Established by
Personnel Files	Privacy	HR Requirement
Contracts	Privacy	NDA w/ Co.
System Monitoring	Data Integrity	Engineering

Destination

Building a table of security requirements for destinations is much the same as one for payload. However, some physical controls must be addressed as well. This helps answer questions like, how can the data be maintained? And, how do you know the right payload is handled correctly? An example of some destination requirements is:

Destination Requirements

Security Level	Type of Destination	Mechanisms to have in place
Non-repudiation*	Corporate Partner	Key Management
Privacy*	Production Host	Access Controls or Encryption
Integrity	Production Application	Server Access Controls
Authorization	Production Staging Server	Access Controls
Integrity	Production Host	File checks or Hashing
Authorization	Data Base	Permissions
Id/Authentication	Workstation	NT Authentication
Test Host	User Test Site	Open Code
Lab Server	Lab Only	Open System & Code
None	Public Web Server	Read Access Only

*Includes Id/Authentication and Authorization

The next step is to complete an inventory of any other destinations both within the enterprise and without that cannot be categorized.

Individual Destination Inventory [or Exceptions to the Requirements]

Specific Destination	Acceptable Security Level	Established by
Company ABC	Privacy	Legal Documents
Company DEF	None	Physical Site Review

Transport

Getting a handle on the transport element is the final phase for establishing the baseline information in the roundhouse mode. This table of requirements addresses how the data is delivered. It also includes information showing how the right payload is picked up, how the right destination is in place, and how the delivery cannot be done any other way.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Transport Requirements

Security Level	Type of Transport	Mechanisms to have in place
Non-repudiation*	Frame Relay w Encryption	Contracts, Service Agreements...
Privacy*	SSH	Key Management, Directory Access
Privacy*	HTTPS	Web Resource Allocation
Integrity	all the above	
Integrity	Frame Relay wPVC	Contracts, Service Agreements...
Authorization	FTP	User Enrollment & Authorization
Id/Authentication	NFS	System Controls
None	all the above	

The most important task of all, and probably the most tedious, is the next step: complete an inventory of the specific delivery mechanisms on each platform.

Individual Transport Inventory

Installed Transport	Expected Security Levels	Established by
Host1 FTP	Authorization	Users
Host1 Connect Direct	Non-Repudiation	Operators
Server1 SSH	Privacy	Security Office
Server1 MQSeries	Non-Repudiation	Administrators
ATT Frame Relay	Non-Repudiation	External Engineers

This extensive list becomes necessary before completing the roundhouse model for data management. Having a good inventory of the all the transport choices is mandatory before security can be ensured in the final phase.

Ensuring the Appropriate Levels

Once the requirements and inventories are completed the next step is to ensure that the security levels across the board are consistent for each payload. That is, is the payload's security requirement being met by its respective destination and transport? A simple matrix drawn from the above requirements tables and exceptions lists should resolve the issue:

The Roundhouse Model

Payload/Security Level	Destination / SecLevel	Transport/SecLevel	Verify
Credit Records/Privacy	Prod App / Priv	SSH / Priv	Yes
System Data/Integrity	Prod Hosts/Integrity	FTP/Auth	No

As to be expected, there will be exceptions that will be accepted for some other merit. Documenting these issues is critical, but they should be approved and inventoried individually. For example:

The Exceptions Inventory

Payload	Destination	Transport	Conditions
Business Reports/Privacy	Web Server/Public	FTP/Authorization	Special Approval

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Administrating the Process

Maintaining a complete list of standards and creating an inventory begins to address the security of data delivery. However, confirming that each payload is being handled appropriately does not address all of the security risks. There are also risks in not checking what else can be done. To do this, include activities that close "back doors." This will eliminate opportunities for breaches in security often overlooked. Complete the overall protection processes by including the following:

Hardening

Removing or eliminating the functions in hardware that cannot be secured is crucial. In essence, what is not being used should not be available:

- Turn off the other delivery options when not needed.
- Isolate access to systems that do not protect the payloads appropriately.
- Look at deliveries where special approval has been given. These must be monitored continually.
- Close back doors or processes that can be used without proper administration.

Monitoring

Use tools for verifying that processes are in place and being followed:

- Payload => sniffers, access logging,
- Transport => trace route command, baseline , test deliveries
- Destination => ping, IDS, physical site survey

Auditing

Once the process is in place, there is still the verification that each element is correctly structured. For this assurance, provide an audit:

- Audit payloads, destinations and transports.
- For payloads, drill down to specific files and confirm their actual status.

Automating the Process

Ultimately, new tools can be created to automate the management of data delivery beyond the scope of individual delivery technologies. Until that time this roundhouse model can be used to systematically review the elements controlling data delivery throughout an enterprise. It does not replace the diligence of system administrators, operators and engineers, but it does present a well-outlined inventory of the security structure and a simpler format to address the question, are you in compliance with your data delivery policy.

Sources Regarding Policy and Practice

1) Kabay, M.E., Ph. D., *Identification, Authentication and Authorization on the World Wide Web*.
   URL http://secinf.net/info/www/iaa/iaawww.shtml
2) Miller, Walter M, *Data Warehouse Data Modeling*
   URL
   http://www.dmreview.com/portal.cfm?NavID=91&EdID=216&PortalID=12&Topic=8

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

3) Open Systems Interconnection Reference Model
URL http://www.its.bldrdoc.gov/fs-1037/dir-025/_3680.htm

Sources Regarding Technology and Implementation

1) The National Office for the Information Economy, Government Online.
URL
http://www.govonline.gov.au/projects/strategy/The_Guide_to_Minimum_Web_Site_Standards/Introduction.htm
2) Buckwalter, Jeff T., "Frame Relay: Technology and Practice," Addison Wesley Longman, Inc., Reading Massachusetts, 2000
3) Huston, Brent L, Technical Editor, "Hack Proofing Your E-Commerce Site," Syngress Publishing, Rockland, MA, 2001
4) Wenstom, Michael J., "Managing Cisco Network Security," Cisco Press, Indianapolis, IN, 2001

© SANS Institute 2001, Author retains full rights

Last Updated: October 6th, 2015

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Tysons Corner 2015	**Tysons Corner, VAUS**	**Oct 12, 2015 - Oct 17, 2015**	**Live Event**
SANS Gulf Region 2015	**Dubai, AE**	**Oct 17, 2015 - Oct 29, 2015**	**Live Event**
SANS Tokyo Autumn 2015	**Tokyo, JP**	**Oct 19, 2015 - Oct 31, 2015**	**Live Event**
SANS Cyber Defense San Diego 2015	**San Diego, CAUS**	**Oct 19, 2015 - Oct 24, 2015**	**Live Event**
SANS South Florida 2015	**Fort Lauderdale, FLUS**	**Nov 09, 2015 - Nov 14, 2015**	**Live Event**
SANS Sydney 2015	**Sydney, AU**	**Nov 09, 2015 - Nov 21, 2015**	**Live Event**
SANS London 2015	**London, GB**	**Nov 14, 2015 - Nov 23, 2015**	**Live Event**
Pen Test Hackfest Summit & Training	**Alexandria, VAUS**	**Nov 16, 2015 - Nov 23, 2015**	**Live Event**
SANS Hyderabad 2015	**Hyderabad, IN**	**Nov 24, 2015 - Dec 04, 2015**	**Live Event**
SANS San Francisco 2015	**San Francisco, CAUS**	**Nov 30, 2015 - Dec 05, 2015**	**Live Event**
SANS Cape Town 2015	**Cape Town, ZA**	**Nov 30, 2015 - Dec 05, 2015**	**Live Event**
Security Leadership Summit & Training	**Dallas, TXUS**	**Dec 03, 2015 - Dec 10, 2015**	**Live Event**
SANS Cyber Defense Initiative 2015	**Washington, DCUS**	**Dec 12, 2015 - Dec 19, 2015**	**Live Event**
SOS: SANS October Singapore 2015	**OnlineSG**	**Oct 12, 2015 - Oct 24, 2015**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**