Utilizing the ™ CipherShare Platform within Government and Military

Table of Contents

1. The Challenge – Ensuring "Need to Know"

From intelligence to research and development to human resources data, the spectrum of electronic information stored and shared by government and military personnel is increasingly broad and varied. One of the greatest challenges faced by both government and military agencies is the need to ensure that stored and transmitted information is available only to those who should have access to it. This challenge – providing "need-to-know" access to information – is becoming an increasingly difficult problem to solve as the complexity of the devices, applications, networks and personnel involved in generating, storing and retrieving this information also increases.

This problem is especially acute in collaborative environments, which by intent, are designed to enable the sharing of information among a "community of interest" (COI). In general, collaborative solutions that support COI's do not selectively determine who, between members of the COI, has access to specific data or documents. Even if that selectivity is provided through access control, the data or documents are usually stored in clear text on both the accessing devices (i.e. desktops and laptops) and back-end servers. This information is vulnerable to compromise by insiders, hackers and computer theft.

In fact, insider threat is emerging as one of the most important information security concerns for both the public and private sectors since insiders know where important information is kept, the safeguards used to protect that information and how to bypass them[1]. According to a recent report, insider threat represents a greater security risk than cyberterrorism[2].

Defeating the insider threat requires a new approach, one that recognizes that information security begins with the protection of data – at the level of the data asset itself – everywhere, whether at rest or in flight. By combining asset level protection with very precise control over access to that asset, an organization can ensure that very selective and very secure disclosure over information is established and maintained.

2. ™ CipherShare - Meeting the Challenge

CipherShare is a secure collaboration solution, combining sophisticated document management features, highly optimized file sharing services, shared task lists, messaging and chat with comprehensive data security for all shared information. With CipherShare, organizations establish secure, virtual workspaces across network boundaries to enhance workgroup productivity. CipherShare employs strong authentication, granular access control and transparent data encryption to ensure that collaborative information is protected at all times — on servers, on desktops, on mobile computing platforms, and at all points in between.

[1] Study looks to define 'insider threat' - http://www.nwfusion.com/news/2002/130577_03-04-2002.html
[2] Analysis: Insider Threat Greater Than Cyberterrorism Threat - http://www.eedesign.com/pressreleases/prnewswire/80257

Simple to deploy and simpler to use, CipherShare caters to today's distributed and mobile workforces, where workgroups and other 'communities of interest' assemble, collaborate and often disband, within a short time frame. With its 'always on, no compromise' security, CipherShare provides 'need-to-know' access to sensitive information, ensuring that only authorized persons, whether internal or third-party personnel, can view or modify documents and files. Without explicit permission to view a file, a user will not even know the file exists.

A high performance client/server application, CipherShare offers a number of features that combine to offer strongly enforced "need-to-know" access:

1. **Strong Authentication and "End-to-end" Encryption** – All CipherShare users are strongly authenticated and transparently issued public and private keys, and data is encrypted everywhere: on the client, during transmission and on the server. No data – even the data on a lost or stolen laptop – can be accessed unless the right public/private key combination is provided. A specific document or file is only visible to, and can only be de-encrypted by, those individuals with whom the file has been explicitly shared.

2. **"Server ignorance"** – The CipherShare server itself does not directly reference – or "know about" - the content housed within it. Even in the event of a server breach resulting from attack, the degree of data compromise is extremely limited since no unencrypted data can be directly accessed through the attack.

3. **Absence of a "Super User"** – All data is encrypted at the level of an individual user. This has two consequences:

    - **Administration functions are separated from data access functions** – A designated administrator cannot access any CipherShare data that has not be explicitly shared with that administrator. This substantially reduces the impact of insider threat since an individual can expose only that data shared with them.
    - **Limited data replication** – Only CipherShare data that is shared explicitly with a specific individual is replicated on that individual's client machine. Thus even if a client machine is compromised, the damage in terms of data exposure is limited to the data shared with that individual.

4. **Key Signing / Verification**: CipherShare offers a rapid method to achieve identity verification through key signing, an essential component of secure environments. In the CipherShare model, a Security Officer verifies and digitally signs the identity of each user through an established security protocol and the user's digital signature. Other users are alerted when the user has been fully verified.

5. **Digital Signatures for Data**: Encryption alone does not protect against forgeries. For example, if a server is compromised, an attacker can intercept messages and shared documents and replace those messages or documents with his own. This attack can be combated by automatically applying a digital signature to each sent message and each document shared. These digital signatures authenticate the encrypted data and prevent forgeries, even on a compromised server.

6. **Digital Signatures for Share Lists**: If a server is compromised, an attacker could add a forged user to a Share List in order to gain access to a document. To combat this attack, CipherShare applies a digital signature to the Share List at the point of encryption. A compromised server cannot modify a Share List without being detected.

3. CipherShare Case Study

The following is a case study of the way in which one of our customers has utilized CipherShare's highly secure and flexible framework to meet their specific needs.

3.1 Case Summary:

A nationally distributed organization providing highly sensitive security consulting, the customer relies on CipherShare's fully secured, tightly controlled collaboration and document management capabilities to bind its distributing consulting team together.

3.2 Case Details:

As a consulting firm specializing in security, risk and threat analysis, PKI implementation and PKI integration for government and military organizations, the customer has a considerable stake in ensuring that its internal communication is completely secured, especially since their consultants are working with extremely sensitive client security information. Their credibility rests on operating in a manner that ensures their client's confidentiality and privacy.

This need for full security is exacerbated by the fact that the customer operates as a nationally distributed, and "virtual" team: their consultants – generally operating on client premises - must be able to collaborate effectively across a variety of cross-institutional boundaries and perimeter security systems, while guaranteeing that all communication is secured at rest on all local and central computers, and in transit.

The customer offers consulting report and specifications documents developed through an iterative cycle during which consultants with specialized expertise provide input at various stages. The customer must be assured that all document versioning is tightly controlled, auditable and completely traceable.

Finally, the customer must be able to guarantee that documents are distributed on a "need-to-know" basis only, providing a "Chinese wall" between specific client information repositories.

The bottom line? The customer must be able to rely on a full secured, centrally accessible collaborative and document management environment, which automatically provides check-in/check-out, full versioning, modification auditing, and task management. For over 2 years, the customer has relied on CipherShare to provide these services.

4. About Proven Security Solutions

Proven Security Solutions is a software development and consulting company specializing in highly secure and completely transparent applications of encryption and key management.

Proven Security's mission is simple - making state-of-the-art cryptographic security an invisible component of high value software applications.

For more information on, please visit www.provensecuritysolutions.com or e-mail us at info@provensecuritysolutions.com.

