Serving up data files to multiple classified networks

Doug Stapleton, Executive IT Architect
IBM Australia Limited
Canberra, Australia
dougstap@au1.ibm.com

Abstract— **Today, large and complex geospatial reference files are required on Defence networks of different classifications. This paper proposes a secure mechanism for allowing the same version of a file to be accessed from different classifications, while also providing assurance to users that they are accessing the latest version of that file.**

I. INTRODUCTION

Today, large and complex geospatial reference files such as those showing the terrain detail of training areas need to be available for simulation exercises using simulators that may be at different classifications. Generically, this requirement can be described as a method of hosting reference files on a server that can be accessed from different classifications. This paper proposes a secure mechanism to allow the same version of a file to be accessed from different classifications.

One of the business issues is a file getting out of sync across the environments. Traditionally, these files need to be loaded and hosted within each security domain, raising the inevitable question as to whether a user is accessing the latest file. By hosting the file on a shared server that is accessible from all domains, the user is assured of accessing the latest file.

Figure 1 shows how a single file server can be accessed from three different classified networks. More specifically the figure illustrates how a file that is classified at the Top Secret (TS) level be stored on a file server that has a link to the lower classification networks of Secret and Protected This paper discusses the classification levels used in the *Australian Government Security Classification System* [1]; but the same principles would also apply to other national systems.

The server will hold all files in their encrypted form. The files would be loaded from the secure domain with encryption determined by the classification level. The encryption algorithm used is the method accredited for the highest level network [2 page 234ff]. Using the same algorithm and key length, a set of keys is used for TS files, another for Secret files and yet another for Protected files. The decision on whether to use Symmetric Encryption or Public Key Encryption can be made later, depending on factors such as the ease of securely sharing key material and other key management issues [2 page 254].

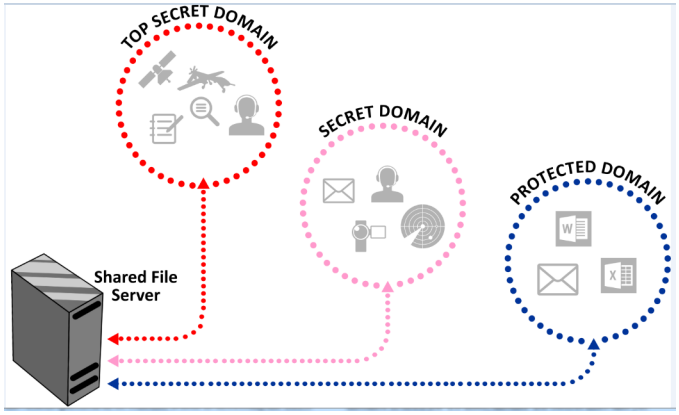

Figure 1 File server accessible from three domains

Typically, the domains are configured to use what is referred to as "System High Security". That is, all users on the TS domain must have a TS clearance, all users on the Secret domain must have at least Secret clearance and all users on the Protect domain must have at least a Protected clearance. Users with a higher clearance can access files at the same or lower clearance level as illustrated in the following Figure 2.

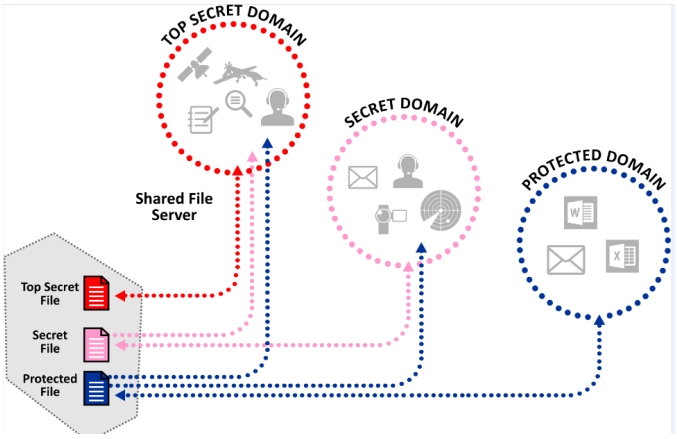

Figure 2 Relationship of files in various classifications with users in different security domains

For example, a geospatial reference file can be loaded at the lowest domain level of Protected and be instantly accessible to users in all three domains (i.e. Protected and above).

With all the data on the file server being encrypted, we can consider the consequences of a data spill. If the file server is hacked from a lower level network, the data that can be revealed is all encrypted and the decryption keys do not exist on the lower level network, thus preventing any unauthorised disclosures.
The shared file server is not accessible from the Internet or other unclassified networks, but it effectively wouldn't matter as the data would be encrypted in any event.
Data is loaded from the classified domain to which it relates. Thus geospatial reference files at the Protected level would be loaded from the Protected domain and instantly be accessible to the higher level domains along with access to the shared file server.

A. Some Infrastructure Detail

Figure 3 shows how for each domain, there is an internal file server visible within the domain and a secure link between that file server and the shared server outside of the domain.

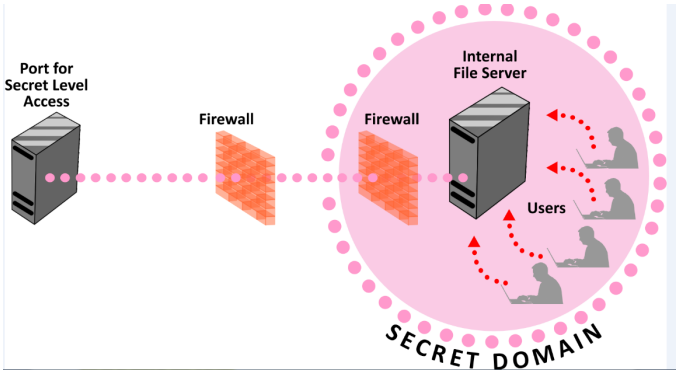

Figure 3 Three domains with internal files servers connected to shared server (illustrated for one domain)

Firewalls
The shared file server has three ports for access, one for each classification level or domain which is making a connection, as illustrated in Figure 3.
It is important to note that data visible on each port is strictly only at the classification level for that port and secondly that it is encrypted. Thus, the port connecting to the secret domain will only have encrypted files visible which are at the Secret classification level. Decryption of a file does not take place until it is available within the domain on the internal file server.

B. File Loading

This section considers how a file is loaded onto the shared file server. Files are passed unencrypted to the internal file server, and are encrypted using the key applicable to that domain and then passed in encrypted form across a secure link to the shared file server where they are stored.
What is passed? The encrypted directory structure and file name and the encrypted file contents. With each file, an encrypted pass phrase is included which allows the shared file server to work out the port to return the file list to within its appropriate directory structure. This pass phrase is known only to the internal file server and the shared file server, an example might be; "this file is classified at the Secret level". This phrase is used consistently in the encryption of all files from that domain. The shared file server can examine this pass phrase stored with the file and test the decryption algorithm with each domain pass phrase key to determine the classification of the file. An important point to note is that the shared file server only has decryption keys for the pass phrase associated with the file, it does not hold the decryption key for the file content since that decryption is performed inside the domain on the internal file server.

C. File Retrieval

This section considers how a file is retrieved from the shared file server. From a user perspective, they will connect to the shared drive as a networked drive mapping to their local computer. When using file explorer, the user will expect to see files that are at or below the classification level of the domain on which they are logged on. For example, a user who is logged on to the Secret domain, will expect to see files on the networked drive which are Secret and below (i.e. including Protected). Users must not be allowed to see any files from a higher domain (i.e. TS in this example).
This raises two generic issues; firstly how does the internal file server see files on the shared file server which are at the same classification, and secondly how does the internal file server see files on the shared file server which are below the classification level of this domain.

1) Files at the same Classification Level

The internal file server makes a "List File" request to the shared file server. This request goes to the port on the shared file server dealing with the same classification level, as illustrated in the following Figure 4.

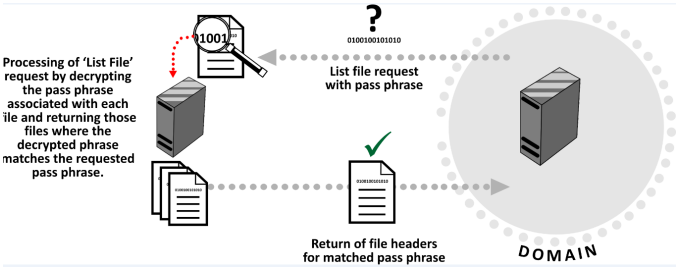

Figure 4 Illustration of same classification level file transfer

The shared file server then scans the list of files on the shared drive and attempts to decrypt the pass phrase associated with each file. If the decrypted (pass phrase) is equal to the known (pass phrase) then the encrypted name of the file is passed back to the internal file server for decryption and display to the user. When the user selects a particular file, the encrypted file is retrieved and passed to the internal file server within the domain where it is decrypted for passing to the user.
Depending on internal policy, the link between the user and the internal file server can be encrypted for greater internal security within the domain. This would prevent unauthorised

users or processes from being able to inspect the file as it is being delivered to the correct user.

2) Files at a lower Classification Level

Referring back to the illustration at Figure 2, the internal file server will have legitimate access to files at a lower classification level. Because those files can only appear on the port of the shared file server applicable to that lower classification, the internal file server makes a separate "List Files" request to that lower classification port.
This is illustrated in the following Figure 5.

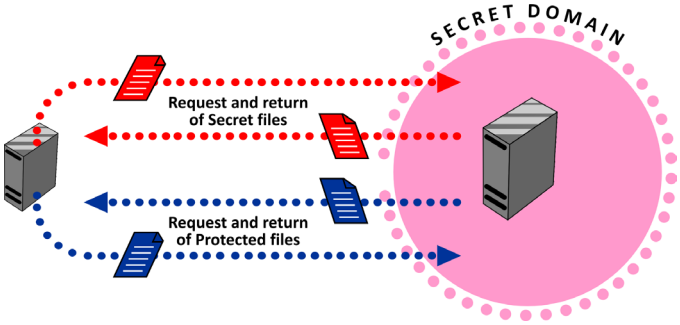

Figure 5 Retrieving protected data at the secret level

In our example of a user in the Secret domain, the networked drive would display for that user, two sets of files; the first directory structure at the Secret level, followed by a second directory structure at the Protected level.

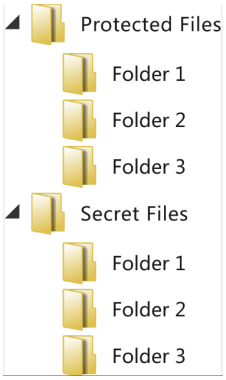

Figure 6 Directory structure for both Protected and Secret files

When the user selects a file at a lower classification than this domain, it would be retrieved and decrypted for that user. This is done by holding the applicable decryption keys in the related internal file server and each domain above that classification. In our example, the internal file server on each domain for TS, Secret and Protected would hold the decryption key for Protected. A point to note is that an internal file server can only load files to the shared file server at its clearance level. For example, in the Secret domain, files which are loaded to the shared file server are automatically encrypted at the Secret level. If the intent is to load a Protected file, it must be done on the Protected domain.

D. The security enforcement point.

Given that the shared file server is connected to three different domains, how and where is the security enforcement done? As illustrated in the following Figure 7, the classified domain is connected to the shared file server via a firewall which is considered to be the security enforcement point. The firewall rules state that the only traffic that can pass across this firewall is between the internal file server and the shared file server. A refinement of this, which is commercially available in firewalls and routers of today is to allow the higher classification internal file server to connect to the ports on the shared file server for the same or lower classifications.

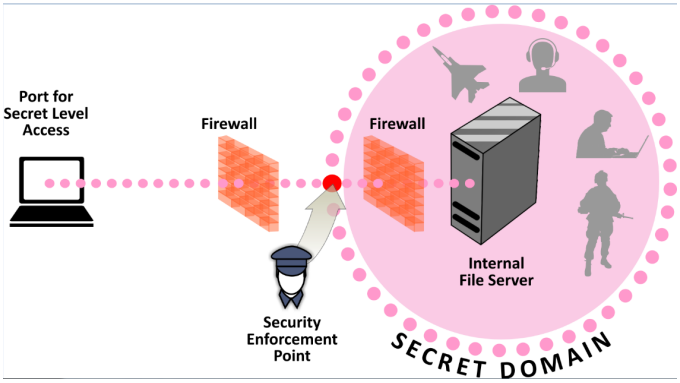

Figure 7 Security enforcement point

Additional assurance is available by grouping the port combinations in a "domain" and "priority" as appropriate [3].

E. The Cross Domain Aspect

Taking a broad view of the ability to load files in one domain and read them in another, would introduce this as an aspect of Cross Domain Transfers and thus subject to the extensive rules in the ISM [2 page 258ff]. At a practical level, only certain file types would be suitable to ensure that malware of any description cannot possibly be transferred from one domain to another. Thus, careful file type filtering and assurance needs to be implemented twice, once on the loading of a file and secondly on the decryption of the file. For example, JPEG may be a suitable image format that can be filtered on the file load to provide assurance that the JPG file follows all the rules applicable to the JPEG format. Then again on the file decryption, a file claiming to be a JPG file would be subjected to the rule check to ensure that all JPEG format rules were observed.

F. Benefits and further refinements

The networked drive will appear to the users showing reference files available to them at the same or lower classification of the domain to which they are logged in. This scheme will not deal with individual access control which can be provided as an additional layer. A future option could also deal with files with particular caveats, however the decryption

would rely on the user providing the appropriate decryption key for that caveat. Another refinement would be to provide a shared database which would follow the same concepts but return only rows and elements of shared tables that were at or below the classification of the user.

A refinement for efficiency would be to build a copy of the domain directory file structure on each internal file server, and only go out to the shared file server for files held at a classification below this domain. Thus a TS internal file server, would only reach out to the shared file server to scan files at the Secret and Protected level. A Secret internal file server would only reach out to the shared file server to scan for files at the Protected level. This arrangement may also have implications for security accreditation, since the top level classification (presumably TS) does not need to place any files on the shared file server

II. REFERENCES

[1] http://www.protectivesecurity.gov.au/informationsecurity/Pages/AustralianGovernmentSecurityClassificationSystem.aspx

[2] 2015 Australian Government Information Security Manual - Controls. http://www.asd.gov.au/publications/Information_Security_Manual_2015_Controls.pdf

[3] Greg Goblirsch, "Secure Routing Features in Thinklogical's VX Router", 2011 www.thinklogical.com/pdf/white-paper-secure-routing.pdf