Preventing Data Spills from Classified Networks

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

Abstract— **When classified files are moved around, from one network to another, often over unclassified networks such as the Internet, they may be protected by simple encryption. This paper proposes a more secure method which ensures that the target network is authorised by the file owner and that access is controlled in an agreed manner.**

I. INTRODUCTION

The creation of classified files (whether data or documents) is under control of the file owner at the time of their creation. Subsequently when the file is moved, it is easy for the original document owner to lose control of who has access to the file over time.

The original system that creates the file has responsibility for the protection of the classified file when it is at rest in its original environment. From a security enforcement point of view, this is often done by ensuring that the file is created in a domain corresponding to the classification of the document, so that all users at least have a clearance to view the document or data in the file. Of course they may not have a 'need to know' and further access control within the domain will limit access rights of users who do not have a 'need to know' (such as payroll or operational data

The challenge is to move the file to a new security domain without allowing a data spill to occur in transit across unclassified domains such as the Internet. The ISM [1 page 303] defines a data spill as "The accidental or deliberate exposure of classified, sensitive or official information into an uncontrolled or unauthorised environment or to persons without a need-to-know".

As illustrated in Figure 1 the original system that creates the file is responsible for secure storage within the domain. Apart from metadata that may tag the file classification, the file itself at rest may be left unencrypted on the basis that all users in the domain are at the required classification level to view the contents (acknowledging the further access control issues).

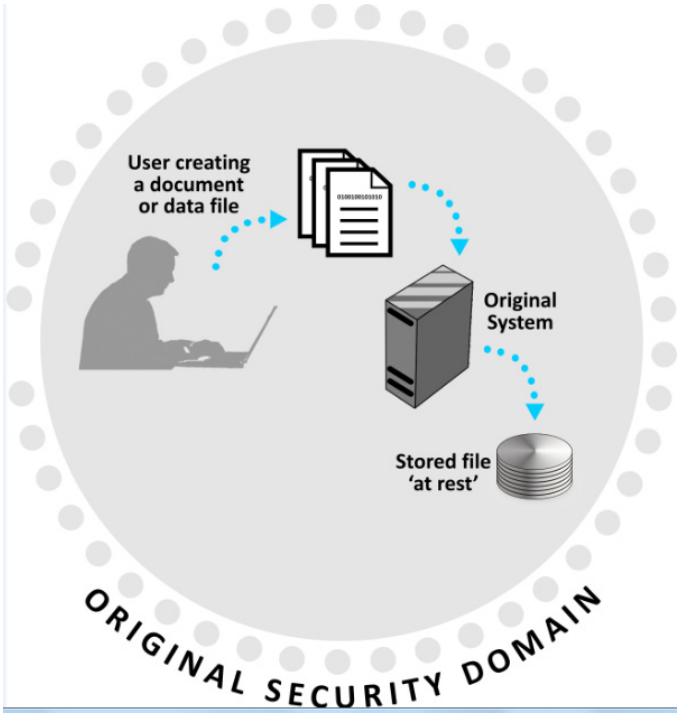

Figure 1 Creation of a file in the original security domain

II. MOVEMENT OF FILES

When the file is moved away from its original creation system, how can the integrity of the file be assured and in particular, that the target network is authorised and the individual user is authorised before the file is decrypted and made available at the end destination. These concepts are illustrated in Figure 2

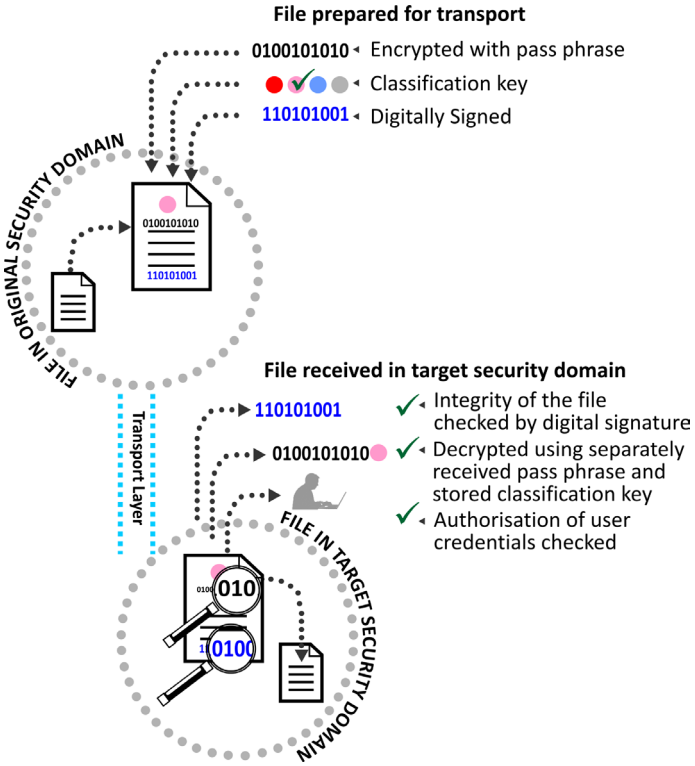

Figure 2 Moving a file to a Target Security Domain

A. *Infrastructure Requirements in Original Security Domain*

To prepare a file for moving, there must be a set of trusted infrastructure in the Original Security Domain, which will accomplish the following things:

- having regard to the classification metadata tag, encrypt the file with a unique system generated pass phrase. This will mean that files cannot be generically decrypted but must be correctly decrypted by the receiving system that will have separately received the generated pass phrase.
- digitally sign the completed encrypted file and keep the signature results.
- securely and separately to the file transmission send to the matching infrastructure in the Target Security Domain, both the system generated pass phrase and the signature results.
- specify as part of the file package whether there are any user restrictions on the Target Security Domain (a set of named users or a generic classification level that is check by the infrastructure at the Target Security Domain.
- package the file and attributes into a self-executing archive which will check in with the matching infrastructure on the Target Security Domain.

B. *File Transfer*

The transfer of the file to the Target Security Domain, can be accomplished by any desired means, such as email attachments, web file upload, FTP, other file transfer mechanisms. Noting that the file is encrypted and signed. This will prevent the file being revealed in transit (unless the encryption itself is broken).

C. *Infrastructure Requirements in Target Security Domain*

To receive a file from the Source Security Domain, there must be a set of trusted infrastructure in the Target Security Domain, which will accomplish the following things:

- check the digital signature of the file and if valid pass it for decryption;
- this infrastructure will already be setup with the classification decryption key (sent separately by safe hand);
- using the combination of the classification decryption key and the applicable separately received pass phrase, to decrypt the file if possible;
- ensure that the local system presents acceptable individual identities if the file is locked down to that level.

D. *When files go astray*

What happens when a file is opened on a security domain that is not intended, as illustrated in Figure 3. Someone who intercepted the file may for example try to open it in an unclassified environment or a lower level network or another countries national infrastructure; other than the intended target. In each of these cases, opening a file runs a small part of the file as an executable that will look for a local instance of the specialised infrastructure set. This can be done via a URL which will be resolved in each different domain to point to different sets of infrastructure with different results. As an example, the URL might look something like:

www.mysecureinfrastructure.com

Using ordinary TCP/IP mapping techniques this can be setup within a network to resolve to a particular point, i.e. the legitimate set of infrastructure. If the file is opened on the internet, this would resolve to a special catch-all set of infrastructure that would log the file opening attempt and raise suitable alerts, but would not decrypt the file (that infrastructure would not hold any decryption keys).

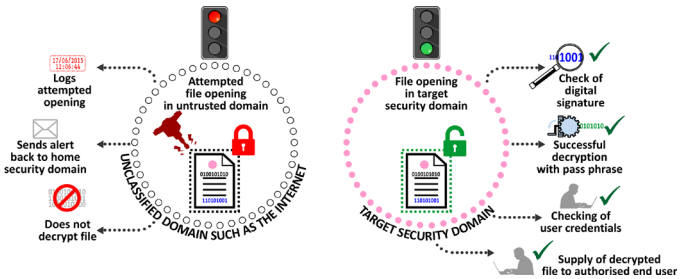

Figure 2 Illustration of an attempt to open a file in an unauthorised place

The other possibility is that a file is opened in a set of national infrastructure which is not authorised. It would be likely that when the executable reaches out to find www.mysecureinfrastructure.com that this would be blocked locally. Thus the behaviour of an attempt to open a packaged file set when it cannot connect to trusted infrastructure (or is redirected to untrusted infrastructure without the correct pass phrase and decryption keys) would default to no action, leaving the file contents encrypted and secure, thus preventing any data spills.

III. REFERENCES

[1] 2015 Australian Government Information Security Manual - Controls. http://www.asd.gov.au/publications/Information_Security_Manual_2015_Controls.pdf