IT03.09

Document Access Servlet
(DAS)

warfighter/Operator RESULTS

PERFORMANCE | ASSESSMENT LEVEL | TECHNICAL SUPPORT/TRAINING | CAPABILITIES/FINDINGS | WARFIGHTER PERSPECTIVE | WARFIGHTER COMMENTS | CONCLUSIONS | RECOMMENDATIONS | HOME

IT03.09 ASSESSMENT COMPONENTS

WARFIGHTER | TECHNICAL INTEROPERABILITY | INFORMATION ASSURANCE | SEIWG

(If a text entry is not linked, there is no assessment in that category for this trial)

PERFORMANCE

The Document Access Servelet (DAS), IT03.09, was an excellent product to control access to mass circulated documents. DAS provides a significant improvement to control access in this modern era for documents re-transmitted to offices not authorized to view the enclosed data. The trial worked consistently well and issues encountered were easy to troubleshoot and solve. Most issues related to system configuration, setup, and MSEL execution not product performance. The DAS trial met the CWID objective for Net-centric Enterprise Services.

BACK TO TOP

Assessment Level

Thirty-eight warfighters evaluated the trial through JDCAT questionnaires or observation forms at the following sites: NSWC Dahlgren, VA, US (11 warfighters), USNORTHCOM, CO, US (5 warfighters), SPAWAR, CA, US (6 warfighters), USEUCOM, Stuttgart, GE (5 warfighters), Shirley's Bay, Ottawa, Ontario Canada (2 warfighters), Hanscom AFB, MA, US (6 warfighters), NZDF RNZAF AOC, Auckland, New Zealand (3 warfighters).

Technical Support/Training

DAS was very easy to use and required minimal training. Site support varied as some had on-site representatives while others coordinated via internet chat, email and telephone to tech reps at other sites. Warfighters at most sites without tech reps said remote trial reps were responsive. One warfighter reported emailing requests for support but the response was not timely. Technical documentation was available, but one mentioned the handbook did not cover the certificates installation procedures. Warfighters mentioned that the server identified in the

playbook for file retrieval was not listed correctly. Once the proper download location was known, the rest of the procedures were clear and easy to follow.

BACK TO TOP

CAPABILITIES/FINDINGS

IMPROVE INFORMATION ASSURANCE Warfighters almost unanimously agreed that DAS improved information assurance and was a simple and effective means of distributing sensitive documents. From their observations, the warfighters could not determine if the sensitive documents were indeed secure or if the decryption key (or decrypted file) could be intercepted.

Files were encrypted before posting and community of interest (COI) members downloaded and decrypted them. This limited the number of people who could read the file. One concern was that once someone gets the file and decrypts it, there is nothing preventing distribution. This is not a tool limitation, but a security and personnel issue. The warfighters wanted to know who in the group has encrypted file access. The encrypted file access list was only available to the trial operator who controlled the users in each group and ensured proper certificates for the appropriate warfighters.

DAS worked well for information assurance within changing COI and demonstrated usefulness in a coalition environment where file access control is required. The trial also showed potential in non-wartime operations, such as access to sensitive files (e.g. acquisition data or privacy act data).

Warfighters questioned whether there was a file size limit and commented that this area required more robust testing. Recommendations to improve encryption and decryption testing included using larger files and different types (e.g. text, pictures, Power Point and tables).

IMPROVE VERTICAL AND HORIZONTAL INFORMATION DISTRIBUTION DAS improved vertical and horizontal information distribution as it applied to access control. The trial used a COI concept to securely share information between users in certain groups. These groups could be organized vertically, horizontally and any combination thereof. The trial technology improved information security so that individual documents were safely distributed and accommodated in an ever-changing need to know environment.

One significant information distribution issue is that the encryption process did not automatically add the creator to the access list. If a warfighter forgot to add himself, they lost all access to their own document as the original was always deleted.

Warfighters had mixed feelings about data access. Distribution through a web portal worked well coupled with the encryption. On the other hand, there was a lack of accessibility to files encrypted by the software when connectivity was loss or a workstation removed from the network. When not connected to the network, COI membership verification was not possible, and encrypted data files were not accessible to the user until connectivity was reestablished. Connectivity may be a problem for units or personnel with intermittent connectivity issues.

IMPROVE HORIZONTAL DATA ACCESS, FUSION AND INTEGRATION Most warfighters thought horizontal data access was improved but they were less sure about fusion and integration capabilities. Access will definitely improve if all documents are kept in the same location yet protected by annotating the appropriate COI. This is a much easier solution than creating separate inaccessible areas in order to deny certain COI access.

The Secret Agent software was almost transparent as it allowed control of shared data on network servers. General file sharing would not have been possible in a coalition environment without a similar tool. The software did not in itself speed up data movement or provide a delivery mechanism for information exchange, but it allowed documents to be quickly encrypted, transmitted by normal email or portal means and quickly decrypted. A user certification drag and drop procedure allowed operators to access COI as well as deny data access to unauthorized users.

BACK TO TOP

WARFIGHTER/Operator PERSPECTIVE

Almost all warfighters recommended using DAS (in its current configuration) in a military or HLD/HLS environment. Its familiar Windows layout and simple, intuitive features provided an effective means of distributing sensitive documents of all file formats. Although they thought DAS was secure, they did not know to what classification and deferred to more robust testing and the Information Assurance assessment. Almost all warfighters said they had never used a system like DAS before. The most similar warfighter experience was using Windows with security groups to setup file sharing or email digital signing via PKI.

During the scenario, warfighters downloaded CTF daily briefings or HLS/HLD SITREP files from the respective file servers. Warfighters saved the downloaded file to their desktop and then decrypted it based on their membership within specific COI. When they opened the document, the file was unencrypted, the encrypted container file was automatically deleted and warfighters were subsequently removed from the COI. Warfighters that deleted the briefings and SITREPS from the desktop noted that there should be a warning when the user deletes something that was originally decrypted. Also, files should be deleted securely. If files are not securely deleted, the computer can be compromised. To securely delete files, it must be performed through DAS.

Warfighters encountered very few problems, but reported some administrative issues, such as not being added to a COI, or not being able to read an encrypted document. Hanscom reported that certificates were not loaded originally. Some warfighters reported that an encrypted file failed decrypting during the first attempt, but decrypted on the second attempt.

The warfighters responsible for encrypting briefings for different COI had no problems doing so. A problem arose where the user encrypting the file lost access and rights to the file unless they saved a copy in another location with a different directory and/or name. Encrypting files only took a few seconds.

The DAS operators encrypted and decrypted documents, and controlled access to COI as

necessary by adding and deleting members. Members were added and subtracted based on MSEL-based requests from staff role players. When members were removed from a COI, they could not decrypt documents. When added back into the COI, they successfully decrypted documents associated with the COI. COI membership and decryption rights control worked well, was very effective, and immediately enforced. Ad-hoc testing also supplemented the MSELs and proved that this function worked. During MSEL play, only individual files were encrypted, although DAS does have the capability to encrypt and decrypt folders of files.

Although the majority of warfighters encrypted documents without problems, a few warfighters experienced some minor technical issues, such as connectivity and Windows locking up while decrypting the downloaded document. Some warfighters thought encrypting within a closed CTF Secret network was of questionable value and if the network allowed emailing DAS encrypted docs to the HLD/S network then it would be more valuable.

Warfighters also expressed concerns about deleting files in the system directory as it could have disastrous effects, as well as the risk of inadvertently sending the wrong file to unauthorized personnel. System users must be briefed on information assurance requirements to ensure information is not compromised.

Warfighters had several suggestions for improvements. Quickly and safely encrypting documents is extremely important with the amount of information exchange via emails and internet. Incorporating encryption capabilities into email software such as Outlook would allow email encryption and decryption, including attachments and documents on the desktop.

Another suggestion was modifying the Secret Agent icon for an encrypted file indicating that one does not have decryption access or those files are not visible to the end-user. When a file is encrypted, the original file is deleted. Therefore, if the party that encrypts the document is not added to one of the COI, they cannot view it again. This was an issue for some warfighters and they recommended that Secret Agent software automatically add the encrypting party to a COI when a file is encrypted. At a minimum, the software should not delete the original so that the user still has access to personal documents.

Warfighters also recommended improvements with the DAS audit log and system messages. Warfighters tasked to export the DAS audit log to a file, encrypt it, and post the document to the file server, did so without any issues. These warfighters noted that the current audit log does not capture all events executed and requires a more detailed user action event history. Secondly, the system messages could be more user-friendly. Several messages are generated in machine language, which requires some level of translation to be fully useful to operators.

Warfighters conducted some supplemental testing during Execution Free Play periods. They used SATSIM hardware configuration to simulate a bandwidth-constrained environment. San Diego and Dahlgren sites participated in this testing and encryption and decryption worked successfully. The activities performed slightly slower due the lower bandwidth network, but worked well. One warfighter encountered a situation where the first attempt to encrypt and decrypt a ZIP file occasionally failed but succeeded on subsequent attempts.

BACK TO TOP

WARFIGHTER/Operator COMMENTS

“Pending Technical certification I was very impressed with the technology's capabilities and envision operational employment within the HLD/HLS environment.”

“The versatility and utility of this product make this a viable technology for advancement.”

“Seems like a very simple and transparent application. Just the kind of thing a warfighter needs.”

“Enjoyable and easy to do. The Secret Agent DAS program was extremely easy to learn and operate.”

“This is one of the smoothest operating trials I had. We worked with pretty small word documents. I wonder how it would perform with larger files, or pictures.”

BACK TO TOP

CONCLUSIONS

The DAS trial performed excellently in CWID, successfully demonstrating improved information assurance and improved vertical and horizontal information distribution. The user-friendly software easily disseminated information through a secure means and is a good application for sharing information between DoD and other agencies that do not have a way to protect data. It may also be useful for sensitive but unclassified traffic such as for HLS/HLD data. For military applications, it adds a level of security for personnel data and other sensitive information.

BACK TO TOP

RECOMMENDATIONS

- Investigate putting the originator in the distribution so they can decrypt their own documents.
- Give all warfighters the ability to determine who is in the different certificate groups so they can check who they are authorizing access.
- Modify Secret Agent software to add the encrypting party to the COI when a file is encrypted.
- Improve the user-friendliness of system messages by deciphering machine language for the user.
- Demonstrate Secret Agent software using a variety of file types and sizes in a bandwidth-constrained environment.

BACK TO TOP

WARFIGHTER/Operator RESULTS ON THIS PAGE

PERFORMANCE | ASSESSMENT LEVEL | TECHNICAL SUPPORT/TRAINING | CAPABILITIES/FINDINGS | WARFIGHTER PERSPECTIVE | WARFIGHTER COMMENTS | CONCLUSIONS | RECOMMENDATIONS | HOME

IT03.09 ASSESSMENT COMPONENTS

WARFIGHTER | TECHNICAL INTEROPERABILITY | INFORMATION ASSURANCE | SEIWG

(If a text entry is not linked, there is no assessment in that category for this trial)

GENERAL DIRECTORIES

FINAL REPORT DIRECTORY | ASSESSMENT BRIEFS BOOKLET | HOME