Remote Automatic Test Equipment Software Management

Information Assurance Vulnerability Alert Management

Craig Koepping
NAVAIR
Highway 547
Lakehurst, NJ 08733
craig.koepping@navy.mil

Paul Rajcok
NAVAIR
Highway 547
Lakehurst, NJ 08733
paul.rajcok@navy.mil

Christopher Yoon
NAVAIR
Highway 547
Lakehurst, NJ 08733
christopher.yoon@navy.mil

***Abstract — Information Assurance Vulnerability Alerts (*IAVAs) have become an important part of protecting and securing our systems. Operating systems and their applications are all susceptible to bugs/problems that need to be fixed. Virus definitions, which are released daily, are another important piece of IAVA compliance. IAVA updates are released almost weekly to ensure the integrity of the operation systems and its applications. Systems that are already fielded need to be updated with these approved IAVA updates. These fielded systems aren't always connected to the World Wide Web, so obtaining updates on their own isn't a viable option. They are however, connected to approved servers. A service was needed to obtain these updates on a weekly basis with little user interaction. A user reboot of the system might be needed to ensure that the updates take effect. For the most part the update service is free from user interaction. The application could also be run manually at a fielded site if needed.**

An application with Secure File Transfer Portocol (SFTP) capabilities was used to solve this problem and keep the remote, fielded, systems up to date with the latest IAVA patches. The remote systems are able to connect to the SFTP server, download the approved IAVA updates and install them all without user intervention. The remote computer might need to be rebooted for some of the IAVA patches, but this can be done at the user's convenience. The download and installation status are kept in a log file and database on the remote computer for future reference. If an IAVA patch fails during installation it is marked in the database as an attempted install and another attempt will be made to install it during the next automated update. During the next update this failed patch will be redownloaded and reinstalled. If this process fails a total of three times, it will be marked as failed and no more attempts to download or install will be made. Some updates require a reboot but this is not done automatically for fear that it could possibly affect a user that is currently using the system.

Newly fielded sites already have all the latest patches, they are updated before being sent out, so the application could be run manually to update the database accordingly reflecting that the patches have already been installed. The ability to manually connect to SFTP server and download the updates was also necessary, in case we needed the updates sooner than the weekly update.

Consolidated Automated Support System (CASS) Operations Management Software (OMS) contains this update service for the Navy and Marine CASS ATE and all of this functionally is needed to keep our systems secure/protected and up-to-date with the latest security patches.

This paper will provide an overview of how we provide these IAVA updates to our clients.

I. INTRODUCTION

As security updates, bugs and viruses become more and more prevalent, the need to keep DoD systems up to date has become increasingly important. When approved IAVA updates become available, usually weekly, they need to be installed on the systems usually within a week of its release. Some high priority updates need to be installed even sooner than a week. Keeping the systems up to date manually would require a user at each site to physically log in to each of the systems download the updates and install them. Do to the ever changing complexity of the systems and the users level of system training, this could prove to be a very timely process. We created an update service on each CASS OMS to do most if not all of this work with little to no user interaction. This service runs on a weekly basis but can also be run manually as needed.

II. BACKGROUND

A. System

Consolidated Automated Support System (CASS) Operations Management Software (OMS) supports maintenance and acts as a management information system for the CASS "I" level ATE testing at the Navy's Aircraft Intermediate Maintenance Department (AIMD) and Marine Aviation Logistics Detachments (MALS), and Foreign Military sites that utilize the CASS ATE for avionic repairs. This accounts for 50 sites and approximately 300 pieces of ATE.

OMS primary mission is to assist in the management of a network of CASS stations, leverage aircraft BIT data and historical maintenance data and to process logistics data. This includes Unit Under Test (UUT) job scheduling, monitoring

and automated processing of the Visual Information Display System Maintenance Action Forms (VIDS/MAF). In the US Navy configurations, OMS serves as the Interface between CASS and the Optimized I Level Naval Aviation Logistics Command Management Information System (NALCOMIS) system and will be the link to the Optimized "O" Level NALCOMIS system.

The secondary functions include:

- CASS reliability Analysis (Test Program Set fault isolation/ UUT Trend Analysis)
- CASS Integrated Logistic Support (ILS)
- CASS Configuration Status Accounting
- CASS Availability/ Manpower impact analysis

B. Policy

The Deputy Secretary of Defense issued an Information Assurance Vulnerability Alert (IAVA) policy memorandum on December 30, 1999[2][3]. Recent events demonstrated that widely known vulnerabilities exist throughout DoD networks, with the potential to severely degrade mission performance. The policy memorandum instructs the Defense Information Systems Agency to develop and maintain an IAVA database system that would ensure a positive control mechanism for system administrators to receive, acknowledge, and comply with system vulnerability alert notifications. The IAVA policy requires the Commanders in Chief, Services, and Defense agencies to register and report their acknowledgement of and compliance with the IAVA database. According to the policy memorandum, the compliance data to be reported should include the number of assets affected, the number of assets in compliance, and the number of assets with waivers. The policy memorandum provided for a compliance review by the Inspector General, DoD.

III. UPDATE SERVICE OPERATION

A. Normal Conditions

Server Side: When an IAVA is released it is first tested locally on a similar system to ensure that it doesn't break any functionality of the system. If successful it's added to the Data transfer Server utilizing the Secure Shell (SSH) protocol (Secure FTP) for data transmissions.

Client Side: On a weekly basis, the client application attempts to connect to the host Data transfer Server via a SSH socket connection and download and new or failed updates. New updates won't exist in the client's local directory. Failed updates will exist in this local director, but their corresponding status in the database will be failed. The local database and a log file are updated with the name of each new update. After all downloads are completed, each update is installed. Upon completion the local database and log is again updated with the status of the install.

B. Initial Run

When the system is initially connected, the updates are typically already on the systems but the database hasn't been updated accordingly. Downloading and reinstalling these updates would be a duplication of a process that has already been run. The application can be run with a special argument to simply connect over to the host Data transfer Server via a SSH socket connection and retrieve the filenames of the updates and add them to the database with a status of already installed. This functionality can also be used if the updates were installed manually by a user. The database simply needs to be updated to reflect that as well.

C. User Interaction

If an update needs to be installed before the weekly scheduled time, a user can manually run the application to get the updates off of the host server.

If an update fails, when it should be passing, the update can be run manually. All the downloaded updates are stored locally on the client's computer and they can be run manually for further investigation as to why its failing.

Occasionally an update will require a reboot of the client's OMS. While this could be done automatically, we did not want to interrupt what the user might be doing on the system at the time. As part of the standard operation procedure of OMS, it is policy that the sites reboot their servers monthly, however after certain IAVAs the user will be notified that a reboot it required.

If remote desktop has been set up, a reboot can be performed remotely by an administrator.

D. Errors

If an IAVA fails on a test system, further investigation is needed and an IAVA exception might need to be written. This update will not be pushed to the clients.

If the update service application can't connect to the server an error is logged on the client and the application quits.

If an update fails to install an error is logged and the status of the update is changed in the database. During the next scheduled update, this failed update will be re-downloaded. The application has no way of knowing whether the download was bad or the install failed. This process will occur a total of three times. After the third attempt if the download/install does not work, it is marked as failed in the database. The site administrator and remote administrators can looks at the logs and or database to verify proper IAVA implementation.

IV. AUTOMATED IAVA DATAFLOW

Upon receiving a new IAVA, it must first be verified to work without breaking any functionally before it is added to the SFTP server and ultimately added to the clients.

Identify applicable sponsor/s here. *(sponsors)*

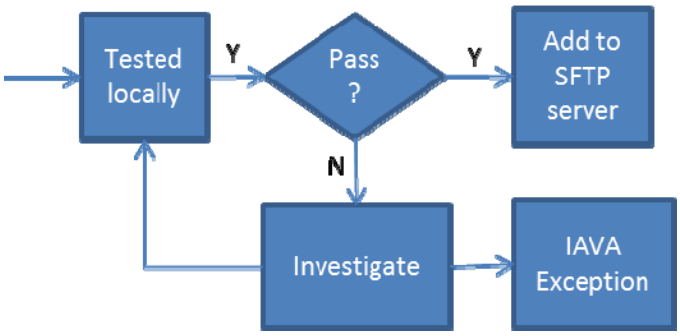

Figure 1. Receiving a new IAVA (Server)

The weekly update service application follows the following process for IAVAs.

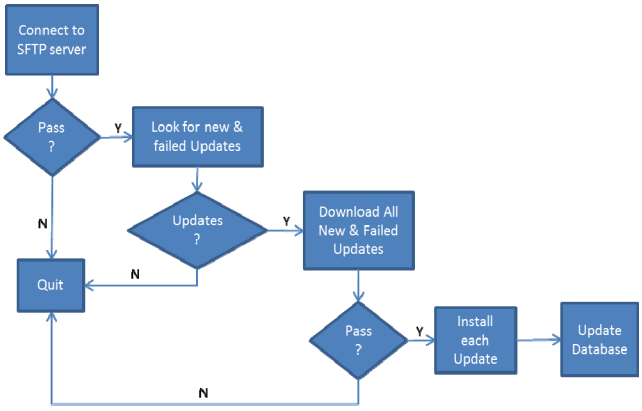

Figure 2. Update Service Application (Client)

V. STATUS

The service currently handles the following updates:

- Microsoft Windows
- Microsoft Office
- Microsoft Hotfixes
- Adobe Flash
- Adobe Reader
- McAfee Virus Definitions
- Other *.exe files (this includes user created install scripts)

VI. PLANS

Further improvements continue to be made:

- Decrease the amount of user interaction needed. Having the computer reboot itself when in an idle state is detected.
- Warning the user that a reboot is about to occur by implementing popup administrative messages.
- Installation of more specific file types. User manuals, temporary work around procedures, registry edits.
- Downloading the latest Test Program Sets (TPS) to the client
- As the next generation of Automatic Test Equipment is produced for use in DoD, the current system will transitioned to the Next Generation OMS (NxOMS) software application with an expanded Software Update Service capability that will handle multiple ATS platforms running different operating systems.

VII. CONCLUSIONS

The CASS OMS software application contains this update service for the Navy and Marine CASS ATE and all of this functionally is needed to keep our systems secure/protected and up-to-date with the latest IAVA security updates today. As this current system evolves and the IA requirements and ATS components increase across all DoD services, the IAVA update management service will also need to continuously evolve to protect the Automatic Test Systems from all network threats

ACKNOWLEDGMENT

None

REFERENCES

[1] Integrating Information Systems into the Net-Centric Environment, Nielson, Angela R., Koepping, Craig. AutoTestCon 2006 IEEE 18-21, Sept.2006 Page(s): 403-409

[2] Utilizing A Service-Oriented Architecture to perform closed-Loop Diagnostics In network Centric environments Nielson, Angela R., Alwardt, Anthony. AutoTestCon 2007 IEEE 17-20, Sept.2007 Page(s): 332-339

[3] DOD COMPLIANCE WITH THE INFORMATION ASSURANCE VULNERABILITY ALERT POLICY Report No. D-2001-013 December 1, 2000