Global Information Assurance Certification Paper

Managing Vulnerability Alerts from Top to Bottom

Kenneth F. Schmidt
October 9, 2000

Overview

Defending corporate and military information from intruders is becoming more and more difficult as companies and the government incorporate technological advances. Unscrupulous individuals or groups have the upper hand because they are often well organized, have the time, and the willpower to find the loopholes that they can exploit.

Intrusions by hackers and other organized groups into computer networks, servers, routers, host computer systems, workstations, and desktop personal computers has intensified and reached a level that could jeopardize a company's financial or business operations or a military organizations ability to provide national defense. In addition, attempts to penetrate and invade individual applications and corporate/military databases containing highly sensitive information is on the rise, as is the number of hostile code viruses now being detected.

To combat hackers and organized groups intent on invading computer systems, national, federal, military and civil agencies have created Computer Emergency Response Team (CERT) organizations that respond, report, and assist organizations that have suffered successful intrusions. They also compile, assess, and disseminate system, network, and software vulnerabilities throughout their area of responsibility. Original Equipment Manufacture's (OEM's) have established their own in-house computer/vulnerability assessment teams that also disseminate vulnerabilities and fixes to their customers, and often to the CERTs mentioned above. The attempt to disseminate vulnerabilities and initiate defenses to known vulnerabilities is well intentioned and can work, providing all system/network administrators get the word and have the time and ability to implement the required changes to close the loopholes.

In June 1998, the Assistant Secretary of Defense for Command, Control, Communications and Intelligence (ASD C^3I) decided that a formalized process for disseminating computer vulnerability alerts to the lowest levels was necessary. The ASD C^3I intent was to ensure vulnerabilities were addressed and corrected throughout the Defense Information Infrastructure (DII), and that corrective action at all levels was reported. As a result, the Secretary of Defense established the Information Assurance Vulnerability Alert (IAVA) process as Department of Defense (DoD) policy and announced this process to the field in a message designating the Defense Information Systems Agency (DISA) as the DoD agent for the IAVA process[1]. In response to DoD's new policy, DISA established a process where basically an alert, once issued, would require an acknowledgement receipt within 5 days and reporting of corrective actions back to DISA within 30 days[2]. To date, no similar process exists in the commercial or federal government sectors.

1998 also saw the establishment of the National Infrastructure Protection Center (NIPC), a joint venture between the Department of Justice (DOJ) and the Federal Bureau of Investigation. This organization also disseminates vulnerability alerts.

Much progress has been made at the national level in creating incident and response organizations, such as the NIPC mentioned above. All of these national level organizations disseminate vulnerability alerts not only downward, but also laterally among themselves. This sharing of information is good. However, it often results in duplicate alerts being sent downward to local level system/network administrators.

The Problem

System/network administrators are having a difficult time sorting through the large volume of vulnerability alerts received and deciding if an alert affects them. As such, they have no organized way of managing vulnerability alerts. There are a number of factors causing this dilemma and are outlined below.

- The proliferation of organizations dedicated to disseminating vulnerability alerts has increased.

  The organizations often send their alerts to each other and are then repackaged and sent out to system/network administrators. As a result, the system/network administrators often receive two or more alerts concerning the same vulnerability. A partial list of organizations disseminating vulnerability alerts is shown below:

  - The National Infrastructure Protection Center (NIPC)
  - DISA (DoD CERT)
  - Three DoD Service CERTs (Air Force CERT, Navy CERT, Army CERT)
  - Regional CERTs from each of the DoD components (five or more regions per Service)
  - Carnegie Mellon CERT Coordination Center (CERT/CC)
  - The Department of Energy's Computer Incident Advisory Capability (CIAC) center
  - National Aeronautical and Space Administration (NASA)
  - Federal Computer Incident Response Capability (FedCIRC)
  - OEM's
  - The SANS Institute

- No standardized reporting format or vulnerability naming convention has been established for use by all the organizations disseminating vulnerability alerts.

  Locating pertinent information in any alert becomes time consuming since there is no consistent format that aids the system/network administrator in deciding if the alert applies to the systems he/she is responsible for maintaining. Lack of a standard vulnerability naming convention deters creation of databases to help manage

vulnerability alerts. However, some progress in this area has being made by Mitre Corporation with the creation of their Common Vulnerabilities & Exposures (CVE) database. This database is a list or dictionary that provides common names for publicly known information security vulnerabilities and exposures. Using a common name makes it easier to share data across separate databases and tools that until now were not easily integrated[3].

- The sheer number and increasing frequency of alerts being sent to lower levels is beginning to overwhelm system/network administrators.

  As the numbers and frequency increase, system/network administrators find they need to take time away from their daily duties to address vulnerability alerts. To make matters worse, many alerts received by system/network administrators do not apply to the systems they manage. Often the rigors of daily duties, responding to customers and higher authorities, system failures, and additional duties leaves precious little time to determine if a particular vulnerability pertains to their systems. As such, alerts are not always immediately read or acted upon.

- Many system/network administrators have limited experience and only minimal training.

  They often are responsible for more than one system and not necessarily skilled enough to implement corrective actions. In addition, they often don't understand the impact of the vulnerabilities. Determining which alerts apply to them is often difficult and at times confusing.

We've come a long way in trying to make our first line system/network administrators aware of all the possible vulnerabilities that might affect their systems. However, they are very busy people and unfortunately, responding to alerts is often low on their priority list. So, is there a solution where a system/network administrator can be quickly notified of a vulnerability that affects only the systems they may manage? The answer is yes. However, the security community needs to collectively develop a process that will be responsive to system/network administrator's needs while also providing a mechanism to show management that patches/workarounds have been implemented.

To stimulate discussion within the security community in addressing this problem, I offer a possible solution in figure 1 below. Some of the mechanisms and required software needed in the process diagramed below is either already in use or available for use. Other portions would require some extensive programming to tie the entire process together. Some key elements that would need to be developed in the diagram below are:

- A text database where vulnerability alert messages can be parsed, based upon predefined keywords, and associated data placed into specified fields.

- A topology (network mapping) and configuration management database with associated applications for the databases.
- A database that can store the vulnerability applicable to the system being fixed to include vulnerability alert number, date received, vulnerability, date fix implemented, and name/telephone number of individual implementing the corrective action.

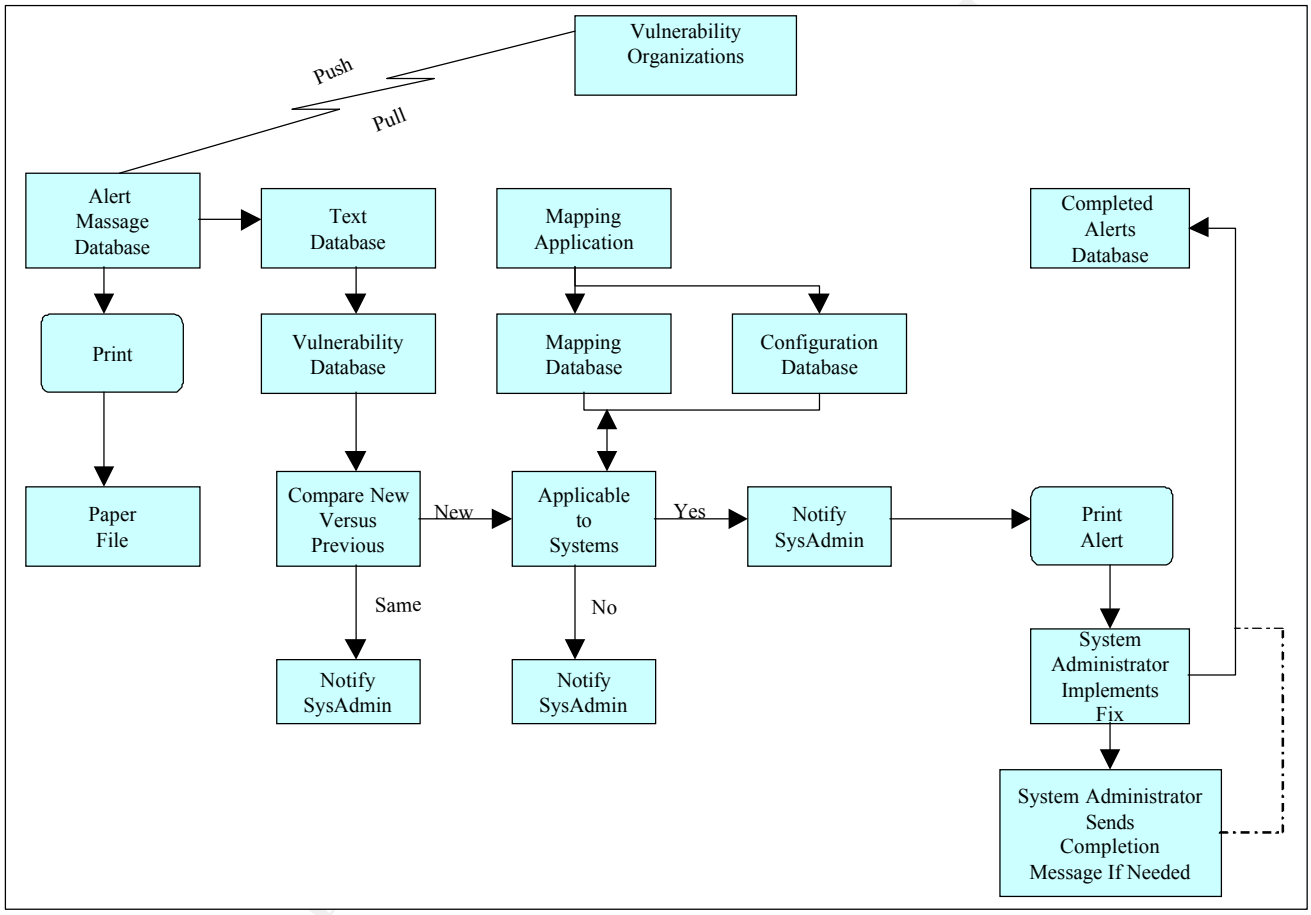

Figure 1

The Envisioned Process

As envisioned, the system/network administrator would obtain the vulnerability alert using the push/pull method. The alert would be placed into an Alert Message Database (AMD) and then printed, so that a hard copy could be filed in an ordinary administrative paper filing system.

The AMD would be input to the Text Messaging Database (TMD), where the message would be parsed and information placed into the appropriate fields. Once parsed, the data would be fed into the Vulnerability Database (VD), which will house all public and government vulnerability information. A simple compare action will then be

accomplished to determine if the new alert already exists in the VD or if it needs to be added. If the vulnerability alert already exists, the system/network administrator will be notified of this fact. If not, the data is then passed to the Applicable Systems Database (ASD).

Once the applicable data is placed into the ASD (represented as Applicable to Systems in the diagram), the Mapping Database (MD) and Configuration Database (CD), produced as output from the Mapping Application (MA), is accessed to determine if the alert applies to any of the existing hardware or software found on the systems controlled by the system/network administrator. Based on this search, the system/network administrator is either notified that the alert does or does not apply to any of the system/network administrators systems. If the alert does not apply, the system/network administrator is notified. If the alert applies, the system/network administrator is notified and provided with a printed copy of the alert.

For any alert that does apply to the system/network administrator's systems, the system administrator will follow the instructions provided in the alert message, obtain any necessary patches, and/or take the necessary actions to implement the fix. Once the vulnerability has been eliminated, the system/network administrator will need to access the Completed Alerts Database (CAD) and enter the necessary information that will include the vulnerability alert number, date received, vulnerability, date fix implemented, and name/telephone number of individual implementing the corrective action.

If the system/network administrator is required to send a message or an e-mail detailing the information that would go into the CAD, a pre-canned message or e-mail template could be designed that would contain the appropriate information in the CAD. The message could be printed out or the e-mail sent on behalf of the system/network administrator. In lieu of entering the information into the CAD, the information provided to the template could be used to automatically update the CAD.

Conclusion

The envisioned processed offered above is not purported to be the only or even best answer available. It is intended to draw attention to the security community that a much better process is needed to alert all segments of our nation regarding vulnerabilities and the necessary methods to correct the vulnerabilities. At the same time, the national level organizations need to know what vulnerabilities have been corrected, and where, so that a more accurate picture can be developed concerning the strength of our computer defenses.

References

1). Secretary of Defense. "Information Assurance Vulnerability Alert Process". 25 June 1998. URL: http://www.cert.mil/iava/r252016z-jun-98%20iava%20policy.txt (6 Oct. 2000).

2). Evans, Beth. "DoD's IAVA Process" Summer 2000. URL:

http://www.cert.mil/iava/dodiava.pdf (6 Oct. 2000).

3). Unknown Author. "CVE, The Key to Information Sharing" 17 August 2000. URL: http://cve.mitre.org/about/introduction.html (6 Oct. 2000).