Critical Security Patch Management for Nuclear Real Time Systems

Dave Hinrichs – Exelon Corporation

Abstract

Until fairly recently, the issue of operating system patch management was relegated to traditional business computers, those on the company's local and wide area networks running a version of Microsoft Windows. The SCADA and real time computers were either on isolated networks, networks with limited access from the company's local and wide area networks, or in some cases just not included because it was too hard. With the advent of recent regulatory requirements and the increased use of Microsoft Windows as the operating system for real time computers, patch management strategies for real time computers is an issue that must be addressed.

Nuclear real time systems are most likely to be engineered-systems in that they are under engineering configuration control. Support from the application vendors is particularly important for these systems so that engineering design concerns can be properly addressed. This paper describes the patch management strategies for Exelon Nuclear real time systems, how the strategies were developed based on regulatory requirements and historical events with the company's real time systems. An example of one application vendor's support for providing this information will also be shown.

Introduction

Exelon has the usual mix of operating systems in our Nuclear and Energy Delivery real time systems. At the time most of these systems were installed, cyber security, security patch management and virus/Trojan threats were not a consideration. The operating systems were setup per the vendor recommendations, and put in production. Reasonable system administration practices were followed to maintain them. Many of these systems were also standalone or air gap systems where access from outside threats or even internal network threats. Additionally most of these real time systems operated using operating systems such as VMS in which hackers had little interest.

The landscape has changed significantly over the past several years. .Microsoft has been successful in making inroads into the process control and industrial market. With their huge market share, Microsoft products are a popular target for attack. Other operating systems, to one degree or another, also get the attention of attackers. As Linux gains in popularity, for instance, the number of vulnerabilities is bound to increase. Security patch management must now be addressed as part of the deployment design, and included in ongoing system administration.

This presentation will focus on security patch management of Exelon's Nuclear real time systems. Corporate and regulatory events will be used to illustrate how the management philosophy evolved. The resulting patch management procedure will be described, and shown how it is implemented and used.

Two terms need to be defined so that their use in this presentation is clear. As used here, an AIR GAP SYSTEM is a computer system with no network ties outside of its defined environment. The security computer system at a nuclear station is an example. While in the business computer environment a distinction is made between a Local Area Network (LAN) and Wide Area Network (WAN), for clarity, the term Wide Area Network (WAN) will be used to describe Exelon's traditional business networks.

History

For purposes of our discussion, we go back to the year 2000. Exelon's Information Security group had completed a review of Exelon's Energy Delivery real time and SCADA systems and indicated that Exelon Nuclear's real time systems should implement some of the same principles. Energy Delivery's systems were either air gap systems on isolated networks. Others had minimal ties to the company WAN, and these tie points were protected by firewalls. Exelon Nuclear real time infrastructure contained various configurations due the different approaches taken by the merged companies. In 2004, an Exelon Nuclear project was initiated to install plant process computer firewalls at all sites to protect the plant process computer and core monitoring systems. Coincident with implementing this project, Nuclear Real Time Support management met with Information Security and obtained their concurrence that the installation of these firewalls alleviated the requirement to apply security patches to systems protected by the new firewalls.

In August of 2005, the W32.Zotob virus and its variants appeared on the Internet. Unfortunately this one made it past the Exelon business Internet firewalls to a limited degree, as occurred at other businesses. In addition to problems with some of the business computers on the WAN, the virus response team flagged some Energy Delivery substation security camera systems as also being affected. The W32.Zotob variants were an ongoing issue with business IT support for several months. Then in October, Energy Delivery IT support identified that a W32.Zotob variant was found on an air gap SCADA system because someone inserted an infected floppy disk. Those of us on the IT Operations call from real time support groups the morning it was announced let out a silent collective groan. The timing of this event could not have been worse. Three days later Energy Delivery announced another of their systems had been infected. The agreement between Nuclear Real Time Support and Exelon Information Security, concerning the PPC firewalls, was about to be null and void.

Developing a security patch management strategy for Nuclear Real Time supported systems

Nuclear Real Time Support and Exelon Information Security reviewed the status of security patch management for nuclear real time systems in light of recent company events, and evolving cyber security regulations. It was agreed that the PPC firewalls no longer alleviated the need to apply security patches to Nuclear real time systems, but it was also recognized that most of these were considered nuclear plant systems under design engineering configuration control. It would not be practical, in every case, to initiate an engineering change to apply each security patch as it came out. In the case of a Microsoft based system, this could be once a month. The Nuclear Simulator IT support group was also looking for an approach to allow deferring security patch application to the downtime between training cycles. What evolved is a policy of evaluating security patches as the vendors release them, and performing a risk rank determination on a per-system basis to decide when to apply the patch. This approach took a defense in depth approach to ensure that patch management was performed on risk and impact based criteria.

Implementing the Security Patch Management Procedure for Nuclear Real Time Systems

The purpose of Exelon Nuclear's security patch management procedure is to establish a standard method to apply critical security patches, emergent and/or hotfixes of all operating system, infrastructure services and application software to IT managed Nuclear Real Time Systems. The methodology though not fool proof consists of identifying the threat, assessing the scope of the threat and the associated security patch, and performing a risk evaluation of deploying/ not deploying the security patch. These steps establish a risk rank that provides the preferred approach for security patch installation.

Nuclear Real Time Support identifies potential threats by subscribing to vendor security threat announcements, by reviewing the various Internet security forums, and participating in the daily IT Operations teleconference.

Once a potential threat has been identified, Nuclear Real Time Support assesses the scope of the threat. This determines which systems are affected, the level of urgency, available vendor support, and what testing options are available. Currently the scope is limited to those systems for which IT provides support. As such this includes plant process computers, core monitoring systems, data historians and security systems.
Once the assessment has been completed, the procedure assists in assigning the threat a risk rank using a matrix that compares the anticipated business disruption to the degree of system vulnerability. The vulnerability includes both the type of operating system and the associated network configuration.

Table 1 Risk Rank Determination

Business Disruption \ Vulnerability	High	Med	Low
High	1	2	3
Med	1	2	2
Low	1	1	1

Vulnerability Examples (Defined by type of O/S as well as level of network security)

High	Windows outside Firewall / located on the business network
Med	Windows behind a Firewall or Unix / VMS – Outside Firewall
Low	Unix, VMS, (older O/S) behind a Firewall or any system with an Air Gap

---

Disruption Examples (Defined by how the user community is affected when patch is applied)

High	Loss of plant production; Resource intensive / limitations; Regulatory requirements. (Would Require Extensive Testing)
Med	Does not constitute a severe or catastrophic loss but does disrupt normal organizational functions (Would Require Functionality Testing)
Low	Will not result in any significant loss in productivity (Would Require Minimum Testing)

Using this ranking method, our nuclear station security computers, which are part of an air gap system, would receive a rank of '**3**'. An OpenVMS-based plant process computer protected by a firewall would receive a rank of '**2**'. A Microsoft Windows-based plant process computer display workstation would receive a rank of '**1**'.

Table 2 Patch Urgency Timeframe Determination

Risk Rank	Patch Urgency
1	Patch As Soon As Practical.
2	Patch on Minor base application, O/S upgrade, or hardware platform upgrade.
3	Patch on Major base application, O/S upgrade, or hardware platform upgrade.

With the risk rank assigned, an implementation plan is developed, using the existing Nuclear Real Time Support work package generation procedures. These procedures develop the necessary testing and installation instructions to update the system. Items that are risk rank two or three are tracked to ensure installation at the future date. Items that are ranked as 1 but cannot be tested or are not recommended are also tracked and an Exception Request is prepared.

Most risk rank 1 items are then given to the Site IT group for deployment. Site IT coordinates with engineering as needed to prepare EC or work order documents. If Site IT or engineering determines to delay installation of a recommended patch, an Exception Request is prepared using Exelon Information Security procedures, and documented in the system notebook.

Limitations and other considerations

Implied in our discussion so far is that we are addressing computer systems under IT control. At the power stations, some computer devices are specified and installed exclusively by Engineering. PLC's, digital feedwater control, and the digital Woodward governor are examples of systems not currently covered by our patch management procedure. As the distinction between PLC's and PC's continues to blur, and the mainstream operating system vendors increase their market share in the embedded system market, more of the traditional engineering-controlled systems will be included in our patch management methodology. Good engineering practice, industry events and regulatory changes will drive us to periodically review our installed systems, and adjust which of them will be included in our patch management procedures.

Looking ahead, we are taking several steps to improve the security of our nuclear real time systems. The focus of our patch management procedure is to apply patches where we can. However the risk rank may cause a deferral, and we need to insure the configuration of our nuclear real time systems and networks provide the best security possible.

We are developing a list of operating system services that should be turned off. In this effort we are building on recommendations currently in place for business computer

systems and will use this in defining future system requirements. In addition, as a result of recent audit, Exelon is working with Scientech to evaluate several services in use at Dresden in hopes of being able to disable them.

We have also recently completed a periodic review of the firewall rule base for each of the PPC firewalls to insure the rules are current and relevant, and made rule changes to address identified weaknesses.

There are also ongoing discussions with engineering about "IT Turf Talk" to better define which systems need EC's and which do not, to facilitate operating system upgrades in the future.

Vendor Support in a security patch management strategy

Support from the software vendors is essential in any security patch management strategy and deserves special consideration. Potential threats are identified by any number of different organizations, but once identified, we rely on the software vendors for technical details and impact. In some cases a test/development system is available to evaluate a potential threat, but the software vendor remains the primary source of information.

Operating system vendors provide varying levels of detail for their patches. HP for example, provides detailed engineering information for patches to the OpenVMS and HPUX operating systems, and associated system software utilities. Microsoft tends to abstract technical details in their documentation, making a test system almost a necessity to provide the level of detail required for a risk rank evaluation. While improving, it is a special challenge to get information on potential threats and patches for Microsoft embedded operating systems. Unlike the Microsoft update website for desktop software, the update website for embedded operating systems requires a username and password, which is given to OEM licensees of the software.

Support from the real time application system vendors is especially important because their software is designed to be customized by the user. For purposes of our patch management methodology, we refer to the base application, and station specific applications built with the tools provided by the application vendor, or tools the vendor has provided software interfaces for. R*Time interfaces to Microsoft Office and MKS Toolkit are examples of support for third party applications. In establishing a risk rank, both the base application and associated station specific applications must be considered. In the case of application support for third party tools, multiple vendors may be involved.

Exelon has recently entered into a maintenance agreement with Scientech to support the various installations across the fleet. In order to provide a reasonable approach, this agreement allows Exelon to determine which patches they are interested in testing, and then having Scientech perform the work on an as needed basis, rather than testing every patch. This approach supports installations that will be based upon engineering priorities, and schedules that have longer timelines than the Microsoft patch schedules.

Software vendors and integrators can help support our risk rank evaluations by verifying patches work on their base systems, building applications using standard tool sets that can be tested, and providing training and information on their web pages regarding the systems and support available. An example of a real time software application vendor who provides this kind of support for security patch management is Invensys, a Microsoft Solution Provider. Invensys provides software tools with their software, rather than interfaces to third party tools. Their PacWest division website clearly states their software has been tested with the Microsoft patches as they come out, providing a hotfix to run to fix any incompatibilities. Technical details are available to customers with a support contract. In addition, the company offers a training seminar which is free to customers with a support contract, and at very modest cost for users without a support contract.

Conclusions

The requirement for security patch management is here it stay. Current efforts try to provide protection and compliance with IT requirements, but still have gaps. Sites need to develop a long-term engineering strategy to move beyond mere compliance, and move to more thorough protection. A collaborative effort with IT, Site Engineering and software vendors and integrators is necessary to ensure system reliability, and maintain business needs in this new world.