LAWRENCE
LIVERMORE
NATIONAL
LABORATORY

LLNL-CONF-674448

Physical Protection Systems and the Cyber Security Component

S. Porter

July 14, 2015

Physical Protection Systems and the Cyber Security Component
Indian Wells, CA, United States
July 12, 2015 through July 17, 2015

Disclaimer

Physical Protection Systems and the Cyber Security Component

Authors: Stephen J. Porter[1], Kenneth Masica [1] (contributor), Jeremiah Porter[2] (contributor)
[1]Lawrence Livermore National Laboratory, Livermore, California, USA, [2]Hewlett-Packard Corporation, Roseville, California, USA

ABSTRACT

Advancements in technology as applied to Physical Protection Systems (PPS) have made them more robust and responsive. However, with these new technologies PPSs are becoming more vulnerable to cyber-attacks. The convergence of IT (Information Technology) and PPSs with respect to design, configuration, and ongoing support has evolved in both industry and government. Nevertheless, these two areas intrinsically continue to be treated separately, especially when it comes to support. With analog components giving way to IP (Internet Protocol) based technologies, vulnerabilities are introduced that can be exploited by both the outside hacker and the informed insider with access. Therefore the cyber component must be considered when designing or upgrading PPSs. If systems are protecting nuclear material or information they should have dedicated non-routable networks. Still, what about attached subsystems, are they connected to the outside world? Are VLANs (Virtual Local Area Networks) utilized, and who manages them? Is the IT staff who maintains the networks also cleared at the same level as those who manage and maintain the PPS, or are they one and the same? What about redundancy? Is configuration management implemented properly? These are some of the many questions that need to be asked. While computer forensics sounds exciting, it is usually too late—you've already had a breach. Due diligence is needed to appropriately address the cyber threat to Physical Protection Systems, especially when those systems protect Nuclear and radiological material and their associated control and accounting systems.

BACKGROUND

Before computers became available to the masses for personal use, and well before server-client relationships were established, Physical Protection Systems configured to protect major assets were made up of dedicated midrange computers, self-contained networks, hubs, terminal servers, dumb terminals, and associated peripherals; while most of the outlying detection and assessment components were still analog devices. Operating systems (OS), such as DECs (Digital Equipment Corporation) VMS (Virtual Memory System) ruled the day, out-of-the-box the OS was secure or locked down, and had to be configured by system managers or administrators to open them up for access.

Then there was a game-changer led by David Cutler who left DEC to join Microsoft, where Windows NT (New Technology) was developed, establishing the server to client (workstation) relationship. Though there were others in industry who contributed to the revolution, most would agree Microsoft brought this new server-client open architecture to industry, government, and the general public at large. This out-of-the-box open Operating System, coupled with the explosion of the internet that now reaches every corner of the globe, has application developers, IT managers, and system engineers scrambling to secure systems from hackers, rogue system and IT managers, or even tech savvy custodians (yes janitors). IP based architecture has permeated the security systems sector as well, including server-client configurations, NVRs (Network Video Recorders), and entire network backbones; while outlying analog alarm components have also given way to digital IP based technologies (e.g. IP cameras). These new technologies have changed the way physical security systems are designed, managed, and maintained.

CONVERGENCE • OPERATIONAL TECHNOLOGY • RESILIENT SYSTEMS

The natural progression of system and network technologies has forced industry as a whole to address the convergence of operations with information technology (IT), which is now commonly referred to as Operational IT or simply Operational Technology (OT). This melding or convergence of these technologies has been occurring by default, well before the OT term was applied. PPS designers and manufacturers are seizing on this concept and marketing their systems as turn-key commercial-off-the-shelf (COTS) systems. Even long-time manufacturers of dedicated network architecture and hardware (e.g. Cisco) have entered the market, as present day PPSs are becoming more about digital 0's and 1's than analog open and closed relay contacts.

These new systems do not fully address the cyber security component of Physical Protection Systems. Though some COTS systems may work for protecting less critical assets in home or industry, they are not entirely suitable for protecting extremely valuable assets where security breaches are unacceptable, such as protecting nuclear material and associated intellectual property. The ever increasing cyber threat to these OT systems and the roles and responsibilities of those who support or use them, has necessitated a paradigm shift toward what is now being referred to as Resilient Systems.

Resilient systems are still evolving toward the goal of thwarting even the most subversive never-before-seen cyber-attacks in real-time versus diagnosing attacks following a breach. Resilient systems consider all elements, such as cognitive psychology, computer science, and control engineering to create systems robust enough to withstand the onslaught of documented and undocumented cyber-attacks. This is an ongoing process that keeps

hardware, software, and technical security engineers working overtime to counter the threat. Most of the systems deployed today are not even close to being there yet, but most would agree they need to get there fast. Once established, these systems need to be sustained by a new management schema and support structure.

SOLUTIONS

Until resiliency can be incorporated into existing Physical Protection Systems, there are things PPS system managers can (and should) do to make their systems more robust and secure in the near term. There are the obvious items, such as password management (including enforcing complex passwords), multifactor authentication, permissions via software ACL's (Access Control Lists), enabling port security on network switches, physical hardening of host computer locations and wiring closets, redundant non-routable dedicated networks, and employing as much encryption as the system can handle, including Suite-B encrypters for transmission of network traffic across unprotected or untrusted network links.

In conjunction with these aforementioned items, PPS engineers with their IT staff should map out all interconnectivities and identify attack paths in the system in order to establish appropriate protections. Existing firewalls should be re-examined and configured to eliminate any vulnerabilities (e.g. turn off unused ports), and if available utilize the firewalls DMZ as applicable (e.g. drop boxes).

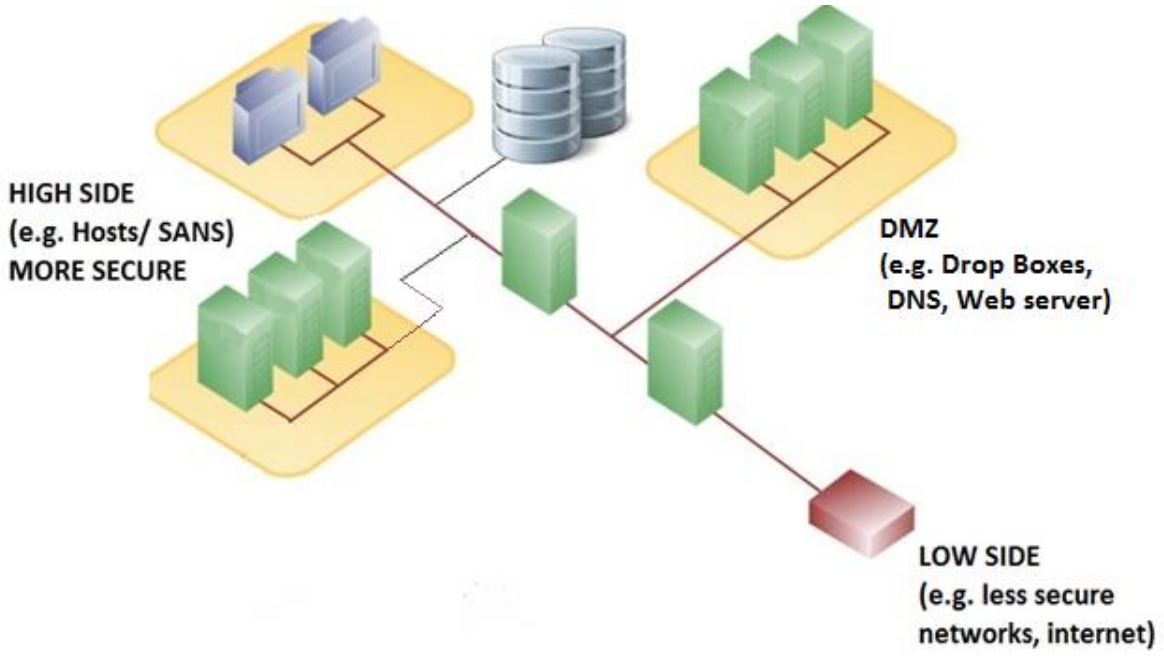

Figure 1. Firewall configured utilizing DMZ

New firewalls should be added where needed and directional high and low side traffic should be configured appropriately. This is especially important where outlying sub-systems have been identified to be not only connected to the secure PPS networks, but also connected to less secure networks (e.g. for access to public domain tools). Of course, the best firewall is the air gap which does not allow any connectivity to the outside world 'by any means.' With that in mind, access to public domain tools if not absolutely necessary should be turned off and sneaker-net should be used instead. Firewalls can also be used to establish security zones where entire secure physical locations are isolated from less secure locations.

Regarding access to systems that protect valuable assets (e.g. nuclear or radiological material), multi-factor authentication is required. There are two components to consider, physical access and software access. Specifically, access control systems (ACS) used for controlling physical access to locations where security systems hardware reside, and login access to the operating system or security applications once physical access is granted. In addition to username, password or pin (something known), several other factors should be employed to gain access to secure systems. Factors, such as something one possesses (e.g. smart card, random generated number tokens), and/or something uniquely inherent to the individual (biometrics), such as fingerprint, IRIS scan, or facial recognition. If tokens are used as one of the factors, the server (e.g. RSA SecurID) should be maintained by authorized security cleared system managers, and protected in a hardened environment at the same security level as the rest of the PPS host systems.

These technologies and those that follow work in conjunction to create a Defense-in-Depth approach, where one technology or application is not solely relied on to mitigate the cyber threat. There is much more that can be said about Defense-in-Depth as it relates to security systems and overall systems in general, but basically it looks at the interactions of people, technology, and operations, while employing multi-faceted technologies and methodologies as described to thwart the cyber threat.

Hackers look for opportunities in the fabric using tools such as Metasploit to find holes or open ports. Network IDS (Intrusion Detection Systems) could be incorporated as part of the Defense-in-Depth approach to counter such intrusions. NIDS are different than physical security intrusion detection systems (IDSs) that Physical Protection Engineers are most familiar with. NIDSs can enforce traffic flows and detect anything out of the ordinary. In-line NIDSs incorporates the blocking capabilities of a firewall, reviews signatures, inspects packets for vulnerabilities, performs packet scrubbing, and scans for unused ports to help thwart cyber-attacks. Network IDSs can assist in identifying behavior indicating a compromised system, bad actors, backdoor RAT (Remote Access Tool) installations, deliveries that could exploit the system, reconnaissance and probing behaviors used to learn about the institutions network,

suspicious communications, and a host of other attack vectors. Custom build packets can also be written to provide information about attacks and malicious activity. NIDSs have become more automated and standalone, whereas in the past IDSs required extra staffing, albeit they still require attention and have their design drawbacks.

Sandboxing is another tool that could provide additional front end security to most existing systems. Similar methodologies on other platforms are also used, such as containers, zones, or jails (UNIX/ Linux world). Though each differs somewhat in their approach, each tool essentially captures untested code or programs from unverified third parties, suppliers, untrusted users, or websites spreading viruses or malignant code. Scratch disk space or memory is set aside for these programs to execute in (virtualization) where they will not interact with or cause harm to the host system. The code is tested and scrutinized within these sandboxes or jails, in order to ascertain its authenticity before allowing it to be released for use. To take the concept a step further, entire Operating Systems could run as a Virtual Machine inside of a sandbox. For example, a Windows OS could run inside of a Linux configured machine, using applications such as VirtualBox, VMware, and others. Primarily this type of configuration was done to isolate OSs during development, but now is being considered as a method to secure entire OSs while in production.

Configuring Honey Pots is another methodology used to combat the cyber threat. Honey Pots as the name implies are used to lure and catch hackers or intruders to learn their methods, then preferably trace the source of such attacks. Like other methodologies this would not be a replacement, but 'in addition to' the previously described tools and configurations, though it would employ some of the same previously described technologies. Honey Pots can be placed anywhere, that is, on the high side, low side, or in the DMZ (reference Figure 1). Some administrators prefer it to be behind the firewall (high side) for security purposes. Honey Pots have many of the same tenants of a standard IDS, but with more of a focus on gathering information and being deceptive while doing it, making it enticing in order to lure the would-be intruder, without giving away the farm.

The move toward more resilient systems combines previously mentioned tools and architectures with even higher level technologies that are now available, such as employing new hybrid firewall switches that can be used to apply policies instead of just using routers that are inherently vulnerable and/or network switches with only port security. Unified threat management (UTM) or unified security management (USM) is another evolution of traditional firewalls, where they are able to combine multiple security functions, such as network firewalling, IDS, gateway antivirus, anti-spam, VPN, filtering, load balancing, data leak prevention, and on-appliance reporting. There is also research being conducted in the area that combines technologies with cognitive science into complex sociotechnical systems that

looks at the functional relations of systems and the integration of the human element. These are just some of the methods and tools in the ever-evolving move to resilient security systems.

Most of the systems and tools described to this point are very robust and applicable to PPSs protecting extremely valuable assets such as nuclear material. For protecting assets that fall below certain thresholds or different categories of material, such as radiological versus nuclear material, many of the same methodologies could be applied. In most cases not of all of the costly improvements mentioned can be instituted due to funding restrictions. Facilities or institutions using radiological material, such as, blood banks, hospitals, or universities most likely will not have the financial resources available to incorporate the same robust systems as those protecting nuclear material. However, every possible measure should be considered, while keeping an eye on more cost effective emerging technologies and solutions. The PPS engineer should also consult the respective standards and criteria documentation for protection requirements regarding certain materials.

Most institutions using radiological sources for medical applications, research, development, or academic purposes also lack the financial resources to install and maintain self-contained dedicated networks for their physical protection systems. When asked about the PPS network's backbone or infrastructure, often security managers or IT staff responds with great pride that they have their own VLANs (Virtual Local Area Network). The VLAN is certainly an improvement as it is segmented 'in a virtual sense' from existing LANs or other VLANs, that support less secure areas or departments within an institution. However, the VLAN is still riding on top of existing architecture (hardware) and is most likely managed by the same general IT staff that supports the less secure institutional networks.

After a lot of time and resources are expended to incorporate new physical protection technologies into existing PPSs, again most still communicate over shared institutional networks (VLAN or otherwise). The reader can already see the fallacy in this false sense of security, as the VLAN can be easily compromised by those supporting it. That is, the management and support of such systems is often left to personnel with limited training and basic security background checks, and/or by an IT staff with no security background checks. In order to address these system vulnerabilities, small standalone redundant systems could be deployed that are designed to be completely separate from the institutions security system and network infrastructure, therefore devoid of the above mentioned pitfalls and vulnerabilities of such institutional systems.

These small redundant systems can be solely dedicated to the protection of radiological targets. Therefore, alarms can be limited to a subset (including radiation detection) protecting just the area or room where the radiological source material is present in a device, or where material is stored. In addition, separate communication paths should be part of the design (e.g. cell

service, satellite, or where possible its own dedicated network). In the event the institution's network is compromised, the redundant system can failover to its alternate communication channel. This redundant system should be placed on the high secure side of the institutions security system, which by default should be mounted close to the target. The redundant system should be monitored by the institutions own dispatch center, but more importantly it also needs to be monitored off-site by either a LLEA (Local Law Enforcement Agency) or remote monitoring service. This redundant system very well may provide the last line of detection should the institutions house security system be rendered inoperable.

COMPUTER FORENSICS

If after all available resources to harden a security system are employed, the system is still compromised by a cyber-attack; the institution will want to ensure it does not occur again. Computer forensics should be used applying the following methodology.

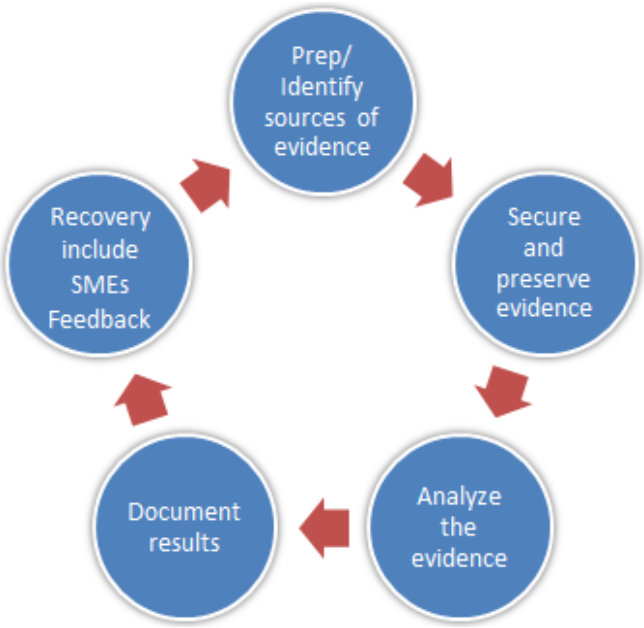

Figure 2 Resolving computer breaches (computer forensics)

Like a coroner performing a post mortem autopsy, preparation should have already been established for securing and examining all media or information once a cyber-attack is detected. The breach should be analyzed and the media preserved (contained), while the evidence is identified, extracted, and documented. The offending malicious code and its various links should be eradicated, while statistics should be performed to identify trends and

patterns. Recovery of the data should also be accomplished. If redundancy was designed into the system (e.g. SANS, DAS) the data could be quickly restored from previous uncompromised snapshots. Well documented assessments or reports may need to be shared with the intelligence community in order to fully understand not only the methodologies of the hacker, but also the source of the attack (terrorist groups, industrial sabotage, foreign governments, etc.). With this approach one could also draw on the research of other entities or SMEs to assist in resolving the cybercrime. Conversely, thorough analyses and reporting the results of the assessment could provide law enforcement and other Subject Matter Experts much needed support.

MANAGEMENT • SUSTAINABILITY

Management and support of the Physical Protection System is as important as the hardening of the systems themselves, to ensure gains made in the battle against the cyber-threat are sustained. Though PPSs have evolved and are increasingly utilizing IP based technologies, including its network, the management and support structure for such complex systems is still fractured. That is, roles and responsibilities for most of the physical security components of the security system (e.g. detectors/ sensors, badge readers, security booths, video surveillance equipment, security application software and computers, etc.) are supported by Physical Protection Experts (PPEs), whom are usually made up of electricians/ technicians; while support for the communication infrastructure (network backbone, switches, routers, firewalls, etc., and the cyber component) are still left up to the IT staff. The two sides usually only communicate when there are connectivity issues, upgrades to the system or network, or recognizable gaps. Most often PPEs do not fully understand the IT functions, while IT staffs typically only look at their systems and network domain and fail to recognize the larger picture of how their actions impact the overall system.

There are so many interdependencies in today's PPSs, it has created the need to move the management and support structure of such systems into what was previously described as Operational Technology. Ideally, the entire physical security system, from the operating system and application software running on a secure server, through the network backbone, to the outlying system workstations and alarm components — would be managed by the same team. Individuals who have knowledge of entire PPS systems are difficult to find. It is even harder to locate individuals who are also steeped in the knowledge of server-client architecture, Active Directory, network infrastructure & protocols, diverse operating systems (MS, Unix, Linux, MacOS), and in some cases legacy operating systems. We haven't even included the cyber security component in that list.

The following items should be applied as a check and balance to help mitigate the divide between IT and PPS management and support, even if individuals with such a broad based knowledge and caliber could be found:

- Security self-assessments of both systems and networks
- Configuration management (keep current)
- Security Plans (review and update periodically, as well as before and after system upgrades)
- Approved equipment lists, including hardware, operating systems, application software, firmware, etc., and associated revision levels
- Map interdependencies between hardware, software, hosts, and subsystems
- End-to-end testing performed jointly before incorporating new code or technologies
- Procedures (kept current) for performing upgrades, including comprehensive checklists
- License management (e.g. some legacy software won't run on new platforms)
- Automated virus scans and patches
- Documentation control (make sure its kept current and secure)

There is much more to be said in the area PPS management and sustainment, but it's in the application of these practices that makes the difference to ensure systems stay compliant, and compliance helps in the overall fight against cyber-attacks.

CONCLUSION

The future is here! Physical Protection Systems are now configured with high tech IP based components and are vulnerable to the same types of cyber-threats that plague other systems. PPS and IT hardware and software developers, integrators, manufacturers, vendors, consultants, and numerous other professionals are addressing the cyber-threat on a continual basis. It is up to the institution and those who install, maintain, and sustain the systems which will ultimately make a difference by taking advantage of leading edge technologies, and managing them appropriately. This is a multi-disciplined challenge and if personnel cannot be found that encompass the various disciplines, all parties from the operational, PPS, and IT sides of the house will need to communicate and work together, in order to mitigate or preferably eliminate systems being compromised.

REFERENCES

1. IT Infrastructure Security, presentation by Stephen J. Porter at the University of Missouri INMM chapter, Columbia, Missouri, 2010

Prepared by LLNL under Contract DE-AC52-07NA27344