November 2012

CleanSweep Mitigation Measures Acceptance Testing

Prepared for:

Mr. Ed Hugler
Deputy Assistant Secretary for Operations
United States Department of Labor
Frances Perkins Building
200 Constitution Avenue
Washington, DC

Prepared by:

S. Maruoka
Red Team Project Lead
Sandia National Laboratories
P.O. Box 5800
Albuquerque, NM 87185-0620

IDART
Information Design Assurance Red Team

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

For additional Information, contact:

H. Lin
Project Manager

National Nuclear Security Administration

Sandia National Laboratories

Table of Contents

Executive Summary

In the interest of improving the security posture of the United States Department of Labor's (DOL) press release facility, leadership at the DOL engaged Sandia National Laboratories Information Assurance Red Team (SNL IDART) to conduct assessments of the facility and associated business processes controlling the release of embargoed data. These activities comprise Project CleanSweep.

The final SNL IDART deliverable for project CleanSweep is technical acceptance testing of measures implemented by DOL to mitigate against issues identified during the initial evaluation assessment. This document reports SNL IDART CleanSweep team member's observations and conclusions from the technical acceptance testing that was conducted during a site visit on October 17-18, 2012 at DOL headquarters in the Frances Perkins Building.

The purpose of this assessment was to evaluate the efficacy of mitigation measures implemented by DOL prior to "going live." A consequence of assessing before going live was that SNL IDART members were unable to assess the effectiveness of processes as implemented under live conditions. In addition, SNL IDART members were unable to conduct penetration testing on the DOL-owned press network, as planned: DOL IT leadership indicated that doing so was not feasible.

DOL addressed the potential threat represented by IT assets owned by the Press residing in the DOL facility by (a) defining requirements for IT assets, (b) introducing acquisition controls, and (c) limiting physical access to such equipment by the Press while onsite. These combined measures enforce configuration management—a foundational element of information assurance policy.

As implemented by DOL IT personnel, the DOL-owned virtual workstation environment enforced least privilege controls by limiting user actions to those acceptable and consistent with the intended use case. However, the apparent trust relationship between the LAN intended for use by the Press and the DOL intranet indicates a serious flaw in design or implementation of network architecture. SNL IDART recommends disconnecting the DOL-owned LAN from the Internet except during press release events to limit attack opportunities from remote threats.

The Department of Labor made significant strides in improving the security posture of the press release facility in the Frances Perkins Building since the initial SNL IDART assessment, while demonstrating flexibility toward resolving the concerns expressed by members of the press who work from this facility. Overall, the results of this SNL IDART assessment were positive. With the exception of the apparent trust relationship between the press room LAN and the DOL intranet, noted above, the Department's implementation of risk mitigation controls were judged to be sufficient defense against identified threats.

Introduction

In the interest of improving the security posture of the United States Department of Labor's (DOL) press release facility, leadership at the DOL engaged Sandia National Laboratories Information Assurance Red Team (SNL IDART) to conduct assessments of the facility and associated business processes controlling the release of embargoed data. These activities comprise Project CleanSweep. For a full description of these activities and resulting recommendations, please refer to *Red Team Report, CleanSweep: Management Overview*, and *Red Team Report, CleanSweep: Technical Details.*

The final SNL IDART deliverable for project CleanSweep is the technical acceptance testing of measures implemented by DOL to mitigate against issues identified during the initial evaluation assessment. This document reports SNL IDART CleanSweep team member's observations from the technical acceptance testing that was conducted during a site visit October 17-18, 2012 at DOL headquarters in the Frances Perkins Building.

Constraints

The purpose of this assessment was to evaluate the efficacy of mitigation measures implemented by DOL prior to "going live." A consequence of testing before going live was that SNL IDART members were unable to assess the effectiveness of processes as implemented under actual conditions. In addition, SNL IDART members were unable to conduct penetration testing on the DOL-owned press network as planned: DOL IT leadership indicated that doing so was not feasible. Onsite assessment of the press room LAN was limited to (a) exploring workstation functionality from a user account with the same permissions available to members of the press (b) conducting interviews with relevant DOL personnel, and (c) inspecting stated physical security controls. No specialized computer exploitation tools were used. As in the original assessment, press-owned IT equipment was visually, not electronically, examined.

Project CleanSweep attracted some attention in the public eye, resulting in the original assessment reports being posted to the DOL website in the interest of greater transparency. This report is written with the expectation of similar public release.

Mitigation Measures

In October 2012, DOL representatives provided SNL IDART with the department's action plan for mitigation measures. This section describes SNL IDART recommendations resulting from the original assessment, the DOL response, and finally the results of acceptance testing for each of these items. An SNL IDART suggestion to deploy a metal detector at the press room entrance was scheduled to occur at a future date, and so does not appear in Table 1 and could not be assessed.

1. **SNL recommendation:** Disallow non-DOL-owned IT equipment and communication lines from the Press Lockup facility or anywhere else on DOL premise.
    - **DOL action:** The Department's policy allows credentialed news organizations to provide their own equipment, though supply-chain safeguards have been put in place that prevent news organization staff from physically handling any of the items. Production desktops are stored in locked boxes on site in the print media lockup facility; news organization staff access is limited to the monitor, mouse, keyboard, and external DVD drive. DOL staff have locked the BIOS on all news organization computers and physically reviewed equipment to ensure no wireless devices are present or active.

      News organization communication lines no longer connect directly to the print media lockup facility. Lines now terminate in a telecommunications vault, and news organization WAN equipment has been moved to a secure location in the DOL data center (where no physical access is granted to news organization staff or contractors).

    - **SNL IDART assessment result:** Visual inspection of press-owned IT assets conformed to DOL assertions regarding supply chain safeguards.[1] Each workstation was secured in a key-locked cabinet which inhibited physical access to computers, except to a mouse, keyboard, monitor, and an external optical drive at each instance.

      Interviews with DOL Operations personnel confirmed assertions concerning initial hardware inspection for wireless capability, as well as activating BIOS password protection[2].

      Further discussion with DOL Operations staff indicated that original, non-DOL-owned communications lines into the press room had been physically severed, and new lines routed from the communications

[1] Uniform manufacturer markings on visible computer components were consistent with vendor shipping documentation presented by DOL.
[2] BIOS passwords have since been de-activated due to impacting press business processes.

demark point to the DOL data center as described. The data center is not accessible to unauthorized personnel.

Inspection of the network communications interrupt mechanisms between the local area networks (LAN) within the press release room and wide area network (WAN) appliances allowing Internet connectivity were assessed by SNL IDART members to be effective and robust. Demonstrations consistently showed that LAN/WAN connectivity was severed as described by DOL IT design architecture documents. This equipment resides in a locked closet within the press release room, with access controlled by DOL personnel.
NOTE: DOL personnel interviewed indicated that leaving both press-owned and DOL-owned LAN/WAN connections open was the default. SNL IDART members suggest that the cutoff to the DOL-owned network remain closed, except during press events, to limit exposure to Internet borne threats. If members of the press are agreeable, the same mitigation could be applied to their Internet connections. If members of the press decide to accept the risk of having their equipment continuously connected, it should be documented.

A member of the SNL IDART assessment team was given an account on one of the DOL-owned diskless workstations. Configuration was as described in DOL architectural documentation and user permissions were consistent with non-administrator settings. Attempts to create new accounts, to escalate privileges to administrator status, to access administrator/security tools/settings, or to access resources other than the home directory were not allowed. As stated in the "Constraints" section of this report, no specialized exploitation tools were used.
NOTE: While using the web browser on the press room workstation, the IDART assessor was able to access what appeared to be the DOL intranet, or internal business network.[3] According to onsite interviews and previous correspondence with DOL IT personnel, the press room LAN is separate from all other DOL IT environments. Web access from a press room workstation to the internal DOL network without additional login requirements (e.g. web portal) indicates an inappropriate trust relationship between these environments and represents a security risk. While DOL advises that this has been resolved, the IDART team is unable to provide validation.
NOTE: A USB flash memory device inserted by an IDART assessor into a press room workstation was recognized as a valid drive by the operating system. SNL IDART assessment team members suggest limiting USB functionality on DOL-owned equipment to the same mouse, keyboard,

[3] As identified by DOL Operations personnel assisting SNL IDART.

external DVD setup as on press-owned workstations. Though the virtualized environment offers mitigation against malware and other hostile applications which may be introduced via removable media such as USB flash drives, removing this vector would further limit options for inadvertent or hostile introduction of such threats. While DOL advises that this has been resolved, the IDART team is unable to provide validation.

2. **SNL recommendation:** Require technically cognizant escorts to accompany non-DOL personnel into wiring closets and communications hubs.
    - **DOL action:** DOL Telecommunication staff control access to the wiring closets and communications hubs and oversee work performed by non-DOL personnel in these locations.
    - **SNL IDART assessment result:** Interviews with DOL Operations personnel indicated that physical access to communications infrastructure requires escort by IT staff. SNL IDART assessors ascertained that the wiring closets and communications hubs pertinent to this report feature physical access controls and are not accessible to unauthorized individuals.

3. **SNL recommendation:** Require non-DOL personnel to surrender personal items prior to entering the press lockup facility. External storage lockers could secure belongings for the duration of press events.
    - **DOL action:** DOL plans to purchase lockers to be installed outside the press lockup facility and is considering installing a magnetometer outside the room itself.
    - **SNL IDART assessment result:** Storage lockers were installed against the wall opposite the entrance door for the press room. Interviews of DOL OPA personnel indicated that the new entry procedure required press to store personal items in these lockers prior to entry. DOL advises that the magnetometer has been installed since the visit; the IDART team is unable to provide validation

4. **Original SNL Black box recommendations:**
    - Seal Black Boxes with tamper resistant/indicating inventory labels and develop and implement policy to monitor labels for tampering.
    - Mount Black Boxes to wall or on raised shelves so that the equipment is within plain view.
    - Limit the number of Black Boxes each press organization may use.
    - **DOL action:** The Black Boxes are now used for phone access only, and reside in locked boxes under each workstation.
    - **SNL IDART assessment result:** Visual inspection indicated that black boxes were stored as stated, and were limited in function to interrupting telephone connectivity when the power was removed.

5. **Original SNL recommendation:** Install RF shielding in the Press Lockup facility.
    - **DOL action:** In August 2012 the Department hired a contractor to install RF shielding in the print media lockup facility.
    - **SNL IDART assessment result:** SNL IDART personnel physically inspected the accessible construction features of the room, verifying the presence of appropriate RF attenuation components. Interview results from cognizant DOL Operations personnel and construction contractor representatives responsible for the installation were consistent with documentation supplied by DOL and technical guidance issued by SNL in previous reporting. Attenuation levels were within expected parameters given the nature of the facility and resources available for implementing mitigation measures.

Conclusion

The Department of Labor made significant strides in improving the security posture of the press release facility in the Frances Perkins Building since the initial SNL IDART assessment, while demonstrating flexibility toward resolving the concerns expressed by members of the press who work from this facility. The Department instituted security measures for onsite IT equipment and data lines while retaining press organizations' ability to conduct their business.

DOL addressed the potential threat represented by outside IT assets residing in their facility by defining requirements for standardized computer and peripheral equipment, introducing supply-chain controls to acquire such equipment, and limiting physical access to this equipment onsite. These combined measures enforce configuration management—a foundational element of information assurance policy.

Members of the IDART assessment team were particularly impressed by the approach taken to control communication lines for its thoroughness. Severing existing lines into the press room and requiring replacement lines be routed via DOL access-controlled facilities removes the potential risk from legacy lines while creating a new accountability baseline for data line management.

The DOL-owned virtual workstation environment implemented least privilege controls, limiting user actions to those acceptable and consistent with the intended use case. However, the apparent trust relationship between this environment intended for use by non-DOL personnel and the DOL intranet indicates a serious design or implementation flaw in network architecture. Disconnecting the DOL-owned LAN from the Internet except during press release events would limit attack opportunities for remote threats.

Requiring visitors to leave personal items in the lockers provided outside the press release room reduces risks associated with transmission devices such as mobile phones, tablets, and other RF transmission appliances which may inadvertently or intentionally transmit information from the press release room during the embargo period.

Replacement of the black box devices with physically and logically secured media converters as Internet cut-off mechanisms is a notable improvement in terms of reliability and attack surface reduction. Limiting Internet/outside connectivity to press release events would further reduce risks associated with Internet-borne threats (e.g. hackers, worms[4]). Limiting the remaining black box devices to telephone cut-off appliances and securing them in locked cabinets addresses security concerns formerly attributed to their use in the original SNL IDART assessment reports.

The application of RF attenuating materials within the press room offers further mitigation against unauthorized data transmission from the press room during release events by diminishing signal propagation from the affected area while simultaneously increasing power consumption for devices attempting to transmit. This should make it easier to detect these devices as they boost signal strength while attempting transmission. Results of signal strength testing fell within expected parameters for the attenuation measures deployed.

Overall, the results of this SNL IDART assessment were positive. With the exception of the apparent trust relationship between the press room LAN and the DOL intranet, the Department's implementation of risk mitigation controls were judged to be sufficient defense against identified threats.

[4] Self-replicating malicious software programs which often use networks as propagation vectors.