Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

An automated system for rapid and secure device sanitization

*Ralph LaBarge**, *Thomas A. Mazzuchi*, *Shahram Sarkani*

Engineering Management and System Engineering, George Washington University, Washington, DC, USA

ARTICLE INFO

Article history:
Received 9 November 2013
Accepted 27 January 2014

Keywords:
Data privacy
Data sanitization
Disk sanitization
NVRAM sanitization
Security and privacy protection

ABSTRACT

Public and private organizations face the challenges of protecting their networks from cyber-attacks, while reducing the amount of time and money spent on Information Technology. Organizations can reduce their expenditures by reusing server, switch and router hardware, but they must use reliable and efficient methods of sanitizing these devices before they can be redeployed. The sanitization process removes proprietary, sensitive or classified data, as well as persistent malware from a device prior to reuse. The Johns Hopkins University Applied Physics Laboratory has developed an automated, rapid, and secure method for sanitizing servers, switches and routers. This sanitization method was implemented and tested on several different types of network devices during the Cyber Measurement & Analysis Center project, which was funded under Phases I and II of the DARPA (2008) National Cyber Range program. The performance of the automated sanitization system was excellent with an order of magnitude reduction in the time required to sanitize servers, routers and switches, and a significant improvement in the effectiveness of the sanitization process through the addition of persistent malware removal.

1. Introduction

This paper presents an architecture, and an implementation, of a system that automatically sanitizes network servers, switches, and routers so that proprietary, sensitive or classified information, and persistent malware, can be rapidly removed prior to device reuse.

The National Institute of Standards and Technology (NIST) defines sanitization as "the general process of removing data from storage media, such that there is reasonable assurance that the data may not be easily retrieved and reconstructed" (Kissel et al., 2006). Similarly the Department of Defense (DOD) National Industrial Security Program Operating Manual (NISPOM) defines sanitization as "the process of removing the data from media before reusing the media in an environment that does not provide an acceptable level of protection for the data that was in the media before sanitizing" (Deutch, 2004). NIST defines four classes of sanitization techniques: *disposal*, *clearing*, *purging*, and *destroying* as shown in Fig. 1. *Disposal* is "the act of discarding media with no other sanitization considerations"; *clearing* is "a level of media sanitization that would protect the confidentiality of information against a robust keyboard attack"; *purging* is "a media sanitization process that protects the confidentiality of information against a laboratory attack"; and *destruction* is "the ultimate form of sanitization". In general, higher levels of sanitization are recommended if a device will be leaving an organization's

* *Corresponding author.*
E-mail addresses: rlabarge@gwmail.gwu.edu, ralph.labarge@jhuapl.edu (R. LaBarge), mazzu@gwmail.gwu.edu (T.A. Mazzuchi), sarkani@gwmail.gwu.edu (S. Sarkani).
0167-4048/$ – see front matter © 2014 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.cose.2014.01.008

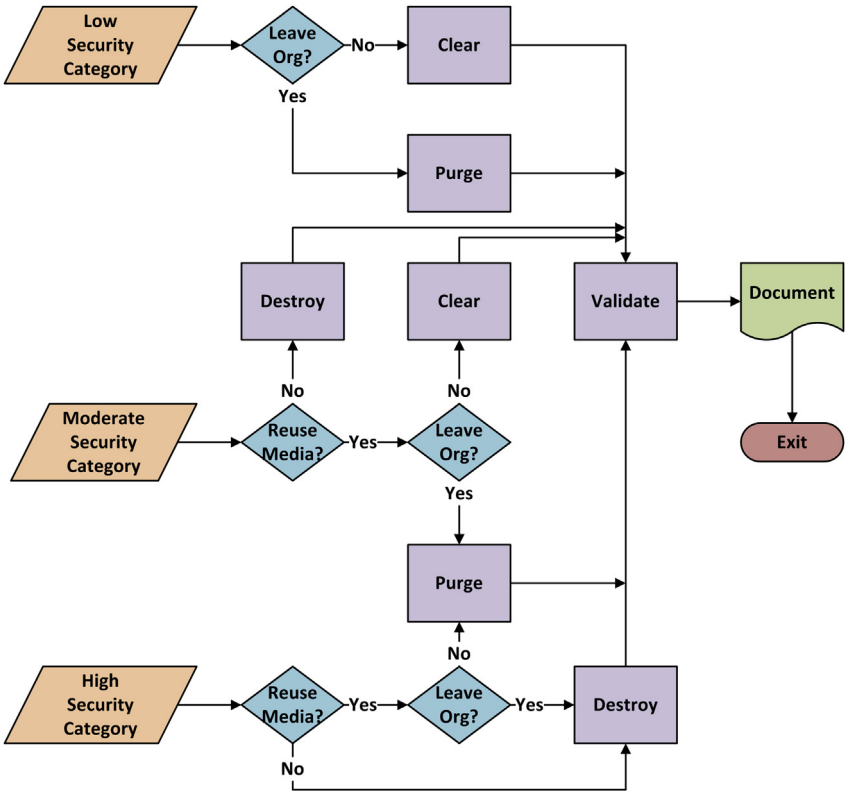

Fig. 1 – NIST sanitization and disposition flow chart.

control. There are several other factors that should be considered before determining which sanitization method is appropriate for a particular type of device. These factors include the cost of sanitizing the device, the amount of time required to sanitize the device, the need to reuse the device after sanitization, and the risks associated with the disclosure of any sensitive, proprietary or classified data that may be stored on the device.

Network servers, switches and routers are complex devices. These devices often contain high capacity hard disk drives capable of storing one TByte or more of data, and flash memory capable of storing many GBytes of data. They also include many different areas of Non-Volatile Random Access Memory (NVRAM) used to store the device's Basic Input/Output System (BIOS) software, hard disk controller firmware, network controller firmware, and other types of firmware. A common characteristic shared by these device components is that the information or firmware they store is persistent, even after the device is rebooted, or power cycled.

There are several reasons for sanitizing a device before it is decommissioned or reused including: (1) to protect sensitive, proprietary or classified data; (2) to remove persistent malware; and (3) to restore a device to a trusted state.

1.1. *Sanitize to protect sensitive, proprietary or classified data*

Several United States laws and regulations require that sensitive, proprietary or classified data stored on electronic devices be properly sanitized if the device is to be reused or decommissioned. These laws include the Health Insurance Portability and Accountability Act, the Sarbanes-Oxley Act, the Fair and Accurate Credit Transactions Act of 2003, and the Health Information Technology for Economic and Clinical Health Act (Hughes et al.,, 2009). Failure to comply with the data protection and sanitization requirements of applicable laws and regulations could lead to civil and/or criminal penalties, damage to an organization's reputation, and the loss of sensitive, proprietary or classified information.

There have been many well documented failures to properly sanitize devices which have resulted in data loss. Improperly sanitized surplus computers sold by the State of Georgia during 2006 resulted in the disclosure of names, credit card numbers, birth dates and social security numbers of many Georgia citizens (Privacy Rights Clearinghouse, 2006). In 2011 Lebanon Internal Medicine Associates disposed of an improperly sanitized network server resulting in the disclosure of 55,000 patient health records (US DHHS, 2011). Device sanitization failures have also occurred at the United States Veterans Administration Medical Center, the Pennsylvania Department of Labor and Industry, Purdue University, and others (Garfinkel and Shelat, 2003).

1.2. *Sanitize to remove persistent malware*

McAfee Labs (2013) recently disclosed they have over 113 million unique samples in their malware database. Many of these malware samples are "rootkits" which are designed to evade detection and persist on an infected computer for an indefinite period of time. Some malware is designed to infect a