EPJ Web of Conferences **214**, 08019 (2019) https://doi.org/10.1051/epjconf/201921408019
CHEP 2018

Increasing Windows security by hardening PC configurations

Pablo Martín Zamora[1,*], *Michal* Kwiatek[1], *Vincent* Nicolas Bippus[1], and *Eneko* Cruz Elejalde[2]

[1]European Organization for Nuclear Research (CERN), Geneva, Switzerland
[2]Universidad de Oviedo, Oviedo, Asturias, Spain

Abstract. Over 8000 Windows PCs are actively used on the CERN site for tasks ranging from controlling the accelerator facilities to processing invoices. PCs are managed through CERN's Computer Management Framework and Group Policies, with configurations deployed based on machine sets and a lot of autonomy left to the end-users. While the generic central configuration works well for the majority of the users, a specific hardened PC configuration is now provided for users who require stronger resilience against external attacks. This paper describes the technical choices and configurations involved and discusses the effectiveness of the hardened PC approach.

1. Introduction

The hardened PCs project began at CERN in November 2016, as a joint effort between the Collaboration, Devices and Applications group and the Computer Security Team. The goal of the project has been to design and deploy a specific hardened configuration to Windows PCs that will provide stronger resilience against external cyber-attacks.

Over the past year and with the help of the departmental technical supporters, CERN has deployed the hardened PC configuration to over 300 computers ranging from administrative sectors and secretariats to public areas around the organization. The reason to begin targeting computers of the administrative personnel (such as Finance officers, Human Resources employees, etc.) is the high exposure to malware they undergo when they perform daily tasks, such as receiving email attachments, especially PDFs and office documents that could contain malicious code or when browsing compromised vendor/partners websites that could put their PC at risk.

Several tools were used to achieve the deployment of CERN's hardened configuration. One of them is CERN's Computer Management Framework (CMF)[[1]], widely used within the organization to manage and deploy application packages, script configurations and security patches; this framework is a web-based application developed in-house that allows central administration of machine sets, e.g.: software installation and removal, software inventory, etc. Another component that facilitates the administration of Windows PCs is System Center Configuration Manager (SCCM) [[2]], used to download and deploy antivirus definitions. Additionally, Group Policies Objects (GPO) are leveraged to deploy global preferences and security configurations.

*Corresponding author: pablo.martin.zamora@cern.ch

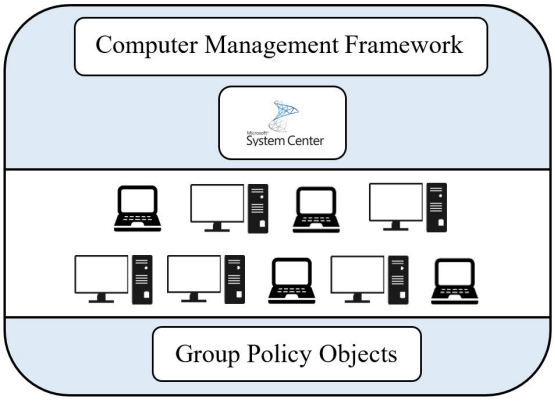

Fig 1. Frameworks to manage PCs at CERN

This paper describes the methods and technical choices used in the design and implementation of the hardened PCs within the CERN IT infrastructure.

2. Hardening features

The approach to harden the target computers included design and implementation of several security layers; we focused the hardening on two main areas: the security of the operating system and addressing widely used office productivity applications such as web browsers, office suites, PDF readers, etc., which are a common target in cybersecurity attacks. Often attackers would exploit vulnerabilities in these applications to get hold of the machine and penetrate further into the organisation's network.

2.1 Hardening the operating system

The main characteristic of the hardened PC configuration is its operating system: Windows 10. This latest version of Windows provides a stronger security foundation over its predecessor Windows 7 [[3], [4]], with security policies and anti-exploit techniques built into the system, making the OS (widely used in the administration sectors) better protected against modern attack techniques.

The preferred method to begin hardening a PC is to install the operating system from scratch using a Windows 10 image with the latest security patches. This is done via network installation, with Computer Management Framework (CMF) [1]configuring the appropriate software and hardened policies for the machine. From the practical point of view, there are two convenient opportunities for provisioning of hardened PCs: when an existing user receives a new PC and when a new employee joins the team and receives a freshly configured hardened PC.

Typically, at CERN, a main user of a centrally managed Windows PC (CERN default configuration) is a member of the Built-in Local Administrator group and hence has local administrator privileges on their PC. The hardened PC configuration aimed to change this behaviour, ensuring that the main user of a hardened PC is never a member of the Built-in Local Administrators group. This ensures that applications do not run with elevated privileges; pursuing the principle of least privilege: users should have only the minimum permissions that are essential to perform their job functions. For users that required

administrator rights on their machines (such as developers, or highly technical staff), a secondary administrator account was provided to enable elevation of user rights.

A common pattern when opening email attachments that contain malware is that the attacker's code runs from the user profile. Therefore, an AppLocker policy was created to prevent the execution of malicious software from this part of the operating system. Microsoft's AppLocker is the natural evolution of Software Restriction Policies, a feature that is built into the operating system since Windows 7 [5]. It consists of a series of rules that allow the execution of programs only from certain paths of the system and deny execution of potentially dangerous files from the user profile, temporary folders and removable storage devices.

```
PS C:\> cMd.eXe /c "PoWerSHEll.exe -execUtIoNpOliCY bYPAsS -nOPROFILE -wInDOWStYLe
HiDDEN (NEw-obJECt SysteM.net.WEbCLIeNt).doWNLOaDfIlE('http://malwaredomain.top/search.php',
'$($env:APPDATA)\romrr.exe'; stArt-pROCesS '$($env:APPDATA)\romrr.exe'";
```

Fig 2. Attempt of payload execution from user profile

```
Start-Process : This command cannot be run due to the error: This program
is blocked by group policy. For more information, contact your system
administrator.
```

Fig 3. AppLocker blocks payload execution

On top of it, we created rules in the Windows Local firewall to lock down PowerShell connections [6] to non-CERN IPs. This configuration blocks any potential PowerShell connection from a malicious program that tries to contact an external entity to download harmful software, a typical attack scenario when a malicious email attachment is opened and the embedded PowerShell code tries to contact an attacker's site to download the main malware program often known as the 'payload'.

```
PS C:\Users\          (New-Object System.Net.Webclient).DownloadFile("http://malwaredomain.top
/search.php","$($env:APPDATA)\romrr.exe");
Exception calling "DownloadFile" with "2" argument(s): "Unable to connect to the remote
server"
At line:1 char:89
+ ... oadFile("http://malwaredomain.top/search.php","$($env:APPDATA)\romrr. ...
+                                                    ~~~~~~~~~~~~
    + CategoryInfo          : NotSpecified: (:) [], MethodInvocationException
    + FullyQualifiedErrorId : WebException
```

Fig 4. PowerShell blocked by Windows Firewall

In line with the trend of controlling PowerShell activity, we decided to enable logs and audits for PowerShell scripting activity in the hardened PCs. For the moment, these logs are stored locally on the machine. The ability to review this data or export it to a log collector will help in the future to analyse patterns of any possible attacks.

Using CERN's Computer Management Framework (CMF), we deployed disk encryption to every hardened PC using Microsoft's BitLocker [7]. This allows users that are travelling with laptops to safeguard their data against attackers who might gain physical access to the computer. This also served as a trigger to expand encryption to other centrally managed computers and MacOS devices.

2.2 Hardening the applications

Once the hardened configuration for the operating system was established, we set to identify and evaluate common administrative applications that could be found in PCs at CERN. The list included several applications that were widely exploited in cyber-attacks such as the existing PDF reader used at the time or the popular usage of Adobe Flash. It was necessary

to harden these applications or to replace them with less vulnerable alternatives that would satisfy the same use cases.

A frequent infection vector is through vulnerabilities found in PDF editor software. To remediate this, an alternative PDF suite, called PDF X-Change Editor, [8] was deployed at CERN; replacing the Adobe Acrobat PDF suite on thousands of computers across the organisation. The number of discovered vulnerabilities for PDF X-Change [9] (one vulnerability) is insignificant compared to the reported numbers for Adobe Reader [10] (878 discovered vulnerabilities) as per CVE statistics. Effectively reducing the surface of attacks in this type of software.

Group Policies for Microsoft Office were tightened to address Word documents, presentations and spreadsheets, which could contain malicious code. This included blocking Macros in Office documents and opening files in 'read mode' when received from the Internet.

As part of the Web browser hardening, it was decided to disable Adobe Flash in all supported browsers, in line with the trend initiated by Adobe to stop supporting the software after 2020 [11].

In addition, AdBlock Plus, an ad-blocker extension [12], was deployed for Chrome and Firefox web browsers.

On top of the Windows Defender, which is the Anti-virus software built into Windows operating system, Malware Bytes [13] Anti-Malware and Anti-Exploit were deployed to offer an additional protection layer by monitoring suspicious activity patterns and Web browser exploits.

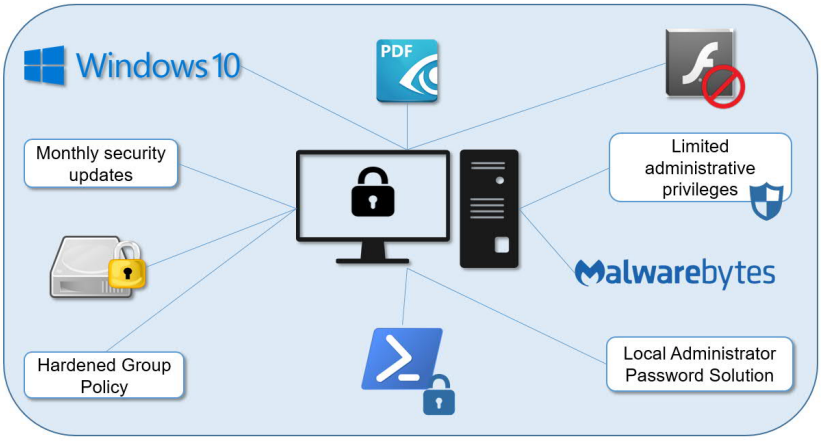

Fig 5. Hardened PC configuration

Users who needed to receive emails from unknown senders as part of their official duties (e.g. reception of invoices) were encouraged to use a separate hardened virtual machine for e-mail and web browsing. The provisioning of this machine is done using CERN Cloud infrastructure, with a Web interface in which the user can select to create a hardened machine in a few minutes. This creates an additional layer of protection for sensitive actions carried out by the same users.

3. Impact

Measuring the effectiveness of the hardening approach is a challenging task. The complexity lies in identifying which parts of the deployed configurations are the most effective. If the main driver is the new Operative System as a whole, or the anti-malware solution or the AppLocker configuration that restricts execution of programs from the user profile. This, added to the lack of meaningful statistics on malware infections in the administrative departments at CERN prior implementing the hardening PCs, makes it difficult to establish exact measurement points. To find out which measures are the most effective against malware infections is useful to further understanding the benefits of deploying this configuration and improving it in the upcoming years.

Before the PC hardening project started, it was reported by departmental supporters that an average of 15 PCs per month were reinstalled in the administrative sector because of malware risks. Considering these reports, after the roll out of the project, these numbers went down to zero reinstallations.

As an approximate indicator of the effectiveness of the configuration, we use the number of machines in which the Antivirus detected something malicious for hardened PCs against the number of machines in which the Antivirus detected something malicious for centrally managed PCs (CERN's default configuration for Windows PCs). As shown by the data collected by System Center Configuration Manager (SCCM) for the Antivirus detections in both categories of PCs, the percentage of hardened PCs in which something was detected as malicious by the Antivirus is almost half than the percentage in which something malicious was detected on a regular CERN PC.

Table 1. Percentage of Antivirus detections on PCs

	Hardened PCs	**Centrally managed PCs**
% PCs with incidents	**3.57%**	**6.37%**

These first findings led us to believe that PC hardening has noticeably reduced the number of PCs where incidents have been detected by Antivirus and is proving to be an effective protection mechanism.

4. Spin offs

Several initiatives have taken place under the umbrella of the project. They either involved the deployment of new tools to the whole organisation as part of a general hardening effort or prompted punctual actions such as security reviews of accesses and permissions or identification of privileged admin accounts.

An example of a successful spin off was the deployment of the Local Administrator Password Management Solution (LAPS) [14], which was installed on all CERN Windows machines, including servers, to ensure that passwords for the Built-in Local Administrator account are frequently changed and randomised.

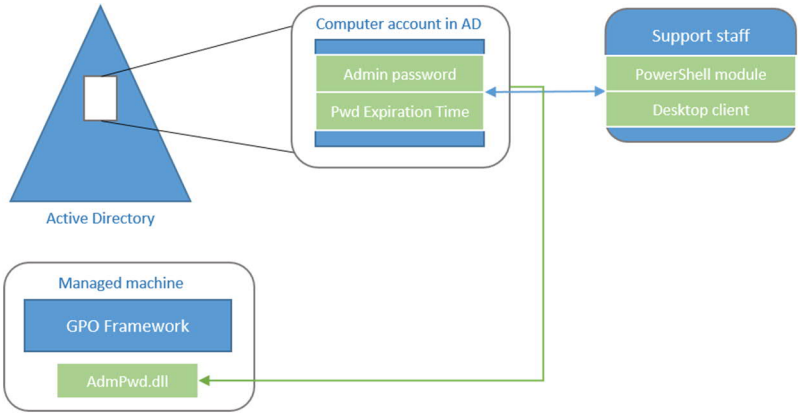

Fig 6. LAPS Architecture

LAPS is driven via Group Policy. It automatically changes the Built-in Local Administrator's password based on a defined schedule and stores it in Active Directory, providing a central place to manage local passwords and their expiration dates. Administrators and users can recover passwords for their machines using a software client or the LAPS PowerShell module. LAPS was integrated into the provisioning process for machines, which are provided with a LAPS-managed randomised password.

High privileged accounts were identified. Their permissions and group memberships were reviewed to ensure that these accounts were used in line with the needs of the infrastructure. As part of this effort, we deployed an administrative bastion terminal server with the purpose of handling connections from supporters and protecting powerful credentials against pass-the-hash attacks.

An interesting ramification of the hardened PCs project is Bloodhound [15], a tool that uses graph theory to reveal the hidden relationships within an Active Directory environment. For context, CERN only trusts Domain Controllers and Bastion Hosts (secure Terminal Servers) enough to enter Domain Admin credentials on them. As an initial experiment, Bloodhound was used to find out on which machines Domain Administrators had sessions open and the experiment revealed many sessions that would have otherwise been ignored. The Bloodhound tool will be used along with logs from Domain Controllers to discover potentially insecure activity.

5. Future steps

The PC hardening project is in constant evolution to leverage the latest security techniques and incorporate new ideas into CERN's PC configurations. With this in mind, new features are introduced periodically into the configuration and the existing solutions evolve.

One of the latest ideas currently on test is to implement PowerShell Constrained Language [16], a PowerShell feature designed to support day-to-day administrative tasks, yet restrict access to sensitive language elements that can be used to invoke arbitrary Windows APIs.

Additionally, the team is piloting the deployment of GRR Rapid Response [17]: a forensics agent that will serve to analyse machines showing signs of suspicious activity and enable quick incident response.

Following a long-term discussion on Web browsers usage at CERN, we are considering proposing Chrome as the default web browser for hardened PCs, while we investigate other browser protections such as Windows Defender Application Guard for Microsoft Edge [18].

This feature will open untrusted sites in an isolated Hyper-V-enabled container, which is separate from the host Operative System.

Another interesting direction of development is to expedite the migration from LanMan authentication protocols towards Kerberos using *RDP Restricted Admin* mode wherever possible. This is being considered because when operating in *Restricted Admin* mode, in an RDP connection scenario, the client will not transmit credentials to the server machine. This is especially useful for supporter/user relationships because user computers may at some point be untrusted.

6. Conclusion

The PC hardening configuration has proved that a centrally managed security configuration works well for users who do not require full administration capabilities on their PCs, allowing users to perform their duties in a more secure environment without affecting their work habits.

The main challenge of the hardening process has been to encourage a disruptive change in the organization's philosophy: from a 'user freedom' paradigm where a user had administrator permissions on its machine to a more 'controlled' approach where regular users don't longer have full control of their PCs and advanced configurations are restricted by design.

The adoption of the project has been very positive and the hardened PC configuration has been established as the standard for new PC installations in departments such as Finance or Human Resources.

The major success of the project lied in the establishment of a breeding ground for security features that have been later adopted by all Windows PCs at CERN, examples of such cases are LAPS or BitLocker. The effort continues to introduce new features and increase the adoption of the configuration to other departments.

References

[1] CERN, *Computer Management Framework*, version 2018. Available from https://cmf.web.cern.ch/cmf/Help/?kbid=001001 [accessed 2019-02-04]

[2] Microsoft, *System Center Configuration Manager,* version 2012 R2 SP1, 2012. Available from https://www.microsoft.com/en-us/cloud-platform/system-center-configuration-manager [accessed 2018-09-18]

[3] Microsoft, *Security features comparison: Windows 7 vs Windows 10*, 2018. Available from http://download.microsoft.com/documents/uk/enterprise/windows10/win10-win7-security-comparison.pdf [accessed 2018-10-05]

[4] Microsoft, *Windows 10 security features*, 2017. Available from https://docs.microsoft.com/en-us/windows/security/threat-protection/overview-of-threat-mitigations-in-windows-10 [accessed 2018-10-05]

[5] Microsoft, *AppLocker,* version Windows 10, 2017. Available from https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/applocker/applocker-overview [accessed 2018-09-18]

[6] SANS ISC, *Blocking PowerShell connections via Windows Firewall*, 2016. Available from https://isc.sans.edu/forums/diary/Blocking+Powershell+Connection+via+Windows+Firewall/21829 [accessed 2018-10-06]

[7] Microsoft, *BitLocker,* version Windows 10, 2017. Available from https://docs.microsoft.com/en-us/windows/security/information-protection/bitlocker/bitlocker-overview [accessed 2018-09-18]
[8] Tracker Software, *PDF X-CHANGE Editor*, 2017. https://www.tracker-software.com/product/pdf-xchange-editor [accessed 2018-10-18]
[9] CVE Details, *PDF X-Change vulnerability statistics* https://www.cvedetails.com/product/23116/Tracker-software-Pdf-xchange.html?vendor_id=12248 [accessed 2019-02-04]
[10] CVE Details, *Adobe Reader vulnerability statistics* https://www.cvedetails.com/product/497/Adobe-Acrobat-Reader.html?vendor_id=53 [accessed 2019-02-04]
[11] Adobe Communications, *Flash Update*, 2017. https://theblog.adobe.com/adobe-flash-update/ [accessed 2018-09-20]
[12] Eyeo GmbH, *Adblock Plus*, 2018. Available from https://github.com/adblockplus [accessed 2018-10-18]
[13] MalwareBytes, *Malwarebytes Endpoint Security*, 2018. Available from https://www.malwarebytes.com/business/endpointsecurity/ [accessed 2018-10-18]
[14] Microsoft, *Local Administration Password Solution*, version 6.2, 2018. Available from https://technet.microsoft.com/en-us/mt227395.aspx [accessed 2018-09-18]
[15] BloodHoundAD, *BloodHound*, version 2.0.4, 2018 Available from https://github.com/BloodHoundAD/BloodHound [accessed 2018-10-18]
[16] Microsoft, *PowerShell Constrained Language*, 2017. Available from https://blogs.msdn.microsoft.com/powershell/2017/11/02/powershell-constrained-language-mode/ [accessed 2018-10-26]
[17] GRR, *GRR Rapid Response*, 2018. Available from https://github.com/google/grr [accessed 2018-10-26]
[18] Microsoft, *Windows Defender Application Guard*, 2018. Available from https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-guard/wd-app-guard-overview [accessed 2018-10-26]