LIA project proposal: Enhancing USB policies

Authors:

Thom Does
Thom.Does@os3.nl

Ruben de Vries
ruben.devries@os3.nl

February 22, 2016
1 Introduction

Infected USB thumb drives are the cause of numerous attacks on IT infrastructures. A study from 2010 shows that 13.5% of all (detected) malware attacks were conducted utilising USB devices [1]. A 2011 experiment run by the U.S. Department of Homeland Security showed that 60% of people who picked up thumb drives or computer disks they surreptitiously dropped in government building and private contractor parking lots plugged the devices into office computers. If the thumb drive or CD case had an official logo, that figure increased to 90% [2].

It has been shown that even sophisticated malware, such as Stuxnet and Flame, relies on USB as the initial entry point to further infect an entire computer network [3, 4]. Stuxnet used this technique to infiltrate the highly secured network of a nuclear power plant facility that was disconnected from the Internet. Moreover, the loss of USB drives has contributed to a considerable amount of (sensitive) data breaches [5, 6, 7].

Current device management policies offer some solutions to these problems: it is possible to (dis)allow all USB devices, certain types of USB devices (e.g. storage devices), or certain USB devices based their properties (e.g. manufacturer, type, product). However, none of them seem to be fully satisfactory for certain use cases, for instance: an organisation wants to only allow a limited set of USB storage devices, authorised to be used by the organisation, which can only be used within the organisation. Such a policy may be used to prevent data leakage and infections within the organisation’s IT infrastructure while still offering the possibility to use USB storage.

In this research, we will discuss the current USB policies and design a new architecture that can be used to enforce such a policy for the use case as described above.

2 Research Question

The main research question can be stated as follows: How can the risk of malware infiltrating by USB thumb drives be minimized in a corporate environment by implementing technical policies?

Answering the following sub-questions will result to the answer of the general research question as stated above:

- What is the current state of USB policies?
- What are the advantages and disadvantages these policies?
- What use cases have been overlooked by these policies?
- How can these policies be improved to minimize the risk of malware infiltrating via USB thumb drives in a corporate environment?
3 Related Work

Pham et al.[8] have analysed vulnerabilities in the default settings of the Windows operating systems which allow malware from attached USB storage to launch attacks on the computer. The solutions and patches provided are ready-to-deploy scripts that can be run by any computer user.

Instead of a technical written piece about portable device security, the article published by Mathie Gorge [9] concentrates on the flow of data that is traveled by PSD’s (Portable Storage Device) in and out of a corporate environment, with accompanying questions like what security measures should be taken and should USB devices be fully banned?

In our research, we will investigate current USB policies. We will analyze these policies and describe the advantages and disadvantages of each one in a variety of use cases. To conclude, we will design a new architecture that can be used to enforce a policy for use cases that have not yet been addressed.

4 Scope

For our research, we will limit the scope to USB storage devices, such as thumb drives. We will investigate current technical policies and provide an overview of the advantages and disadvantages of the possibilities for a variety of use cases. In our research we will mainly focus on Windows Server, since it comes with a variety of USB policies and it commonly used in enterprise environments. However, if we find a significant difference in policies incorporated by Windows Server as apposed to a different platform, we will also take these policies into account.

5 Approach

To answer the first subquestion we will investigate current USB policies offered by Windows Server. After the current state has been determined we will be able to list the advantages and disadvantages of each policy in certain use cases and thereby answering the second subquestion. This will also reveal the shortcomings of all policies in certain use cases which will enable us to describe a new architecture to address these deficiencies.

We will develop this new architecture by creating models of how it should be implemented and which deficiencies it solves. Optionally we will make a prove of concept to demonstrate our models.

6 Ethics

No ethical issues are addressed here since this project will emphasize on theory, without gaining any sensitive data from USB thumb drives or any external storage devices for that matter.
7 Planning

<table>
<thead>
<tr>
<th>Week</th>
<th>Tasks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Week 1</td>
<td>Get acquainted with Windows Server and USB policies</td>
</tr>
<tr>
<td></td>
<td>Determine the current state of USB policies</td>
</tr>
<tr>
<td></td>
<td>Create use cases for different business models</td>
</tr>
<tr>
<td>Week 2</td>
<td>Develop model to address advantages and disadvantages of USB policies</td>
</tr>
<tr>
<td></td>
<td>Determine advantages and disadvantages of USB policies</td>
</tr>
<tr>
<td></td>
<td>Address deficiencies in current USB policies</td>
</tr>
<tr>
<td>Week 3</td>
<td>Develop new architecture which addresses deficiencies</td>
</tr>
<tr>
<td></td>
<td>Optionally, make a PoC for the architecture</td>
</tr>
<tr>
<td>Week 4</td>
<td>Write report</td>
</tr>
</tbody>
</table>

Table 1: Planning

References


