CAUID: Chip Against Unintended Information Disclosure

Sunday 12th May, 2024 - 23:33

Georgi Bozhkov
University of Luxembourg
Email: georgi.bozhkov.001@student.uni.lu

This report has been produced under the supervision of:
Bernard Steenis
University of Luxembourg
Email: bernard.steenis@uni.lu

***Abstract*—As technology continues to develop and become more accessible, becoming a victim of a cyber becomes more and more probable. Advancements in the sphere of cybersecurity are continuously made, but in some instances, that might not be enough, and rather than relying on software that works in conjunction with the internet to prevent malicious attempts at data theft, a more convenient and responsive method could be implemented against security penetration attempts. A computer chip named CAUID collaborates directly with the CPU in order to immediately stop any attacking attempts.**

1. Introduction

The story of antivirus systems goes back to 1971, when Ray Tomlinson, an American computer programmer, developed a program called "Reaper" with the intention of protecting the first wide-scale packet-switched network and the predecessor of the Internet, ARPANET, from a detected virus called "Creeper". Even though the created program was essentially also a virus, made with the goal of finding files corrupted by "Creeper" and erasing them, this could be considered the first concept of an antivirus system. Since that point on, antivirus systems have become a necessity for every device that is connected to the Internet.

A method of penetrating the security system of a computer, more commonly referred to as "hacking", is an act that allows the gaining of personal information without the consent of an individual. Despite numerous advancements made to various security systems throughout the years, people with technological expertise and malicious intent are still able to frequently manage to get past the barrier-like layers and access confidential information. Additionally, it is inevitable for the occurrence of such unethical events to rise due to the globalisation of technology over time.

Due to the aforementioned increase in danger on the Internet, people have been searching for the most reliable and secure antivirus systems for their devices in order to maximise their safety online. The Chip Against Unintended Information Disclosure, or CAUID for short, aims to be a dependable security system that minimally affects the performance of the device while reducing its chances of being compromised by malicious attacks targeting it.

The task of this BSP is to develop and proof the concept of a convenient and responsive antivirus system that does not interfere with the experience of the user but also enhances the security of the device it is implemented on. The task in the scientific deliverable section is to justify the implementation choice of CAUID, which is done by answering the scientific question, "Are hardware-based antivirus systems better than software-based ones?" In order to find an answer to the question, a number of features that the security systems acquire are evaluated based on given and defined criteria. Additionally, a table is created, containing the final results, which are then analyzed and provide assistance with effectively reaching a conclusion.

The goal of the technical deliverable of the BSP is to prove that the concept of a CAUID antivirus system is achievable, which is done in two parts. The first part contains a description of the implementation of the chip. It includes an explanation about all the components CAUID is comprised of and what their purpose is, as well as a comprehensive explanation of its working. For the second part of the proof, a Python program is developed with the intention of simulating how the chip functions under its intended circumstances. Important sections of the code are further interpreted.

2. Project description

2.1. Domains

2.1.1. Scientific. The Domain of this scientific deliverable is centered around the knowledge sphere of cybersecurity. As the goal of the deliverable is to compare two types of antivirus systems, it is essential for this section to provide an elementary level of knowledge regarding their working processes. That includes various algorithms and monitoring methods utilized by them.

2.1.2. Technical . The technical deliverable of the BSP focuses on the hardware components of an ordinary computer. In order for CAUID to work as intended, it needs to be able to operate in conjunction with the CPU. For successful communication process, instructions and data buses are to be utilized

2.2. Targeted Deliverables

2.2.1. Scientific deliverables. The goal of the scientific deliverable is to find an answer to the question "Are hardware-based antivirus systems better than software-based ones?" This is achieved by doing a comprehensive analysis of both types of antivirus systems across various criteria. Afterwards, the comparisons are shown in a structured table format, showing a clear comparison between the two types of antivirus systems. Through an assessment of the results, a conclusion is reached.

2.2.2. Technical deliverables. The goal of the technical deliverable is to justify the existence of CAUID as a concept. This is done by providing a detailed explanation of the structure of CAUID, including its components and working procedures. For clarity, a scheme is applied to visualise the security chip and its connections with the CPU. Additionally, Python language is used to create a program that simulates the working process of CAUID.

3. Pre-requisites

3.1. Scientific pre-requisites

From a scientific standpoint, before beginning with the BSP, a solid understanding of the procedures of an antivirus system is required.

3.2. Technical pre-requisites

From a technical standpoint, before beginning with the BSP, one must have an understanding of how a computer is structured on a physical basis, knowledge about how communication between parts of the computer works, assembly code, and intermediate Python programming skills.

4. Scientific Deliverable

Question: Are hardware-based antivirus systems better than software-based ones?

4.1. Requirements

The goal of this scientific deliverable is to provide a probable answer to the given scientific question, which is to be the result of a detailed theoretical comparison between the hardware-based antivirus (HBA) and software-based (SBA) systems. Before beginning with the comparison, this subsection presents a set of thoroughly defined criteria, which are based on characteristics that outline what an effective antivirus is. The procedure for the juxtaposition between the SBA and HBA systems is as follows:

- **Feature and its Definition:** Antivirus features are algorithms and data recognised by the system to increase the protection of a device against potential threats. The features listed in this comparison are necessary for antivirus systems to be acquainted with in order to establish a secure space against cyberattacks. Before the comparison, a paragraph containing an in-depth definition of each given feature is given with the purpose of showing its importance for the creation of such systems.
- **Comparison between HBA and SBA** With the assistance of the predetermined criteria as well as the detailed definition of the feature, the comparison between HBA and SBA is possible to be carried out correctly. We show the positive and negative traits of both systems and compare their performances in regards to the current feature. As a conclusion, we decide if HBA and SBA are either equivalent in their performance or if one is superior to the other.

4.2. Design

4.2.1. Criteria. In order to justify the results of the comparison between the HBA and SBA systems, it is essential to establish specific criteria for evaluation. These criteria will serve as benchmarks to assess the capabilities of each type of antivirus.

Usability Usability in antivirus systems refers to the ease with which users can interact with and manage the software. It encompasses factors such as installation, configuration, navigation, and user interface design. A highly usable antivirus system is one that is straightforward to install and configure, requiring minimal technical expertise. The user interface should be intuitive, with clear navigation and easily accessible features. Users should be able to understand and utilize the various functionalities of the antivirus software without encountering unnecessary complexity. Additionally, usability includes the availability of comprehensive documentation and user support, ensuring that users can troubleshoot issues and utilize the software effectively. Ultimately, a usable antivirus system enhances the user experience and facilitates the efficient management of security measures.

Performance Performance refers to the utilization of system resources by the antivirus software during operation. It includes the consumption of CPU processing power, memory (RAM), disk input/output (I/O), and network bandwidth. Effective antivirus software should have minimal resource usage to avoid impacting the overall performance of the system. High usage can lead to slowdowns, system freezes, and decreased productivity. Therefore, antivirus solutions are evaluated based on their ability to maintain low resource usage while providing efficient protection against malware threats. Optimized usage ensures that the antivirus software

runs smoothly in the background without significantly affecting the performance of other applications and tasks on the computer.

Effectiveness Effectiveness in antivirus systems refers to the ability of the software to accurately detect and neutralize threats. It should utilize multiple detection methods, including signature-based detection, heuristic analysis, behavior-based detection, and machine learning algorithms, to identify and block malicious files and activities. Additionally, the antivirus should have a low false-positive rate, meaning it should correctly identify legitimate files and applications without flagging them as malware. Moreover, effectiveness also encompasses the speed and responsiveness of the antivirus system in detecting and responding to threats in real-time. A highly effective antivirus system provides timely protection, minimizing the risk of malware infection and ensuring the security of the computer system and its data.

4.2.2. Real-Time Detection. Real-time threat detection allows for the immediate identification and response to malicious activities. Software-based antiviruses continuously monitor system activities and incoming files, comparing them against a database of known malware signatures to detect suspicious behavior. While SBA provide effective real-time protection, their reliance on the operating system can introduce delays in threat detection and response. On the other hand, hardware-based antivirus systems operate independently of the operating system, embedded directly into the CPU architecture. This integration enables HBA to perform real-time threat detection with minimal latency, offering immediate identification and mitigation of threats.

4.2.3. System Resource Consumption. System resource consumption directly impacts the overall performance of the computer system, influencing its effectiveness and usability. SBA systems typically require a significant amount of system resources, including CPU processing power,RAM memory, and disk I/O, especially during scanning operations. This resource consumption can lead to system slowdowns, increased boot times, and reduced performance, particularly on older or less powerful computers. Additionally, frequent updates and background scanning processes further contribute to resource usage, affecting the usability of SBA. In contrast, HBA generally has lower resource consumption compared to its software counterpart because it utilizes dedicated hardware resources for threat detection and mitigation. HBAs have minimal impact on system performance, allowing for smoother operation and an improved user experience, even during intensive tasks or high-demand scenarios. Thus, in terms of system resource consumption, HBA systems outperform SBA systems, providing more efficient protection without compromising system performance.

4.2.4. Resistance to Malware Evasion. Malware creators continuously develop sophisticated techniques to evade detection; therefore, it is important for antivirus software to be able to apply countermeasures as fast as possible. SBA systems primarily rely on signature-based detection and heuristic analysis to identify malware patterns and behaviors. However, these methods can be easily bypassed by encrypted malware variants that alter their code to evade detection. Additionally, rootkit techniques and fileless malware can hide from traditional antivirus scanners by exploiting vulnerabilities in the operating system. In contrast, HBA systems offer enhanced resistance to malware evasion techniques. HBA operate at a lower level of the system, monitoring CPU instructions and system behavior in real-time. This enables them to detect and block malware at the hardware level, making it more difficult for malware to evade detection.

4.2.5. Updating. With the aim of ensuring their reliability, antivirus systems require frequent updates with information about newly developed versions of viruses. In both HBA and SBA, these updates are essential for keeping the antivirus protection current and capable of detecting and neutralizing the latest threats. However, there are differences in their implementation and impact based on these criteria. HBA systems often rely on firmware updates provided by the manufacturer. These updates, while less frequent, are critical for enhancing the system's malware detection capabilities. On the other hand, SBA systems receive regular software updates from the vendor, which are more frequent and seamless but can impact system performance during the update process. Additionally, SBA require internet connection in order for them to be updated. This allows for the creation of files, that could identify as ones needed for updating the software, but are actually malicious. Upon their downloading, they could manipulate and compromise the entire antivirus.

4.2.6. Behaviour-based Detection. Behavior-based detection in antivirus systems involves monitoring the behavior of programs and processes to identify suspicious or malicious activity that may indicate the presence of malware. In SBA systems, behavior-based detection is typically implemented through heuristic analysis and machine learning algorithms. These systems analyze the behavior of programs in real-time, looking for anomalies or patterns indicative of malicious behavior. SBA solutions can quickly adapt to new threats by updating their detection algorithms based on the latest behavioral patterns observed. However, the reliance on software-based algorithms can sometimes lead to false positives or missed detections. HBA systems approach behavior-based detection differently, as they do not recognize software directly but follow sequences of instructions. Instead, HBA solutions focus on monitoring the execution of instructions and detecting deviations from expected behavior at the hardware level.

4.2.7. Scheduled Scanning. Scheduled scanning is a feature in antivirus systems that enables users to set specific times for automatic virus scans. In SBA systems, users can schedule scans to run at designated times, providing convenience and allowing for regular scans without manual intervention. However, scheduled scanning in SBA systems may

impact system performance and usability, as it consumes resources and may slow down other tasks. Conversely, HBA systems do not typically support scheduled scanning due to their real-time monitoring approach lack of software support. HBA continuously monitor system activities, offering immediate threat detection without the need for scheduled scans.

4.2.8. Heuristic Analysis. This approach is used by antivirus systems to detect previously unknown or new malware based on behavioral patterns. In SBA systems, heuristic analysis involves analyzing the behavior of programs and files to identify potential threats based on their attributes and actions. SBA systems use complex algorithms to assess the risk level of files and programs, allowing them to detect and block suspicious activity before it can cause harm. However, heuristic analysis in SBA systems can sometimes lead to false positives or missed detections, as it relies on identifying patterns associated with known malware. On the other hand, HBA systems approach heuristic analysis differently.

4.3. Production

This section contains an assessment on the results from section 4.2. Upon the completion of analysis of the data, a solution to the scientific question is reached.

4.3.1. Creation of a Table. In order to adequately address the scientific question posed in this BSP, a table has been created to summarize the results of the comparison between HBA and SBA systems. This table aims to provide a simplified overview of the capabilities and performance of each type of antivirus system, facilitating a comprehensive analysis to answer the scientific question question.

Features	**HBA**	**SBA**
Real-Time Detection	**Yes** (OS independent)	**Yes** (OS dependant)
System Resource Consumption	**Yes** (Minimal)	**Yes** (Noticeable)
Resistance to Malware Evasion	**Yes** (Strong)	**Yes** (Dependence on Updates)
Updating	**Yes** (Manual)	**Yes** (Automatic)
Behaviour-based Detection	**Yes** (Instruction Monitoring)	**Yes** (Software-based Monitoring)
Scheduled Scanning	**No** (Real-Time Monitoring)	**Yes** (Convenient, Customizable by User)
Heuristic Analysis	**Yes** (Instruction Comparison)	**Yes** (Algorithm Usage)

4.3.2. Result Analysis. As shown in Table 1, HBA systems excel in real-time threat detection due to their integration into the CPU architecture, which enables immediate identification and response to malicious activities. Unlike the software-based antivirus, HBA operates at the hardware level, allowing it to monitor instructions from the processor directly. This deep integration allows the hardware-based systems to detect and block malware in real-time, significantly reducing the window of opportunity for malicious activities. By analyzing CPU instructions, HBA systems can detect anomalies and deviations from expected behavior, making them highly effective in identifying and mitigating threats. Additionally, the hardware-level monitoring provided by HBA systems offers enhanced resistance to malware evasion techniques, such as rootkits and fileless malware. This proactive approach to security makes it more difficult for malware to evade detection, thereby providing a higher level of protection for the system and its users.

One of the strengths shown by HBA systems, as highlighted in Table 1, is their ability to maintain minimal impact on system performance. By utilizing dedicated hardware components for threat detection and mitigation, HBA systems effectively reduce resource consumption compared to their software-based counterparts. This reduction translates into smoother system operation and an overall improved user experience. Furthermore, the integration of HBA systems into the CPU architecture enables them to excel in real-time threat detection and resistance to malware evasion. These hardware-based solutions provide immediate identification and response to malicious activities, making it easier for it to capture malicious attacks.

While HBA systems display superiority in several aspects, including real-time threat detection and malware evasion resistance, they also exhibit limitations. Notably, HBA systems lack certain features such as scheduled scanning and automatic updates. These limitations arise from their real-time monitoring approach and the inherent constraints of their hardware-based design, as indicated in Table 1. Despite these drawbacks, the robust performance and enhanced security offered by HBA systems make them a compelling choice for users seeking advanced protection against malware threats.

In terms of behavior-based detection, Table 1 shows that SBA systems utilize Programs and algorithms to monitor and analyze program behavior in real-time. These systems can quickly adapt to new threats by updating their detection algorithms based on the latest behavioral patterns observed. However, the reliance on software-based algorithms in SBA systems can sometimes lead to false positives or missed detections, especially when dealing with sophisticated malware variants. In contrast, HBA systems, as given in Table 1, follow sequences of CPU instructions and detect deviations from expected behavior at the hardware level. This method of monitoring enables the antivirus system to efficiently detect and respond to suspicious activity without relying on software-based analysis. However, implementing behavior-based detection in hardware can be challenging and may require specialized hardware components, making it less flexible than software-based approaches. Despite these challenges, HBA systems offer robust protection against mal-

ware threats by leveraging real-time hardware monitoring and detection capabilities.

4.3.3. HBA vs SBA. When evaluating HBA and SBA systems, it becomes evident that each approach offers distinct advantages and drawbacks. SBA systems, excel in their flexibility and ease of updates, allowing for seamless integration with existing operating systems and frequent updates to combat emerging threats. However, they also often suffer from higher resource consumption, leading to system slowdowns and reduced performance, particularly on older or less powerful computers. Moreover, their reliance on software-based algorithms for behavior-based detection may result in false positives or missed detections, compromising their effectiveness in detecting sophisticated malware variants.

On the other hand, HBA systems, boast real-time threat detection capabilities and minimal impact on system performance. By integrating directly into the CPU architecture and monitoring system activities at the hardware level, HBA solutions offer immediate identification and response to malicious activities, enhancing overall system security. Additionally, their lower resource consumption ensures more efficient system operation and improved user experience, even during intensive tasks. While HBA systems may lack certain features such as scheduled scanning and automatic updates, their robust protection against malware evasion techniques and efficient behavior-based detection mechanisms outweigh these limitations.

With its real-time threat detection, minimal impact on system performance, and efficient behavior-based detection mechanisms, hardware-based antivirus provides robust security solutions unmatched by software-based alternatives. Given these factors, we can reach a solution to the scientific question that HBA is superior against cyber threats.