Compressing Attack Surface for Advanced Persistent Threats (APT) and Zero Day Vulnerabilities – Innovation Through Hardware Enforced Security Techniques

White Paper By QuikProto Team

TRYAMBAK

Hardware Enforced Security

Introduction

Recent years have been eventful for cyber crimes against high-profile targets, it included major attacks on defense establishments, corporates, social networking sites, movie-streaming giants, music services etc. Conventional security mechanisms are not effective against the advanced form of attacks that are frequently employed against these high value targets. QuikProto's hardware enforced security solutions are designed to counter advanced threats there by filling the gap in defense against emerging cyber-attacks.

Cyber Attacks of Today

Overtime, hacking has shifted its intentions as well as its sophistication. Originally created for thrills to test one's capability to gain access to protected areas, the focus inevitably moved to money and in recent times. The attacks have become even more brutal with state sponsored teams, organized crime rings, targeting defense establishments, critical infrastructures and large corporations. A standout feature of many of these attacks is the complexity of AI embedded malware making conventional security solutions woefully inadequate to detect or prevent them.
Threats that avoid detection and harvest valuable information over a long time are known as Advanced Persistent Threats (APTs). Traditional security measures such as antivirus, firewalls etc. cannot provide protection against APTs thereby leaving systems vulnerable to data breaches. The consequence of an APT attack is devastating as the attack may continue for a long time uninterrupted due to the limitations of most of the current security solutions.

- **State Sponsored Attacks**
  State sponsored espionage incidents are continuing to rise, and these threat actors have objectives aligned with political, commercial, or military interests of their country of origin. One of the most famous of these types of attack is 'Stuxnet' which targets SCADA systems and is believed to have caused substantial damage to Iran's nuclear program. Recently India woke up to the news of a breach in Kundankulam nuclear power plant which is suspected to be the handiwork of Lazarus group from North Korea.
  One of the goals of state sponsored attacks is to remain persistent for months to years by not making noise and they achieve this by having APT capabilities in the malware.

- **Organized Crime Rings**
  Organized crime rings are known to use APTs in the effort to gain personal financial information, intellectual properties etc. from corporates. It is estimated that more than $ 1 B have been stolen from over 100 financial institutions by the Carbanak cyber gang.

Anatomy of APTs

Sophisticated and systematic attacks where the intruder establishes long term presence in the system are called Advanced Persistent Threats (APTs) Security researchers have found that, many of the APTs have kernel mode or even firmware component that shields the malicious code from getting detected there by ensuring that the attack continues uninterrupted. Most of thesecurity solutions of today are not a match against these highly evolved attack vectors.

- **Kernel Mode Rootkit**
  A kernel mode root kit runs at the same privilege level as the OS kernel and hence are hardest to detect and clean. Kernel mode rootkits can manipulate the kernel, memory and other system elements. Primary job of such rootkits is

    - Disable security measures such as antivirus
    - Conceal malware

Rootkits conceal other malware and malicious payloads until the time is right for the attack,that is why rootkits are a preferred tool in stealthy threats like Stuxnet, Turla etc. Often the attacker applies creativity in building the rootkit and then leverages off-the-shelf malwares for rest of the crime. There are also instances where kernel mode rootkits not only hide the presence of malicious user mode components but also leverage the kernel mode privileges to perform sophisticated attacks such as injecting arbitrary code to running processes, directly in the context of kernel. Below are details of how Turla made use of kernel mode privileges to carry out a highly sophisticated attack on Windows.

- **Turla APT**
  Turla is an advanced APT and is suspected to be state sponsored. Some of the key functionality of Turla is implemented as a kernel driver and this allows the malware to bypass the in-built security features in Windows kernel.
  Turla kernel driver is not 'signed' and hence should not be loaded by Windows. The malware authors negate this using a legit signed Virtual Box driver that has a known vulnerability. By exploiting this vulnerability, the driver-signature verification is turned off and malicious kernel driver is loaded. The malicious kernel driver tampers with certain kernel routines there by making PatchGuard ineffective. The modification of kernel routines is possible as the kernel driver is executing at the **same privilege level** as the Windows kernel. The malicious kernel driver then proceeds to hook a number of system calls mainly to **hide/protect** its user-mode components.

- **Firmware and Hardware Attacks**
  Once considered as urban legends, recent changes in threat landscape have proved that firmware and hardware attacks are a reality. UEFI rootkits that once were known to exist as proofs of concepts have been now discovered in the wild, deployed by Sednit group suspected to be targeting government organizations in the Balkans as well as Central and Eastern Europe.

Limitations of Conventional Solutions against APTs

With its kernel mode privileges, APTs such as Turla can hide the user mode malicious components from virus scanners, it also defeats conventional sandbox techniques by disabling any in-host hooking mechanisms. Turla is a classic example of APT that renders conventional security mechanisms completely ineffective.

- **Limitations of Signature Based Detection**
  Conventional security products work by computing the digital signature of each object and comparing the same with a database of known malicious signatures.This is an effective method if the signature exists in the database and the malicious object is visible to the tool for computing the signature for comparison.

  Due to the reliance on known signatures, these technologies will fail to detect zero-day attacks or any malware, signature of which is not present in the database. Malware authors also alter signatures of existing malicious code to avoid detection using techniques such as

  - Code permutation
  - Register renaming
  - Expanding and shrinking code
  - Insertion of garbage code or other constructs

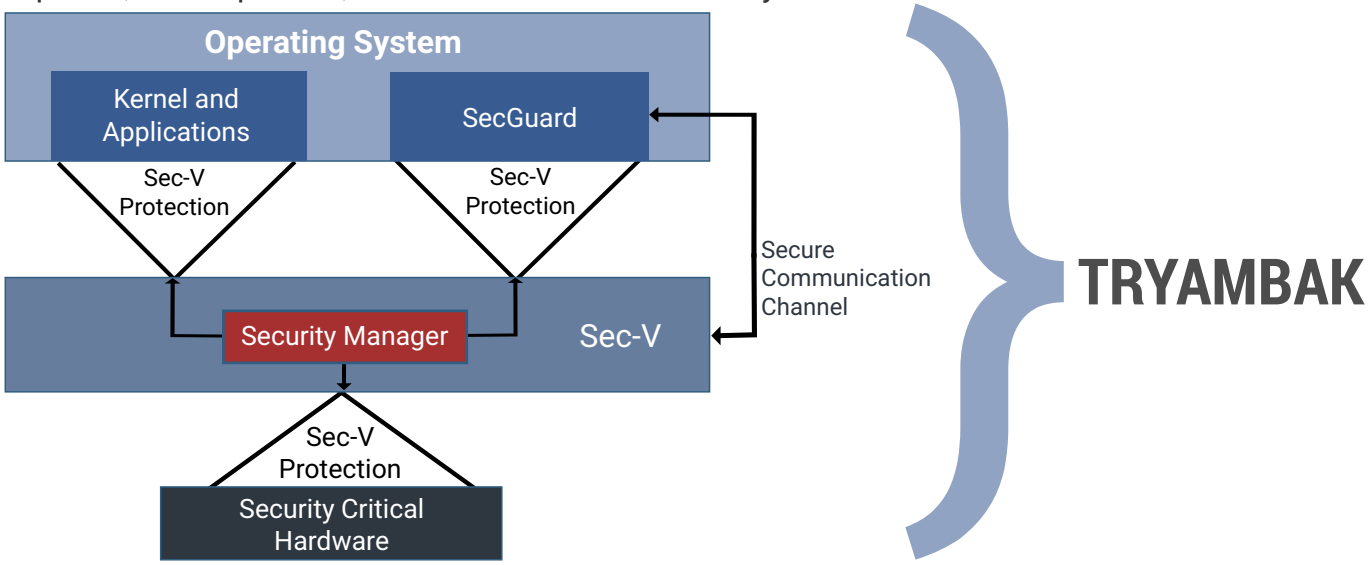
  According to Trend Micro, bad actors create a million new malicious objects every day. Some of these are utterly new threats, but most are variations on existing malware.

Unfortunately, it can be several days after a new malicious object appears in the wild before security vendors update their signatures (although it is not unusual for two weeks to pass before a security vendor makes a signature available). Until the new signature arrives, conventional security controls will not detect the malware and organizations are vulnerable during that time.
Below declarations by Antivirus makers themselves may appear sensational but as far as countering advanced threats are considered it is true.

- **Limitations of Conventional Sandbox Techniques**
  Acknowledging the in-adequacy of signature-based technologies against advanced malwares, security vendors started embracing sandbox technologies. Sandbox techniques rely on behavioral analysis rather than signatures. Sandbox simulates a network environment and hopes to fool the malicious object to demonstrate its true color.
  The sandbox method was once effective, but malware have evolved to evade sandboxes too. Sandbox technologies typically use Virtual Machine environments but the VM environment inserts artifacts that allows advanced malware to discover that it is running in a virtual environment and will lay dormant there by evading detection.

QuikProto's Hardware Enforced Security Solution against APTs

QuikProto's Hardware Enforced Security solution,Tryambak is designed to fill the gap in cyber defense against APTs there by solving the long standing national level security gaps across endpoints, mobile phones, data centers and embedded systems.



The key components in Tryambak

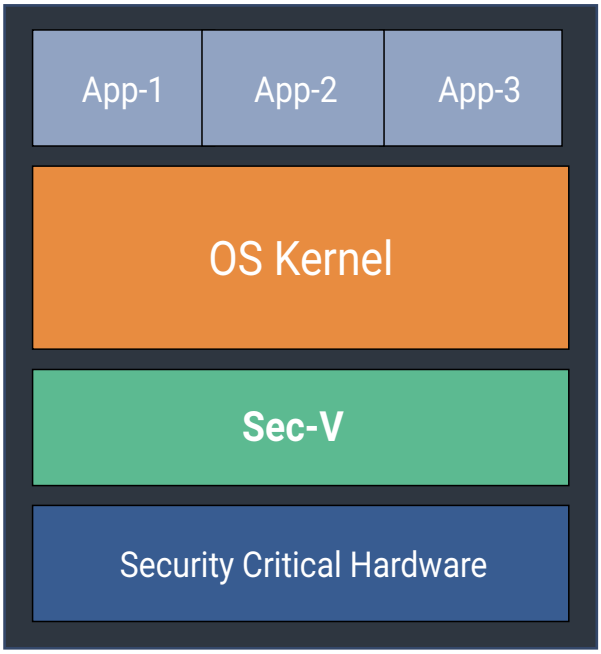
SecGuard

SecGuard is Tryambak's User Interface for alerting, policy configurations, secure update etc. SecGuard will provide RESTful APIs for configuration and management purposes.

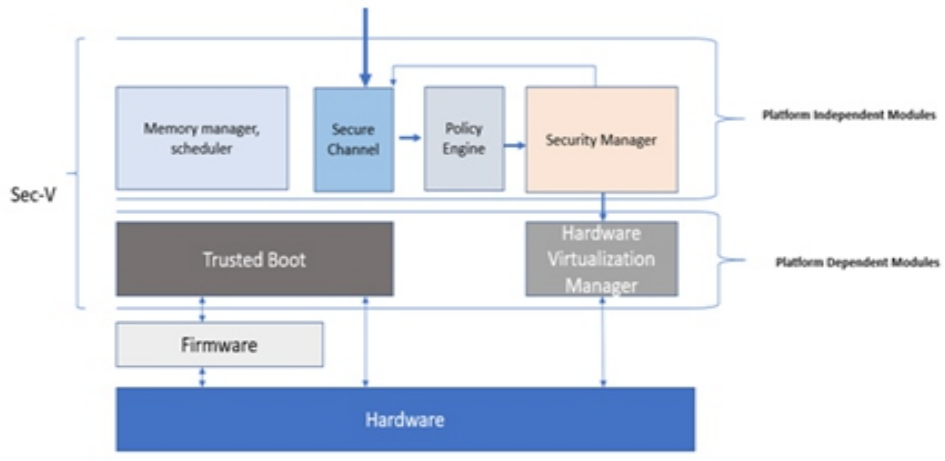
Sec-V the Security Hypervisor

Sec-V is apurpose-built security hypervisor targeted to detect, contain, and analyze kernel mode APTs. The surge in APTs with kernel mode components.

- **Sec-V Design Details**
  Sec-V is a Type 1 hypervisor developed from ground up at QuikProto. Sec-V leverages hardware virtualization capabilities provided by hardware to create necessary isolation and protection against APTs. Secure coding practices have been used during the development of Sec-V.Also, care is taken to ensure that the total footprint of Sec-V makes it amenable to formal verification.
  Sec-V is designed to be easily extended to multiple use cases, apart from the kernel and application protection that is applicable to endpoint devices, mobile devices, and data center entities (servers, white box switches / routers etc.). Sec-V can be tuned to work as a separation kernel as well as malware reverse analysis engine.



During system boot, Sec-V comes up after BIOS and boots the OS to be protected in a virtual machine. This enables sec-V to set desired security policies on the OS and detect malicious actions performed by malware, even the ones with kernel privileges.
Sec-V ensures that the OS under protection does not suffer from any performance issues by leveraging hardware virtualization capabilities and selective virtualization of security critical components. By executing at a privilege level greater than that of the OS kernel, Sec-V is in a unique position to identify attacks from kernel or IO devices.



Hardware Virtualization Manager: Virtualizes security critical kernel and hardware modules.

Memory Manager: Sec-V memory manager

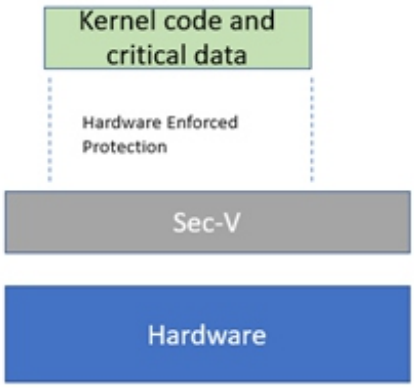
Scheduler: Sec-V VM scheduler

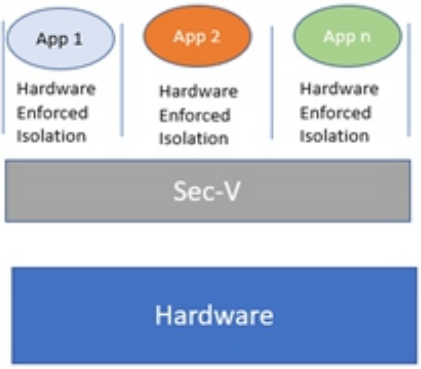
Secure Channel: Trusted communication channel

Policy Engine: Policy handling

Security Manager: Acts on the policies to provide hardware enforced protection.

- **Sec-V for Kernel and Application Protection**
  A key functionality of Sec-V is to provide kernel and application protection by providing the necessary isolation via hardware extensions. The level of protection offered is tunable via SecGuard (User Interface component of Tryambak). As the isolation and protection is via hardware, it prevents malware from breaking out or even go hiding there by enabling users to





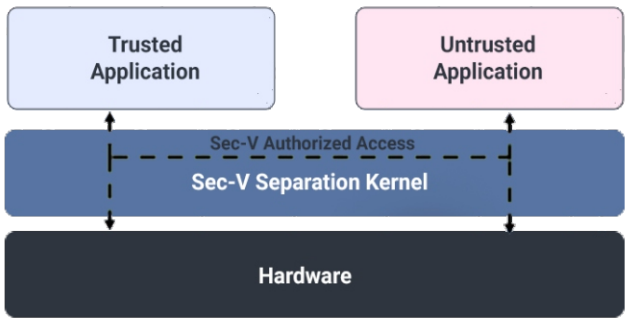
- **Some of the key protections offered by Sec-V are**
  - Prevents malicious kernel code injection
  - Permits only approved code execution in kernel mode
  - Protects tampering of critical kernel data structures and security critical CPU registers.
  - Permits only approved processes from executing
  - Permits only approved user processes from gaining root privileges
  - Prevents malicious applications from accessing unauthorized resources
  - Prevents DMA attacks.

- **Sec-V as a Separation Kernel**
  Sec-V can easily be extended to function as a separation kernel there by providing isolation between multiple VMs and containers. The development framework provided as part of Tryambak security suites would enable developers to build independent secure software

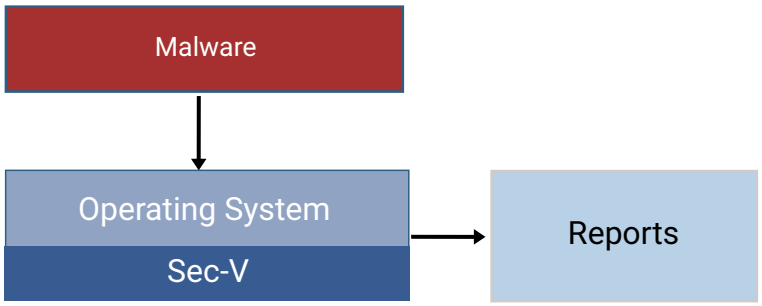
Sec-V Development Framework: Allows developers to build independent secure software components.

Trusted Application: Application developed in-house and known to have no vulnerabilities.

Untrusted Application: 3rd party OS/application that may have vulnerability.



- **Sec-V for Malware Analysis**
  Sec-V malware analysis mode will enable a user to perform deep malware analysis that is beyond the abilities of conventional reverse analysis tools. There will be no artifacts that would warn the malware about the presence of Sec-V. Both static and dynamic analysis are supported and detailed reports of the executed behavior of the sample will be provided.



Malware: Malicious Code.

O.S.: Operating system where malware will be executed under sec-V control.

Reports: Detailed analysis report of the executed behavior of sample.

Conclusion

The constantly evolving AI driven threat landscape created by state sponsored attacks, corporate espionage etc. are becoming a norm rather than exception and the imported security tools themselves are suspected to steal information. Nations have started building advanced indigenous capabilities for cyber defensive and offensive measures. India has not pursued this approach and this oversight has resulted in a strategic gap in the Operating System level security percolating down to the kernel level operations and hardware.

QuikProto, with its deep understanding of kernel, hardware and contemporary security has pioneered a hardware enforced security platform that can be the answer to the gaps in India's national security.