Palitronica

PALISADE

Instant, Active Cyber Protection

OUTPUT
[to PC]
INPUT
[from power adapter]
Instant
Active
Cyber
Protection
Palitronica
Powered by Physics

Powered by Physics

All rights reserved

Executive summary

Securing computers in IT, OT, and PT space is an increasingly difficult task due to these factors: (1) the increased hardware and software complexity complicates enforcing security properties, and (2) the increased level of sophistication of attacks with an increased attack surface causes exponential opportunity to disable existing controls. Ransomware offers direct financial incentives for cybercriminals and motivates them to continue attacking in the foreseeable future.

Palisade offers a revolutionary instant, active, physics-based solution for cybersecurity that monitors the magnetic side-channel emissions of assets under protection (AUPs). With at 1 hour setup time, Palisade can protect any asset that consumes power and provides protection that starts at power-on. Thus, Palisade is suitable for mission- and safety-critical systems, as it is non-intrusive and designed for reliability of 10^{-8} FIT (1 fault in 11,475 years of operation).

The Problem

Ensuring the security of computers and networks, Operational Technology (OT), Platform Technology (PT) is an extremely complex endeavor and has only become worse over the past years. The rapid growth in hardware and software complexity are key contributing factors, making it increasingly challenging to enforce meaningful security properties. Another factor is the increase in the level of sophistication of cyberattacks combined with an ever-increasing attack surface. To make matters worse, ransomware and partially anonymous payment mechanisms started to offer cybercriminals a financial vehicle to monetize cyberattacks. Thus, cyberattacks are here to stay and will continue in the foreseeable future.

Conventional protection mechanisms fall short against today’s advanced threats. The main reason is that conventional protection mechanisms are software-based, running alongside the asset to protect. Once attackers gain control over the asset, they use advanced, automated techniques to disable conventional mechanisms running inside that computer. Traditional mechanisms are helpless against attackers that gained system administrator privileges.

Industrial control systems, medical devices, automotive, aerospace, defense, and critical infrastructure face a similar, even more crucial, challenge. With virtually no exceptions, control and data acquisition systems are computer-based, and financial interests push to connect to the internet. However, most of those systems were not designed with security in mind since they were seen as standalone systems, isolated from the world of attackers and cybercrime. Moreover, adding security to these existing systems is particularly challenging, since (1) often the system as a whole received certification and changes in software will require expensive recertification; and (2) integration of new software may affect the timing or existing operations leading to downtime which incurs unacceptable financial losses.

Palisade

Palisade offers an instant, safe, retrofittable solution based on monitoring the magnetic side-channel that can protect any device, or Asset Under Protection (AUP), that consumes power. By being external and physically independent of the asset being protected, Palisade outperforms alternative protection mechanisms for two main reasons: (1) Palisade is immune to a remote attacker that took control over the asset being protected and thus cannot be disabled; and (2) Palisade cannot disrupt the functionality of the asset being protected — or have any effect at all on the asset, since it is a physically isolated device, having no interaction whatsoever with the internals of the asset. This latter benefit is crucial for safety-critical systems since it makes Palisade a retrofittable solution that can be added to systems subject to stringent qualification and certification requirements.

We highlight that Palisade adds security protection and enhances existing security controls. Computers or networks running software- or network-based intrusion detection systems, antivirus software, or other mechanisms in the same category can have Palisade added to them to provide an additional layer of protection against cyberthreats.

Palisade Basic

Palisade Basic addresses the immediate need to add security controls to existing critical infrastructure and systems. Built to be 100% retrofittable into existing environments, Palisade Basic detects attacks solely through patented side-channel mechanisms completely independent of the AUP. This independence makes Palisade the 100% instant, retrofittable solution, and the easiest to deploy, since Palisade Basic requires no software setup or configuration changes on target systems.

Installation is as straightforward as: plug the Palisade Sensor onto your power circuit, access our web interface, register the hardware and set security policies.

All hardware purchased under Palisade Basic is usable for your Palisade Enterprise setup. If you upgrade, the Palisade Basic hardware will get seamlessly integrated into a Palisade Enterprise setup and provide additional protection for your organization.

Palisade Enterprise

Palisade Enterprise offers the added functionality of correlating logs and telemetry from the AUPs with obtained side-channel information. This additional functionality enhances the intrusion detection capabilities since Palisade verifies a purported ground truth on the fly. As the logs and telemetry are extracted from the protected systems, correlation to the side-channel information corroborates or denies information. Palisade can thus produce intrusion notifications nearly instantaneously as they happen, and Palisade can confirm to third-party tools the validity of existing logs and telemetry information so that they operate on sound data.

Palisade Features

Palisade is ground-breaking, patented technology for the next generation of cybersecurity protection mechanisms in the IT, OT, and PT space. Palisade is cybersecurity powered by physics. Attack attempts will leave significant changes in the power trace of the AUP.

Protection Starts at Power-On

Modern attacks leverage the fact that conventional, software-based protection needs to load and get activated before it can start protecting systems. Rootkits represent a classical type of attack in which assets are compromised before the software-based protection begins to load.

Palisade activates at power-on of the AUP and thus provides instant protection. Rootkits, hardware tampering, and security control tampering at the asset configuration level are scenarios that Palisade covers that conventional software-based solutions cannot detect; additionally, those software solutions are not retrofittable to industrial control systems.

Safely Retrofittable for Unagentable Assets

Many application domains such as ICS include assets that are considered unagentable. Programmable logic controllers execute fixed control logic and cannot host an additional software agent to provide security information to a SIEM. Upgrading critical infrastructure such as an ICS is an all-or-nothing approach that brings a significant existential risk to companies and organizations. Such upgrade projects may require complete shutdowns and typically take longer than planned requiring more budget than initially allocated.

Palisade is physically isolated from the AUP and has been demonstrated safe for even the highest levels of criticality. Palisade operates non-intrusively, connected in series (in-line) with the asset's power supply. This isolation and simple deployment allows operators to deploy Palisade in incremental steps while managing the overall risk for their organization. Moreover, because Palisade does not have any interaction with the internals of the asset, Palisade cannot affect the AUP's functionality in any way. Palisade hardware has been designed to operate with a failure rate of 1 fault in 11,415 years of operation, making Palisade suitable for mission- and safety-critical applications requiring high levels of dependability.

Detect Malicious Intent Before It Becomes Behaviour

Palisade provides the earliest possible comprehensive detection of attacks. Palisade detects misbehaviour of AUPs even if these assets are not communicating on the network. Traditional approaches, especially network-based ones, will see attack behaviour only once attacks spread on the network. At that point, the attack, for example originating from a compromised USB stick sent to an employee, has already established a beachhead in the system and wields destructive power. By monitoring power consumption, Palisade ensures that a compromised AUP is immediately detected upon the AUP deviating from its regular operation.

Integration to Existing SIEM/SOAR

Palisade transparently integrates into deployed Security Information Event Management (SIEM) and Security Operations and Response (SOAR) solutions. Palisade can send alerts in different formats commonly supported by SIEM/SOAR solutions. This integration allows security staff and center operators to build additional abstractions on top of Palisade's alerts in existing infrastructure. Furthermore, they can leverage the data confidence scores provided by Palisade's log and telemetry falsification analysis.

Enhances and Enriches Existing Security Controls

A part of any tactic, techniques, and procedures (TTP) for cyberattacks is to falsify log and telemetry information to avoid detection or to disallow forensic analysis. Attackers successfully use this technique to hide from global cybersecurity controls such as network-intrusion detection and SIEM solutions operating on aggregated logs. The fundamental problem is that existing solutions blindly trust data to be correct.

Palisade offers an unprecedented capability against log and telemetry falsification by providing confidence scores on logs and telemetry delivered to higher-order, global cybersecurity controls. Since Palisade is an external and physically independent system to the AUP, Palisade can provide a guaranteed-truthful account of the asset's activity. Palisade uses its information to report confidence scores on logs and telemetry information reported to other security controls. These security controls can then react when Palisade detects cleaned up and injected log information as well as tampered telemetry.

Use Cases

The following are some of the important use cases where Palisade's unique capabilities can provide effective cyber protection or other benefits.

Ransomware Protection

Ransomware attacks have reached a volume in the hundreds of millions per year, with ransom demands in the tens of millions of dollars for high-profile cases. Conventional security approaches have failed.

Palisade offers unprecedented detection capabilities against ransomware when installed on multiple assets across the organization. Palisade detects characteristic behaviour of spreading crypto-ransomware across an organization and can safeguard critical assets. Analogous to seismic sensor detecting earthquakes, Palisade instantly detects spreading crypto-ransomware by monitoring assets in an organization. In general, Palisade delivers low-volume, high-impact information to security operations centers.

Dedicated, Accredited Insider Attack Protection

A significant portion of attacks originates from a dedicated, accredited insider. If this insider has a significant level of authority, conventional security controls are entirely futile. The insider attacker can assume control over protection software or the whole network domain. However, the insider cannot control the physical domain no matter what.

Palisade monitors the physical domain of AUPs which is outside of the control of even the insider attacker. Palisade collects side-channel data and uses precise signatures as well as machine learning to assess the state of the AUP. An insider attacker would have to make the AUP mimic its normal operational behavior on the physical domain and at the same time execute the attack. This is orders of magnitude more complex than disabling software; and by some even considered impossible for a large-scale, fast-acting attack.

Hardware or Configuration Tampering Protection

Conventional software-based approaches assume that the underlying hardware and its configuration can be trusted as they inspect the asset from within. Sophisticated attacks, however, can capitalize on this assumption and render themselves undetectable.

Since Palisade operates independently and externally to the AUP, Palisade does not make assumptions about the AUP's integrity and thus can detect sophisticated attacks against hardware and system configurations. Attacks such as BIOS/UEFI rootkits, enabling of compromised hardware or its features are instantaneously detectable by Palisade's precise signature-based approach.

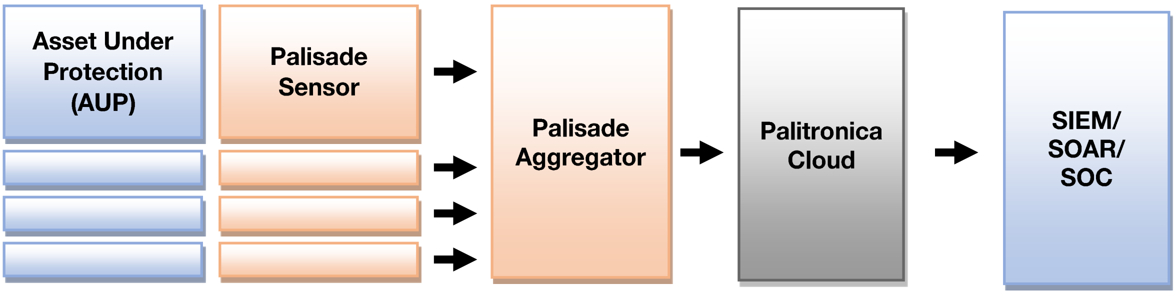
Confirming Operations

Using side-channel information, Palisade can independently confirm operations of the AUP and report on these actions to an auditing system. Because Pasliade uses side-channel information, the reported information can be trusted.

The set of confirmable operations depends on the type of the AUP and includes, among other items, reboots, operational readiness, firmware updates, security status, and action completion. For instance, Palisade can confirm a periodic maintenance reboot at 2am, followed by a successful boot process. So every day in the morning the security staff can receive a daily report on the operational readiness of the AUPs.

Deploying Palisade

Palisade consists of three elements: Palisade Sensors, the Palisade Aggregator, and a cloud component. In Palisade Enterprise, an organization deploys Palisade Sensors and the Palisade Aggregator in their infrastructure. Palisade Sensors monitor key assets that warrant protection. These assets come Assets Under Protection (AUPs), and may include cyber essential computers, industrial control systems, communication/compute/data appliances, or other mission-critical electronics. Palisade Sensors collect side-channel data from AUPs and forward the information to the Palisade Aggregator within the organization. The Aggregator receives data from multiple sensors, performs filtering analysis, and forwards only relevant data to the cloud for deep analysis. In the cloud, Palitronica uses sophisticated, proprietary detection algorithms to analyze the data. If the algorithms detect attacks or suspicious activity, they will notify the organization's security team through a method of choice.



Palisade Sensors need to be placed in series with the power supply (e.g., the wall adapter) for the AUP. Palisade Sensors support a wide variety of power connectors to be daisy-chained into the power supply of the asset. Palisade Sensors receive their own power via a power-over-ethernet (PoE) connection to ensure that the original power remains unaffected. The Palisade Aggregator is a security-hardened appliance (or virtual machine) that manages the deployed Palisade Sensors and provides a secure connection to the Palitronica Cloud. Palitronica's cloud performs the heavy lifting on critical data. If it identifies an alert, it will issue alerts based on the configuration preferences of the client; e.g., forward alerts to SIEM/SOAR solutions or send alerts to a security operations center.

For the Palisade Enterprise, the Palisade also requires access to telemetry and log information from the AUPs. Palisade can read out this information from existing log aggregators, SIEM/SOAR solutions, or from the AUP directly. With telemetry and log information, Palisade will correlate that information to the power consumption to identify attacks and to confirm actions.

Core Technology

Palisade employs proprietary, patented side-channel analysis, digital signal processing and data analysis technologies to verify the operation and enforce security properties of AUPs. Side channels are involuntary, non-functional characteristics of devices during their operation. Side channels include, among others, execution time, power consumption, magnetic field, electromagnetic radiation, and sound. Since side channels are the involuntary result of functional operations within a device, any change to the integrity of the device or its operation, whether it is due to software/firmware or hardware tampering, alters the device's observable side-channel emissions. Figure 1 below shows an example of the side-channel emissions for different hardware configurations. Dotted lines denote the 99% confidence interval for traces measured with normal configuration.

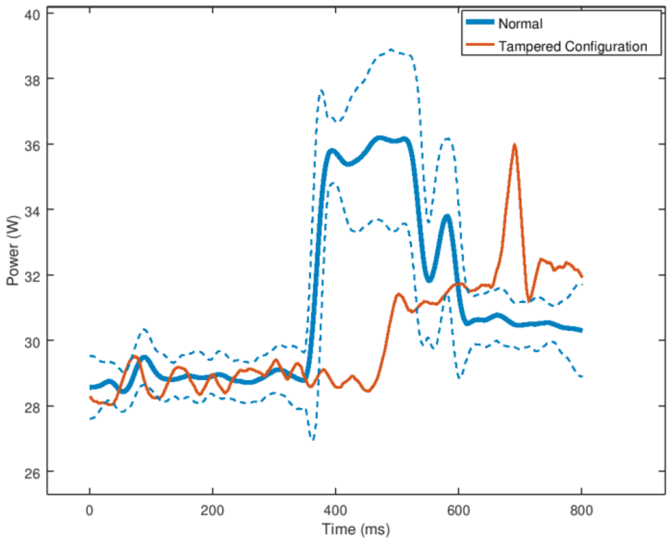


Figure 1. Power traces during boot for different hardware configurations

Palisade applies leading-edge digital signal processing on side-channel data, and novel pattern matching and machine-learning algorithms with in-house hardware sensors to verify device integrity. To counter Palisade's verification procedure, attackers must perfectly mimic the AUP's side-channel emission after making malicious modifications. Given the involuntary and uncontrollable nature of side channels, making changes to the hardware or firmware of a given device and correctly replicating its unique signature is orders of magnitude more complex than bypassing traditional detection measures.

Data and Security

Palisade uses side-channel information collected from the AUP. Extended detection functions use log and telemetry information to correlate to side-channel information. Log entries are anonymized, so it is impossible to pin behaviour to individual users.

Palisade provides all functionality without collecting network traffic and without access to any business information on the AUP. This ability implies that Palisade is ready for Zero Trust Security where data is always encrypted end-to-end.

Reliability of Palisade

For the resistor version of the sensor board, there is only one relevant scenario where the AUP's operation is disrupted due to a failure in the sensor board. This is the case of the resistor failing open; in particular, since two resistors are in series, the failure rate is twice that of each resistor. This is the case because both resistors are of the same type, and are subject to the same temperature at all times.

Our calculation for its failure rate follows Section 11.3 of the IEC TR-62380, one of the industry standards, and recommended, e.g., by ISO-26262 for FMEDA purposes.

As indicated in IEC TR-62380 for fixed, high-dissipation film resistors, 100% of the resistor failures are "fail open". The failure rate, λ, is determined as follows:

$$\lambda = 0.4 \times \left(\left(\frac{\sum_i (\pi_{t_i} \times \tau_i)}{\tau_{on} + \tau_{off}} \right) + 1.4 \times 10^{-3} \times \left(\sum_i \pi_{n_i} \times (\Delta T_i)^{0.68} \right) \right)$$

where the factors π_t depend on temperature, and τ are the duty cycle for each temperature values, and the factors π_n depend on the number of temperature cycles with a temperature swing ΔT.

The units are Failures In Time (FIT), defined as number of failures per 10^9 hours of operation; or, in the context of a failure rate, the units would be 10^{-9} failures per hour of operation.

For a conservative estimate, we assume unrealistically heavy loads: for temperature, we assume 50% of the time at 25°C and 50% at 50°C (this is intended for usage in a controlled environment, typically with air conditioning; thus, these values correspond to a much more demanding workload than that expected to occur in practice).

Following the formulas in Section 11.3 of the IEC document, for 25°C, the factor π_t = 0.91, and for 50°C, the factor π_t = 1.43. The τ values are both 0.5 (assumed 50% of the time at each temperature), and $\tau_{on} + \tau_{off} = 1$ (assumed continuous operation).

For the temperature variations, we assume 10 thermal cycles per day, with a temperature swing of 50°C. Notice that although this is incompatible with the temperature assumptions, this is a much heavier workload that we assume for the purpose of obtaining a conservative estimate of the failure rate.

Following the formula in Section 11.3 of the IEC document, $\pi_n = (3650)^{0.76}$ = 509.7; $\Delta T^{0.68} = 50^{0.68}$ = 14.3. The failure rate for each resistor is:

λ = 0.4 (1.16 + 1.4 × 10^{-3}× 509.7 × 14.3) FIT = 4.54 FIT

For the two resistors in series, this results in 9.1 FIT, or approximately one failure on average in 10^8 hours (more than 11,415 years) of operation.

Why Palisade Is Revolutionary

The evolution of cyber threats in recent years suggests that in the foreseeable future, attacks will become more widespread and critical while being more sophisticated and nearly impossible to counter with conventional cybersecurity measures. Operators of networks of computers/workstations as well as operators of computers controlling critical infrastructure will face increasing pressure to incorporate effective protection against cyber threats, for which conventional techniques will fall short.

Palisade is revolutionary: unlike conventional cybersecurity technologies, Palisade uses emissions that are guaranteed by the Laws of Semiconductor Physics to provide a truthful representation of a device's operation. These side-channel emissions form the basis for assessing the integrity of the AUP. Like a polygraph using a person's physiological parameters to validate the person's statements, Palisade uses a device's side-channel information to validate behavior, logs, and telemetry information to confirm the device's proper operation.

To learn more about how your organization can deploy Palisade to protect your infrastructure and operations, contact us at sales@palitronica.com for a demonstration.