IBM Systems Lab Services

AIX Malware Prevention

with AIX Trusted Execution

Overview

AIX Trusted Execution is a security tool native to the AIX Operating System. AIX Trusted Execution is designed to protect and validate the integrity of the operating system. AIX Trusted Execution provides a powerful countermeasure against ransomware and all types of malware. This consulting service is designed to provide knowledge transfer and step-by-step configuration assistance with AIX Trusted Execution. This service is a proof-of-concept service. The major features of AIX Trusted Execution are listed below:

Trusted Signature Database

The Trusted Signature Database (TSD) is a flat file installed by the AIX operating system. The TSD lists all the files that are trusted by AIX. Every file registered to the database is considered a ”trusted file”. Each file registered specifies a stanza of expected file attributes. This database is a core component used by AIX Trusted Execution’s runtime integrity verification functionality and system audit functionality.

Digital Signatures

AIX Trusted Execution uses RSA digital signatures to validate the integrity of trusted files. A digital signature is a cryptographic value that can be used to verify the authenticity of a file. Files registered in the TSD with a signature can be cryptographically verified for their authenticity by AIX Trusted Execution. This capability detects alteration of IBM published files by an attacker.

Allowlisting

Allowlisting is a security best practice for reducing cybersecurity risk by detecting or preventing execution of unauthorized software. In the context of AIX Trusted Execution, allowlisting is the process of registering AIX authorized executable files to the TSD. When a file is executed that is not registered to the TSD, AIX Trusted Execution can either detect or prevent execution of the unauthorized executable file.

Runtime Integrity Verification

The runtime integrity verification of AIX Trusted Execution provides automatic integrity checking performed by the AIX kernel. Numerous runtime policy configurations are possible that provide a range of detection and prevention capabilities. Provides such things as: reporting of unknown scripts being executed, mandating files to be installed in specific directories for execution, preventing the execution of a file when not consistent with its TSD stanza definition.

System Audit

The system audit function of AIX Trusted Execution verifies the correctness of all files, approximately 4000, registered to the TSD. The system audit function is typically run at the command-line or configured in a crontab job. The system audit function detects such things as improper file permissions, ownership, or cryptographic failures that could correspond to modification of files by an attacker.

Complement to Traditional Malware Prevention

Since AIX Trusted Execution does not maintain a database of known malware, it is best complemented with the use of a traditional endpoint malware prevention and detection solution. This combination is recommended by many existing security control frameworks, such as the CIS Critical Security Controls.

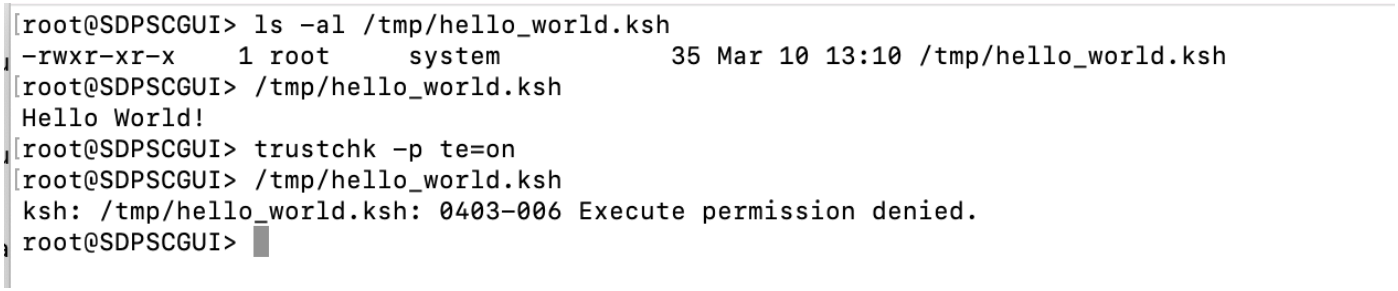

Fig. 1 – The example above shows how AIX Trusted Execution can prevent the execution of an unauthorized script that normally would be executable by any user on the system.

Common Use Cases

- An organization that would like to mitigate the risk of ransomware or other malware impacting their organization
- An organization that would like a guided deep introduction to AIX Trusted Execution
- An organization that would like to fulfill regulatory requirements that mandate allowlisting
- An organization that would like to add a File Integrity Monitoring solution for their AIX systems
- An AIX administrative team that would like a tool to verify AIX files have proper file permissions and ownership
- An organization that would like a malware prevention tool that can be centrally managed by the PowerSC Graphical User Interface server
- An organization that would like to adopt a malware prevention solution that can be configured in a monitoring-only mode

Engagement Process

- Consultant arranges prep call to discuss requirements, scheduling, and agenda
- Consultant works with client to configure AIX Trusted Execution in client environment
- Consultant provides advice on best practice implementation
- Consultant works with client to verify the AIX Trusted Execution functions that are most important to the client
- Consultant provides presentations to facilitate knowledge transfer concerning the numerous capabilities of AIX Trusted Execution

Deliverables

1. Presentation Slides – an electronic copy of presentation slides
2. Configuration documents – an electronic copy of configuration documents
3. Automation script –designed to assist automation of AIX Trusted Execution's runtime-mode configuration