Description of the technology:

Any end point system is a critical component of a computer based information system that not only facilitates the execution of an application, but is also responsible for enforcement of a security policy with respect to that system. An end point system is architected across various logical layers like hardware layer, OS layer, and application layer. Each layer is susceptible to vulnerabilities and by exploiting these vulnerabilities, integrity of the system can be compromised. In these various layers, OS layer is the most critical because OS compromise can lead to compromise of other resources related to it, and would ultimately lead to compromise of the security policy. The compromised state of the OS can be reached not only through adversarial actions, but also due to accidental mis-configurations or apparently benign user actions.

A pragmatic strategy adopted by SEE to achieve run-time protection that drastically reduces the attack surface, and thereby minimizes the possibility of security policy violations, is the segregation of Data Plane from Control and Management Plane; and provide robust protection to the control and management plane from potentially malicious data plane which could be poisoned by the adversary.

SEE, apart from being a hardened and robust platform, is a collection of security enablers that can be leveraged in a system or operational context to establish a security posture, based on strong protection mechanisms. These security enablers can be combined in various combinations, depending upon the requirements of the system and the usage.

SEE is a POSIX {Portable Operating System Interface [for UNIX]) compliant OS, and is capable of hosting any POSIX compliant application. Many applications have already been ported as part of evaluating this compatibility.

Application scenarios/areas

1. *Computer has no classified info, and is connected to networks like Internet:*Here the primary policy to be enforced is that there should not be any infiltration of malware or exfilteration of classified data due to usage of removable media. SEE can be used for Internet facing machines to enforce organizational policies for Internet access.
2. *Computer is used (or creating/processing classified information:*Here the primary

policy relates to network access, media access, user access and logs for forensic analysis. SEE can be used to compose such systems, inclusive of providing necessary productivity applications.

3. *Computer handles classified information, and needs to integrate with a crypto device for transfer (online or through media):*In this context, the SEE provides the capabilities of serial II, and the necessary protocol interface to crypto devices.
4. *Computer handles a critical application, whose integrity needs to be preserved at run-time to ensure desired security properties of the data:*SEE enables a bare-metal integration of POSIX compliant Unix/Linux applications. Such bare metal applications inherit the properties of SEE.
5. *Computers that are connected to military information systems:*Here SEE can be used to enforce the security policy as defined by armed forces for military information systems.

USP

1. Native support for Linux applications (for 64 bit Intel architecture)
2. Support for virtual machines running any flavor of guest OS (Intel architecture)
3. Supports mainstream computer hardware while preserving the security properties