trustifier

Highlights

- KSE™ Servers provably secure access to sensitive data and limit that access to authorized users
- KSE™ Servers ensure that users can only use the data and information for organization's intended purposes.
- KSE™ Servers can create and maintain boundaries to protect against abuse during and after the access to sensitive data
- Powered by Trustifier KSE™ authorization engine that enforces business rules in real-time, Privatize Servers can meet and exceed regulation mandates and compliances
- Trustifier KSE™ powered Servers stop rogue staffers and spies, including evil system-administrators from abusing access to your sensitive environments.
- Trustifier KSE™ cloud server provides complete private-cloud world for all your systems.
- Trustifier KSE™ Detect and stop malicious activities, including collusion, using Decider™ fuzzy human behavior monitoring system.

Trustifier KSE™

Scalable COTS MLS

Authors

Ahmed Masud <ahmed.masud@trustifier.com>

***Abstract**: This document responds directly to Lt. Gen. Charles E. Croom Jr., USAF, Director of DISA:*

> "From the technical standpoint, multilevel security is one capability that is definitely needed…"
>
> "We've wanted multilevel security for 20 years… they [industry] have some solutions, but none of them is scalable across the huge global network."

In particular this paper addresses the question of scalability and MLS as a COTS solution for COTS operating environments.
The paper also discusses KSE capabilities that apply directly to deploying and managing Multi-level Security in a large-scale networked environment.

Document Version: 2.0
Document ID: TBA

Previous date of publication: 2011-04-27

Background

Lt. Gen. Charles E. Croom Jr., USAF, Director of DISA, stated USDoD MLS requirements in the following terms:

> "From the technical standpoint, multilevel security is one capability that is definitely needed…"

Rationale: Multi-Level Security (MLS) is needed to ensure that sensitive or classified information is only accessible on need-to-know basis to cleared personnel, irrespective of channel (covert or overt) used to access the classified information.

He continues:

> "We've wanted multilevel security for 20 years…they [industry] have some solutions, but none of them is scalable across the huge global network."

Rationale: Original systems that delivered MLS capabilities were isolated or centralized systems with physically limited access and only a handful of identified channels. In the world of Intranets, Extranets and Internet, it is impossible to use existing MLS design and implementation approach to achieve desired level of control and security.

Trustifier KSE™ Security Software System

Trustifier KSE is a drop-in security enabler that is designed to address and solve the problems of delivering MLS in highly networked heterogeneous environments such as the Global Information Grid (GIG).

KSE provides the desired Auditing, Role-Based Access Controls (RBAC), Labeled Security (LS) and Protected Execution (PX) facilities for maintaining classified information in a very unique way. KSE security facilities design and implementation make using it in large environments natural and easy.

KSE™ Capabilities

KSE's capabilities make it a unique and powerful Trusted Computing platform implementation. Hereunder are some of its salient capabilities and the rationale behind them:

Capability I: Complete operating system-level security

KSE provides all of its security functions right at the operating system level to ensure that all applications, processes, users and resources become subject to its security.

Rationale: System-level security ensures that security is not limited to a handful of specified applications. Security can be provided across the board.

Capability II: Common off-the-shelf (COTS) systems integration

KSE integrates with normal COTS systems like Microsoft Windows, Linux, and UNIX etc. to provide its security capabilities.

Rationale: Modern network environments are built with COTS systems. The need to deliver MLS in existing infrastructure is imperative because a requirement to replace the entire infrastructure is unreasonable and is prohibitively costly.

Capability III: User centric and role centric security

Trustifier KSE security is defined in terms of users, groups and roles. This makes security simple and intuitive.

Elaboration: Consider the problem of trying to stop a particular user (bob) from using a feature (say setuid). It is simple and intuitive to use a directive like "deny bob setuid" instead of the cumbersome process of adding access control list entries for each object that uses setuid feature, and then have a deny rule for each object. Even "managed" items such as adding and removing bob into a feature capable group is tedious and makes it difficult to trace bob's access grants.

Rationale: It is normal to think of security limitations in terms of people and roles. Direct use of a user-centric security directive (without translations) provides simple and intuitive auditing, visibility, manageability and traceability.

Capability IV: Automatic Labeling of information

KSE is able to classify aggregate and resultant information automatically and provides functionality to automatically label new information based on users and groups.

Rationale: Manual labeling and classification of any significant amount of information can be prohibitive. Without help, ensuring proper labeling and classification can create security risks. KSE provides **user-centric, role-centric and group-centric labeling mechanisms** *that deliver MLS without the overhead of classic MLS.*

Capability V: No outward changes to system and system concepts

KSE is designed such that it can secure systems without the need to change their libraries, applications or services. It uses existing system concepts (user id's, group id's etc.) to enforce its security, rather than introducing something new or alien.

Rationale: By using existing concepts to enforce security, KSE is able to enforce its security across a variety of environments and across the network, as most COTS systems share a lot of these concepts.

Capability VI: Real-time and embedded application capable

KSE is has a small footprint in the computer system, and to run with predictable latency. For example, KSE's core is approximately 256 kilobytes on Intel® x86 64-bit platforms.

Rationale: KSE should not burden the systems it protects. Real-time use makes it suitable for large ad-hoc network deployments. Embedded applications capability allows KSE to be deployed on devices other than generic systems.

KSE Management

KSE's tools, API and integration capabilities enable administration and management on actual systems, through a centrally controlled environment, or a combination of both.

KSE can be integrated with existing identity management and authentication tools to deliver RBAC and MLS capability across very large networks.

KSE provides protection templates and tools to help create protection profiles for large number of users (10,000 or more).

Conclusion

Trustifier KSE is a unique security system that addresses the core need of delivering MLS on highly networked environments, and yet is a COTS solution. KSE has these capabilities because its design and implementation simple, intuitive and robust.

References

[1] Peter A. Loscocco, Stephen D. Smalley, Patrick A. Muckelbauer, Ruth C. Taylor, S. Jeff Turner, and John F. Farrell of NSA in The Inevitability of Failure: The Flawed Assumption of Security in Modern Computing Environments.

(See: http://www.nsa.gov/selinux/papers/inevitability.pdf)

[2] National Security Agency (NSA). Global Information Grid Vision enabled by Information Assurance. (See http://www.nsa.gov/ia/industry/gig.cfm)

[3] National Security Agency Information Assurance Guidance for Systems based on Security Real-time Operating System

(See http://www.nsa.gov/ia/government/IA_Guidance/SSE-100-1.pdf)

© Copyright Trustifier Inc. 2013

Trustifier Inc.
113 Barksdale Business Center
Newark, DE. 19711
U.S.A.

Produced in United States of America
July 2013
All rights reserved.

Trustifier, Trustifier Logo, and trustifier.com are trademarks of Trustifier Inc. in United States, other countries or both. If these and other Trustifier trademarks are marked on their first occurrence in this information with a trademark symbol (® or ™), these symbols indicate U.S. registered or common law trademarks owned by Trustifier at the time this information was published. Such trademarks may also be registered in other counties.

Other company, product service names may be trademarks or service marks of others.

References in this publication to Trustifier products and services do not imply that Trustifier intends to make them available in all countries in which Trustifier operates.

Product data has been reviewed for accuracy as of the date of initial publication. Product data is subject to change without notice. Any statements regarding Trustifier's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

The customer is responsible for ensuring compliance with legal requirements. It is the customer's sole responsibility to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulatory requirements that may affect the customer's business and any actions the customer may need to take to comply with such laws. Trustifier Inc. does not provide legal advice or represent or warrant that its services or products will ensure that the customer is in compliance with any law or regulation.

Please Recycle