Labeled IPsec

draft-jml-ipsec-ikev1-security-context-00.txt

draft-jml-ipsec-ikev2-security-context-00.txt

Presented by: Joy Latten

Document authors: Serge Hallyn,

Trent Jaeger, Joy Latten,

and George Wilson

Problem Description

Mandatory Access Control Systems

- Subjects and objects are labeled with a security context.

  Security context is composed of a set of security attributes defined by the MAC implementation.

Traditionally, MAC implied Multilevel Security (MLS).

- The security context is a security level, consisting of a sensitivity and a set of categories. i.e. topsecret, secret, confidential.

MAC systems have become more mainstream and evolving out of MLS niche.

- Security contexts composed of security attributes besides the security level.

  Linux - SELinux , SMACK

  FreeBSD - SEBD

Problem Description

Windows Vista - Mandatory Integrity Control

MAC on network communications

- IPSO allowed addition of MLS security context to IP header.

  Packet's data not protected.

  Binding between data and security context are not protected.

  MLS specific.

Resolution

Implicit labeling

- **Security Context**

  Domain of Interpretation for the Security Context

  Security context data

- **The Security Context is included in the SPD**

  Defining the DOI for security context

- **The security context is included in the Security Association.**

  Protects the label and the data

  Binds the label to the data

Resolution

IKE communicates Security Context in Security Context Transform

- IKE does not interpret the security context data, thus does not "negotiate" but "communicates" this information.
- MAC layer determines validity of the security context, not IPsec.

Current Status

Individual submission of two drafts.

- draft-jml-ipsec-ikev1-security-context-00.txt
- draft-jml-ipsec-ikev2-security-context-00.txt

A Domain of Interpretation for security contexts is currently being defined.

Initial version of Labeled IPsec implemented in:

- Linux kernel since version 2.6.16.
- ipsec-tools since version 0.7.0

Next Steps

Solicit more reviews.

WG work item

- Labeled networking support was removed from RFC2401.
- As MAC systems and solutions continue to grow and evolve, securing and preserving the various labels across the network will become more necessary.

Trademarks

- Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.
- Microsoft, Windows, Windows NT and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.
- Other company, product or service names may be trademarks or service marks of others.