Context-Based Access Control vs View-Based Access Control

Lewis Kuria, Muchiru
P15/35097/2015
21-January-2018

Context-Based Access Control (CBAC) is a per-application control mechanism that adds advanced traffic filtering functionality to firewalls that isn't limited, as are access lists, to examining packets at the network or transport layer. While CBAC examines both of these layers, it also examines the application-layer protocol data to monitor the state of a given TCP or UDP session. This means, as multiple channels are created or used by applications such as SQL*Net, FTP, and RPC, CBAC can respond by creating temporary openings in the firewall access lists to allow return traffic and additional data connections for specified sessions that originated from within the protected network. This application-layer awareness and capability to evolve with the traffic is beyond the capabilities of access list technologies

View-based access control (VACM) is an SNMPv3 mechanism that regulates access to MIB objects by providing a fine-grained access control mechanism associating users with MIB views. The VACM facilities are essential in ensuring a completely secure agent. *Using SNMPv3 without VACM leaves open a security hole because no restrictions are placed on the level of security that a client must use when accessing MIB objects.* VACM gathers user and security model pairs into *security groups*, which provide a convenient means of identification. Each security group is associated with an *access entry*. Access entries define the access privileges afforded to a security group and they specify the security level that the security group must use in order to access MIB objects. Access entries also list the *MIB views* associated with read, write and notify scenarios. Each MIB view defines a set of *MIB sub-trees* to which a particular access entry is either granted or denied access. MIB sub-trees each consist of a node in the MIB tree hierarchy and all of the node's subordinate elements. You can use bit masks and wildcards in sub-tree definitions.

Differences

- View-based access control enables content-based and context-based security while context based access control does not enable view based access control.
- View-based access control in multilevel secure (MLS) databases suffers from two problems: safety and assurance while context based access control offers filtering services which offer some level of safety.

- Context based access control is mostly used to protect traffic through firewalls while View based access control primarily protects database systems
- View based access control is not a functional solution which as opposed to context based access control which relates to tangible objects, like files, directories, printers etc. It perceives the resource itself as a collection of sub-resources.
- With context based access control. For example when browsing a personalized community web site, context based access control will only allow full access after the user has gone through an "introductory tour" of the web site while with view based access control, Content editors get access to complete contribution details, including author history. Other users only get to see the contribution and author's nickname.

Reference

Denning D, Akl S, Heckman M, Lunt T, Morgenstern M, Neumann P, Schell R (1987) Views for multilevel database security. IEEE Trans Softw Eng SE-13(2):129–140

Miklau G, Suciu D (2004) A formal analysis of information disclosure in data exchange in access control methods. In: Proceedings of the SIGMOD conference, Paris, France. ACM, pp 575–586