Review of SANE: A protection Architecture for Enterprise Networks

Swaminathan Sundararaman

April 18, 2008

This paper presents a bunch of neat techniques to protect enterprise network. The key idea is to have a centralized controller (Domain Controller) which issues capabilities to the clients using resources in the network. During each request the capabilities are verified at every switch and router in the path from the source to the destination. SANE also has a neat way of publishing and accessing services.

Pros:

- Strong attack resistance
- Attack containment in the event of a compromise
- Very practical solution
- Backwards compatible.
- Scalable to tens of thousands of nodes
- Centralized control (easier maintenance)
- Allows natural policies
- Protection at the link layer
- Better fault tolerance by replicating DCs

Cons (incl. Potential Attacks and Vulnerabilities):

- Single point of failure
- Places a huge amount of trust on the switches. Switches could be malicious. Now-a-days networking hardware is programmable and can be easily overwritten.
- Nodes inside the enterprise network could send revocation requests for other nodes in the network thereby creating DoS for other legitimate nodes in the network. SANE does not have a clean way to distinguish misbehaving nodes from well-behaving nodes in this case.
- Inefficient broadcast implementation.
- When the data is encrypted (ssh, VPN etc) the proxies in SANE cannot scan for viruses or apply vulnerability specific filters.
- The authors suggest that proxies can also log application-level transaction. In my humble opinion this is not possible as proxies should have the application level semantic information, which is not always available.
- Solution to revocation state exhaustion will not work. The authors have previously mentioned that enterprise networks are highly optimized and don't have redundancy in paths.
- The solution does protect the system against insider attack. i.e., the administrator of the DC could enter bad configuration values.

To summarize the authors proposed a novel method that helps prevent DoS in enterprise networks. With a centralized DC and capabilities, the authors have shown that better protection can be achieved even with minimal modification to host and the network components.