Fakultät IV – Elektrotechnik und Informatik
Intelligent Networks and Management of Distributed Systems
Research Group Prof. Anja Feldmann, Ph.D.

SANE: A Protection Architecture For Enterprise Networks

Internet Security Seminar
WS 2006/2007

Author: Obi Akonjang
Supervisor: Vinay Aggarwal

February 24th, 2007

Overview

- Introduction
- Current Enterprise Security Mechanisms
- Limitations of Current Security Mechanisms
- The SANE Architecture
- Preventing and Resisting Attacks with SANE
- Prototype Implementation of SANE
- Open Issues (personal opinion)
- Conclusions

Introduction

- Evolution of Enterprise networks
  - From simple LANs to complex Intranets.
  - Growth sustained by complex routing and switching.
  - Adoption of the Internet-based TCP/IP Protocol stack
- Original Internet design goals
  - Global connectivity
  - Decentralized control
  - Openness
  - No security considerations
- Implications
  - Rapid growth and popularity $\rightarrow$ huge success.
  - Medium for easy launch and spread of viruses, worms, malwares, etc
  - Internet-based attacks extends into the enterprise network $\rightarrow$ huge losses.
  - Security of the enterprise network can no longer to be ignored.

Current Security Mechanisms

- Firewalls, IDS, IPS, etc
- Access Control Lists (ACL)
- Network Address Translation (NAT)
- Virtual Local Area Networks (VLAN)
- Enhanced routing protocol and router security.
- Using hybrid trust models.
- Using distributed security policies made up of a combination of the above listed mechanisms running on separate systems as well as on a single system.

Limitations Of Current Mechanisms

- Complexity and difficulty in administration
- Concentrates mostly on secluded security aspects
- Most often only temporarily solves immediate problems
- Built-on solutions still lacks in features and have compatibility issues, e.g. IPSEC
- Fundamental problems still persist, attacks are still very common.

The SANE Architecture (1)

- Definitions

  - SANE: Secure Architecture for the Networked Enterprise.

  - Capability: Encrypted source route between two communicating parties.

- Design goals

  - Establish architecture that supports simple but powerful natural policies, independent of topology and equipment used.

  - Implement security at link layer.

  - Hide all topology and services information from unauthorized parties.

  - Have only one trusted component within the network.

- Approaches

  - Modified network components (clean-slate approach).

  - Unmodified network component.

Ethernet	SANE Header	IP Header	data

The SANE Architecture (2)

- The Domain Controller (DC)

  - Central component in a SANE network.
  - Authenticates users and hosts.
  - Advertises and controls access to available services.
  - Uses capabilities to control communications in network.
  - Consists of 4 Service Modules in 3 functional units.

- Functional Units of the DC

  - Authentication Service Module
  - Network Service Directory Module
  - Protection Layer Controller

The SANE Architecture (3)

- The Authentication Service Module
  - Responsible for authenticating users, hosts and switches.
  - Exchanges and maintains a symmetric key with each.
  - Key is used to secure communication with each.

- Network Service Directory Module
  - Functions like the DNS of a SANE network
  - Maintains a hierarchy of directories and services
  - Uses ACL to control access to each directory and service
  - ACL is declared in terms of principals (users and groups).

The SANE Architecture (4)

- The Protection Layer Controller Module

  - Generates and revokes capabilities.

  - Keeps complete view of network topology.

  - Comprises of *Topology* and *Capabilities service modules*.

- Topology Service Module:

  Use of *HELLO* packets, Minimum Spanning Tree (MST) and link-state updates.

  - Use of *HELLO* packets for immediate neighbor discovery

  - MST only creates default routes for packet-forwarding to the DC.

  - MST prevents switches from learning topology, even via pkt traces.

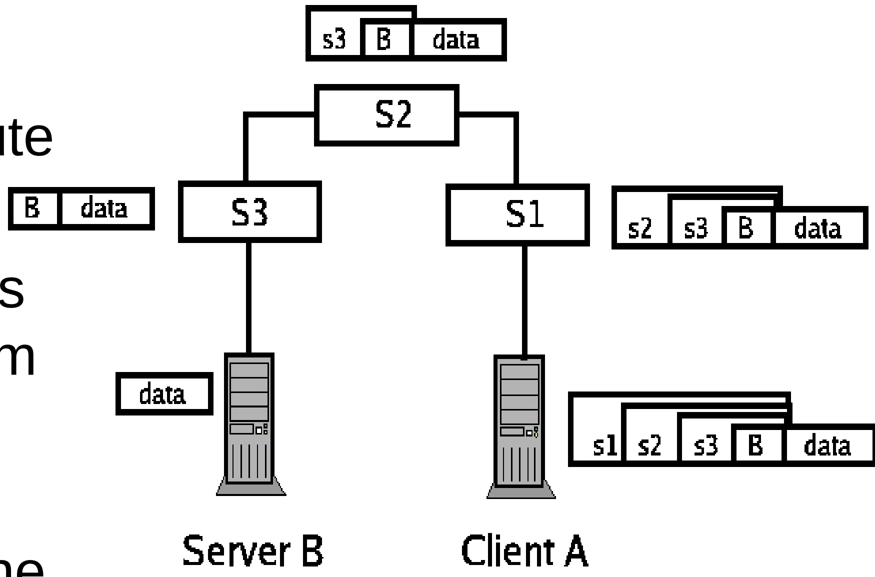
  - Authenticated switches use link-state updates to inform DC of topology.

The SANE Architecture (5)

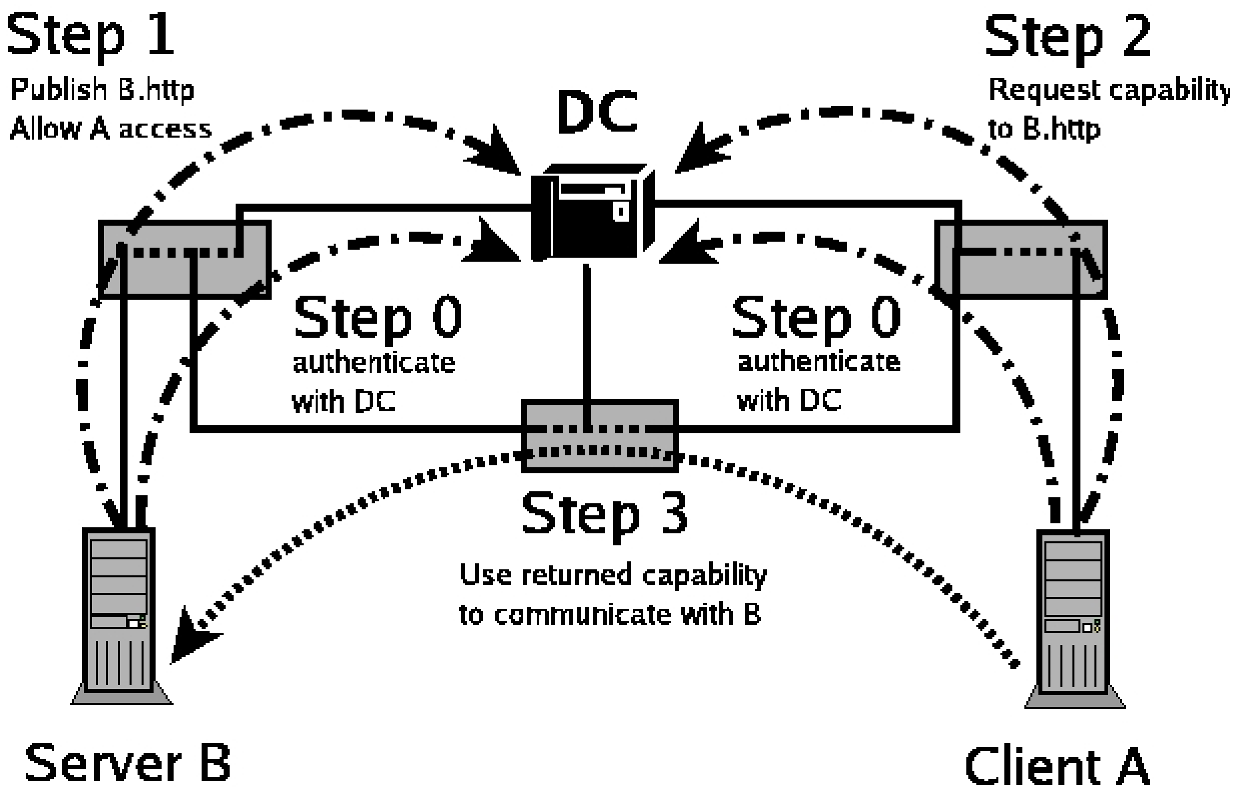
HELLO	Payload			
DC	Request Capability	Authenticator	Payload	
FOWARD	Cap-ID	Cap-Exp	Capability	Payload
REVOKE	Cap-ID	Cap-Exp	Signature_{DC}	

- Capability Service Module:

  - Capability: Switch-level source-route from client to server.
  - Capabilities are encrypted in layers (onion routes) to prove origin from DC and hide topology.
  - Created using client's name & location, service's location and the path between the two parties.



The SANE Architecture (6)

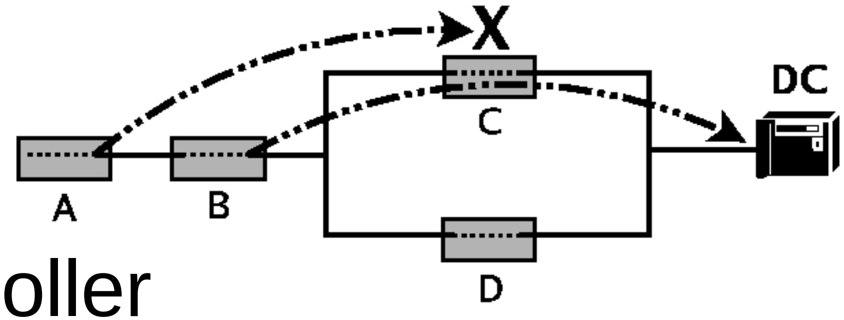


SANE: Preventing Attacks

- Least privilege and centralized control excludes many vulnerabilities.
- NSD uses ACL to control access to Services and directories.
- Exclusive use of only encrypted source routes & encrypted link updates for communications.
- Allows communications only from authenticated principals and switches.

SANE: Resisting Attacks

- Resource exhaustion
  - Flooding attacks:
    > DC Implements rate-limits on number of requests per sender.
  - Revocation state exhaustions:
    > Switch generates new key & invalidates existing capabilities.
    > DC tracks number of revocations per sender, removes sender if threshold is exceeded.
- Malicious switches
  - Disrupting MST discovery.
  - Bad link-state advertisement.



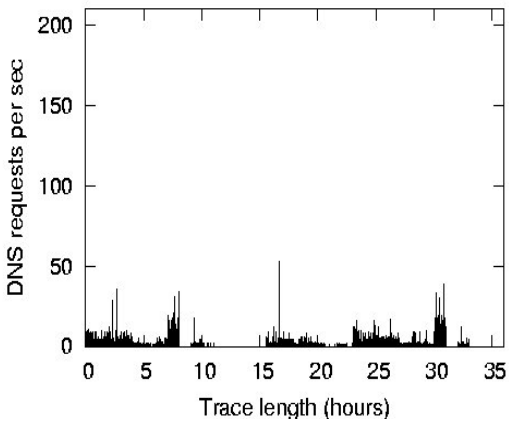
- Malicious Domain Controller
  - Highly trusted, can be single point-of-failure if compromised.
  - Use multiple DCs (threshold cryptography) to distribute trust.

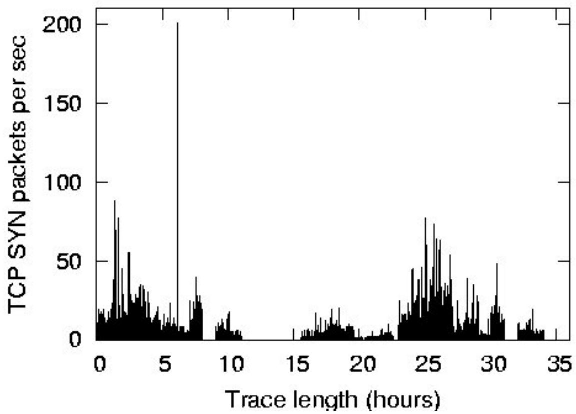
SANE: Prototype Implementation

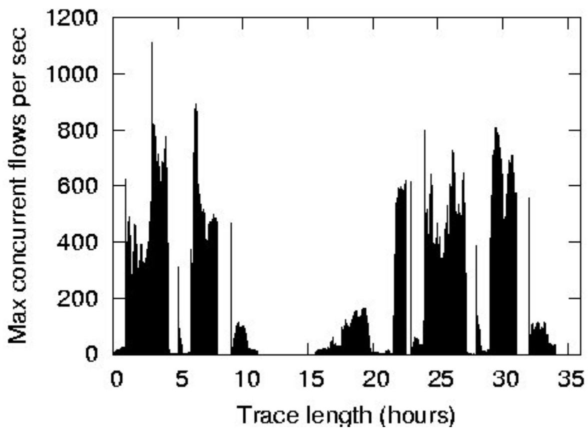
- Using workstations, Switches (10 Hops), IP proxies and a DC.
- MTU of workstations reduced to 1300bytes to create SANE header.
- Use of Virtual Network System (VNS) to specify and test topology.
- Unmodified end-hosts supported by use of translation proxies.
- For authentication, DC pre-configured with public key of all switches.
- DNS queries of unauthenticated users resolves to DC's IP address
- DC provides HTTP interface to browse, request and access directories and services.
- Scalability comparison with recorded traffic traces:
  - 47 Million packets
  - 20,849 DNS requests
  - 145,577 TCP connections

SANE: Evaluation

	5 hops	10 hops	15 hops
DC	100,000 cap/s	40,000 cap/s	20,000 cap/s
Switch	762Mb/s	480Mb/s	250Mb/s







SANE: Open Issues (Personal Opinion)

- Suitability in a hierarchical network environment.
- Support for VLAN.
- Effectiveness and robustness under harsher conditions, such as DDOS affecting multiple components.
- Effective support for services needing broadcast.
- Support for time-sensitive services, e.g. VoIP.
- DC as potential bottleneck and/or single point of failure, even when replicated.

Conclusions

- SANE reduces switching & routing complexity.
- Simplifies network topology and eases administration.
- Centralized approach, network topology concealment and least privilege principle exclude many possible vulnerabilities.
- Centralized approach takes away valuable processing power from otherwise robust switches and routers.
- Restrictive nature of SANE is good on one hand, but reduces flexibility and openness on the other.
- Nevertheless, SANE still provides a good basis with potentials to finally resolve a fundamental problem in an Enterprise network; … the security problem.