System models

Christopher Wee

wee@cs.ucdavis.edu

18 May 1998

1. Introduction

We consider several models of the network system that is protected by the IDIP intrusion detection and response system. The models help us evaluate the appropriateness of the responses of the IDIP system (both detection and response). Thus, the models should consider users and their perceptions of the intrusions and the subsequent responses.

1.1 Tasks

1. Develop a model of how users value services, applications, networks and computing. User's needs are time-varying, so time and contextual events must be considered. Jeff's example is that he doesn't often use the printer (thus, he does not value printer services highly), but if there is to be a presentation or a paper submission deadline, then he values printer services very highly.

   One suggestion for examining the time-varying nature of user values is to use a task-oriented approach. Hypothetically construct tasks that the user performs and examine the needs and priorities at each stage of the task. Thus, the user can indicate what their values are keyed to significant task milestones.

2. We need a process to poll the users about their values and preferences concerning application services. Since we anticipate that their values are time-varying, we use a variety of methods to learn their needs including 1) surveys, 2) periodic re-evaluation of their actual usage and attempted usage, 3) GUIs to interrogate them during the work session. This data might be fed into a matrix of users, services and applications, needs (availabilty, privacy, integrity).

3. Map the user's values matrix (users-applications-concerns) onto actual system architecture (user logins-protocols and servers-security mechanisms)

2. Network model

The network model consists of hosts, routers, sub-networks and TCP/IP-based network traffic. Traffic is characterized by protocol, source and destination IP addresses, and source and destination port numbers.

Availability is characterized by network reachability and bandwidth. The final result would be a huge matrix with host IP address as the columns and rows, and the cells contain the bandwidth from the source IP to the destination IP.

Network Protocol	Network Address	Network Address	Bandwidth
Ipv4	128.120.		
Appletalk			

What language could we use to describe the topology of an IP network? It would be some sort of graph language.

3. Application model

In the application model, the system consists of sets of application servers and clients. Application clients communicate with application servers in a series of overlapping sessions. A session is a sequence of transactions between the client and server. Applications include e-mail, name services, WWW, FTP, …, etc. For example, a user uses FTP to download a set of files from an FTP server.

The system behavior is summarized as follows:

4. Start an application server
5. Stop an application server
6. Start a transaction between client and server
7. Terminate transaction

The system is characterized by the following attributes:

- Application class name
- Network protocols
- list of servers,
- list of clients
- List of transaction types.
- number of concurrent sessions
- session thresholds, minimum, maximum and typical.

Each service is available and uncongested, available but congested, or unavailable. Overall availability of the service may be measured by computing the number of successful transactions that are served against thresholds of minimum service levels indicated by policy.

Application	**Protocols**	**Server**	**Clients**	**Session Thresholds**	**Sessions**
E-mail	SMTP, POP2, POP-3, IMAP	cs.ucdavis.edu	*.*.*.*	0-1000 connections/day	
Naming	DNS, NIS, NIS+, LDAP	olympus.cs.ucdavis.edu	128.120.56.*		
WWW	http (80), HTTPS	128.120.56.77	*.*.*.*		
File servers	NFS (2049)	keep3.cs.ucdavis.edu	128.120.55.* 128.120.56.*		
Interactive logins	Telnet (23), ssh (22), rlogin, rsh	Tallac.cs.ucdavis.edu	*.*.*.*		

Printing	Lpd	Hood.cs.ucdavis.edu	128.120.56.*	10-1000 /day	

How do we assign costs to each of the servers? I would assign costs based on users' perception of the value that the server provides to them. How can we determine how each user values the network services? Can we poll the user. Perceptions change with time, so we have to poll regularly. Can we measure how user's use services, or at least, attempt to use services. If the user attempts to use FTP, but is unable to do so – the server contacted did not reply (unavailable), or was turned away because too many users were logged on (congested), or the files/data was not transmitted successfully.

Users care about application level performance.

Chris Wee needs the following:

- POP-3 access to mailbox.ucdavis.edu from just about anywhere on the Internet, most typically from khumbutse.cs.ucdavis.edu or from the modem*.ucdavis.edu
- Printer service to HP printer (2245 Paper shredder) from Appletalk. I only need this access when I'm connected to the seclab LAN.
- WWW access from anywhere.
- NFS from any of the seclab hosts, *.cs.ucdavis.edu to keep and other seclab hosts.

We can use network monitoring to assess when transactions are successful or whether access has been denied, or even incomplete.

What are the failure states of the model? Servers may be unavailable or congested. What are the client being refused service because of authentication failure? What about loss of confidentiality of transaction data? Damage to data on the server due to client failure.

4. User model

This model represents users as objects and measures the amount of caffiene in each user. Hackers are characterized by a caffiene level of X. We could also measure the command profiles (commands used) of each user.

User	Real-name	Resources used	Services used
Wee	Chris Wee	lhotse.cs.ucdavis.edu, khumbutse.cs.ucdavis.edu	

Policy specifications

Who writes policies?

Answer: Everyone. The users each have one. The site's (administrator) have one (each). The infrastructure owners (ISP) have policies. The problem is combining them, determining the constraits from the combined/aggregate policy.

Who enforces policies?

Answer: Definitely everyone, some enforcement at the origin of the requests (users), some along the way (networks, firewalls), some enforcement at the endpoints (server).

5. Conclusions