SMARTECH

NetCheck Proposal Report

Filiz Alaca
Gülşah Karaduman
Hande Çelikkanat
Kezban Demirtaş
Neslihan Bulut

Department of Computer Engineering
METU

October 2005
1 PROJECT TEAM

1.1 Company Name
Our company name has been decided to be “Smartech”.

1.2 Company Members

<table>
<thead>
<tr>
<th>Name</th>
<th>ID</th>
<th>Email</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filiz ALACA</td>
<td>1297381</td>
<td><a href="mailto:e129738@metu.edu.tr">e129738@metu.edu.tr</a></td>
</tr>
<tr>
<td>Gülşah KARADUMAN</td>
<td>1297902</td>
<td><a href="mailto:e1297902@ceng.metu.edu.tr">e1297902@ceng.metu.edu.tr</a></td>
</tr>
<tr>
<td>Hande ÇELİKKANAT</td>
<td>1347327</td>
<td><a href="mailto:e1347327@ceng.metu.edu.tr">e1347327@ceng.metu.edu.tr</a></td>
</tr>
<tr>
<td>Kezban DEMİRTAŞ</td>
<td>1297704</td>
<td><a href="mailto:e129770@metu.edu.tr">e129770@metu.edu.tr</a></td>
</tr>
<tr>
<td>Neslihan BULUT</td>
<td>1347228</td>
<td><a href="mailto:e134722@metu.edu.tr">e134722@metu.edu.tr</a></td>
</tr>
</tbody>
</table>

1.3 Member Roles

**Contact People:** The contact people are responsible for getting in contact with instructors and assistants. This duty will be handled by Neslihan BULUT and Kezban DEMİRTAŞ.

**Project Archive Keepers:** Project archive keepers are responsible for archiving the soft and hard copies of the documents and taking weekly backup of project repository. This duty will be handled by Hande ÇELİKKANAT and Filiz ALACA.

**Project Schedule Coordinators:** Project schedule coordinators are responsible for determining the deadlines for the tasks and tracking of the weekly progress. Neslihan BULUT and Gülşah KARADUMAN will be the schedule coordinators.

**Project Manager:** General coordination and communication of the team will be the responsibility of project manager. It will be handled by Gülşah KARADUMAN.
1.4 Ground Rules

We have decided the following ground rules in our first formal meeting:

- We will be holding meetings twice a week. Those meetings will be held on Tuesday between 18:00 and 22:00 and on Wednesday between 17:00 and 18:00. Meetings will start and finish on time.
- The members who have an excuse at the meeting time will inform the project manager until 12:00 on the day of the meeting.
- All members will be responsible for checking the project’s mail group every day.
- All actions and tasks performed for the project by the team members will be posted to the project mail group.
- During the meetings, the recorder will take the notes of the meeting and will post these notes to the mail group. In each meeting, the recorder’s duty will be done in turn.

2 PROJECT

2.1 Project Title

Our project title is decided to be "NetCheck".

2.2 Problem Definition

Today, Internet has become the most widely used communication tool. This powerful tool has spread amazingly fast and today all kinds of fields, whether scientific development or entertainment industry or e-commerce have become heavily dependent on it. However Internet may be a realm of chaos because of abuse which may appear in various forms such as malicious code, invalid input, parameter manipulation, and other content based attacks. At that point, security tools may and must appear in order to prevent harmful effects of malicious usage.

Developed security tools such as NetWatch, Snort, and firewalls mainly support some of the following properties: network traffic monitoring, intrusion detection/prevention, accounting and analysing. However, in such tools, there is a missing point which is web-based monitoring, management and automation and our intention is to fill this gap.
2.3 Project Scope

"NetCheck" will be a web-based administrated application level gateway which provides network monitoring, management and automation. It is intended to provide the following properties:

- **Network Traffic Monitoring:**
  All incoming and outgoing web traffic will be displayed on a web page in real time. We are intending to display the following features:
  - Source address
  - Destination address
  - Size of communication packets.

- **Access Restriction:**
  Restriction will be applied by the following criteria:
  - URL black list (the URL’s of restricted web sites)
  - Restricted time intervals for specified URL’s (e.g. URL x is not to be accessed between 09:00-11:00).

- **Download Restriction:**
  The administrator will be able to specify a bandwidth limit for the users’ download operation.

- **Content Monitoring:**
  Contents of incoming packets will be displayed to the administrator in the following fashion:
  - Source address
  - Destination address
  - Date of access
  - URL of the web site

- **Content Filtering:**
  Access to the web sites which include contents listed in "black-list" will be restricted. The content in the "black-list" will be defined by the administrator. For example the list may keep content about sex, alcohol/drug, violence, and gambling. Packets arriving from outside servers will be monitored to prevent malicious content from entering to the internal network.
• **Network Statistics:**
  Various statistical information can be shown by the administrator, including:
  - Web sites with their hit rates and requesting IPs
  - Download information
  - Daily network traffic
  - Etc.

• **Administrative Facilities:**
  The administrator of the system will be able to perform the followings via the web interface:
  - Defining security policies
  - Defining access and download rights for the IPs in the local network
  - Monitoring the active connections
  - Instant interruption of access and downloads via the web interface

• **Other Intended Facilities:**
  We are also intending to provide the following facilities:
  - A caching mechanism for reducing the load on network and increasing the access speed
  - Specifying authorized URLs for update distribution
  - E-mail notification to administrator
  - Content classification for the visited web sites.

### 2.4 Intended Hardware and Software Platforms

Project will be developed for managing a local network, via a gateway. Gateway machine will have at least two network interface card. Related gateway machine will not only deal with routing process, but it will be also dealing with content filtering, restriction, web interface and database management. As a result of this it should have powerful hardware resources such as CPU and memory. Especially the CPU resource should be sufficient enough to meet our needs. Also the client machines located in the local network will be accessing the internet through this gateway. In our project, we will be using a gateway machine built on Linux/Unix platform. The daemon of the
The project will be developed by using C programming language. And the web interface will be developed in PHP or JSP. As a result, the following are needed in the development environment:

- GCC (Gnu C Compiler)
- Web Server (Apache)
- Firewall (Iptables)
- DBMS (PostgreSQL / MySQL)

3 FIRST FORMAL MEETING

We held our first formal meeting on 27 September 2005. It took nearly 3 hours and we decided on the followings:

- Our project title
- Problem definition
- Project scope
- Hardware and software requirements for the project development
- Group members’ responsibilities
- Ground rules for our team