Kurzfassung der Diplomarbeit

Abteilung	**Informatik**
Name der Diplomanden	**Philipp Kocher & Mario Rütti**
Diplomjahr	**2000**
Titel der Diplomarbeit	**S-Tool**
Examinatorin/Examinator	**I.Bütler & W.Sprenger von der Compass Security AG**

Kurzfassung der Diplomarbeit

Unserer Auftraggeber ist die auf Netzwerksicherheit spezialisierte Firma Compass Security AG aus Rapperswil. Um Informationen und Fehler in einem Netzwerk zu suchen, setzen die Mitarbeiter von Compass Security, viele einzelne, auf ein Spezialgebiet beschränkte Programme, wie zum Beispiel ein Portscanner, ein. Ein erweiterbares „Universaltool“ wird sowohl die Installation und Verwaltung, als auch die Bedienung vereinfachen.

Als Studienarbeit wurde deshalb das S-Tool entwickelt, das ein Gerüst bietet, in welches sowohl diese existierenden Programme, als auch neue Funktionen integriert werden können. Das S-Tool wurde als Client/Server-Applikation realisiert. Um eine Funktion den Clients zur Verfügung zu stellen, muss diese ausschliesslich auf dem Server installiert und gewartet werden. Ausserdem erlaubt die Client/Server-Architektur den Betrieb des S-Tools durch einen Firewall.

In der Diplomarbeit wird das S-Tool um Sicherheitsanforderungen erweitert. Damit sind folgende Aspekte gemeint:

- Authentizität (man weiss wer den Server nutzt)
- Vertraulichkeit (die Kommunikation ist verschlüsselt)
- Integrität (die Daten können nicht verändert werden)

Für die S-Tool Funktionen ist es wichtig, ICMP-Pakete senden und empfangen zu können. Deshalb wird das S-Tool den Funktionen neu einen ICMP-Socket zur Verfügung stellen.

Das S-Tool ist dafür ausgelegt, die Authentisierung des S-Tool-Clients über einen Authentisierungsserver zu tätigen. Dafür werden zwei Varianten implementiert, die eine verwendet den LDAP-Server zur Authentisierung, die andere einen RADIUS-Server. Der RADIUS-Server ist in der Lage die Authentisierung zu delegieren, so kann dieser sie zum Beispiel an einen LDAP oder auch ACE-Server weiterleiten.

Die Benutzerdaten werden auf einem LDAP-Server gespeichert. Um eine Investition in die Zukunft zu tätigen und auf eine zukunftsträchtige Technologie zu setzen, wird als LDAP-Server das „Active Directory“ von Windows 2000 eingesetzt. Des weiteren soll aber in zweiter Priorität auch der „Netscape Directory Server“ unterstützt werden.

Um die Vertraulichkeit und Integrität auf der Übertragungsstrecke zu gewährleisten, wird die Kommunikation zwischen Client und Server verschlüsselt. Dazu wird SSL (Secure Socket Layer) verwendet, welches eine von Netscape entwickelte Technologie ist und für Internetapplikationen sehr oft verwendet wird.

Da mit Java keine Möglichkeit besteht auf ICMP-Pakete zuzugreifen, dies jedoch für S-Tool-Funktionen wichtig ist, wird ein ICMP-Socket implementiert. Unter Windows existiert die „Winsock.dll“, die die gewünschte Funktionalität bietet. Um auf diese DLL zuzugreifen, wird das „Java-Native-Interface“ verwendet.