

MAD-Network Monitoring

Diplomarbeit 2014/15

Porcic Alin, Ranalter Daniel, Singh Manpreet
Betreuer: Dr. Michael Weiss
Höhere Technische Bundes Lehr- und Versuchsanstalt Anichstraße
Abteilung Höhere Elektronik und Technische Informatik
5bHEL

20. Januar 2015

Zusammenfassung

lorem ipsum

Inhaltsverzeichnis

| | | |
|----------|--|----------|
| 1 | Einleitung von Stojanovic Marko | 5 |
| 1.1 | Aufgabenstellung | 5 |
| 1.2 | Aufteilung | 5 |
| 2 | Theorie zu den einzelnen Gebieten der Arbeit | 6 |
| 2.1 | Kryptologie von Porcic Alin | 6 |
| 2.1.1 | Allgemeines | 6 |
| 2.1.2 | Kryprographie | 6 |
| | Geschichte der Kryptographie | 6 |
| | Klassische Kryptographie | 6 |
| | Moderne Kryptographie | 6 |
| | Ziele der Kryptographie | 6 |
| | Methoden | 6 |
| 2.1.3 | Kryptoanalyse | 6 |
| | Geschichte der Kryptoanalyse | 6 |
| | Ziele der Kryptoanalyse | 6 |
| | Methoden | 6 |
| 2.1.4 | Verschlüsselungsverfahren | 7 |
| | Symmetrische Verschlüsselungsverfahren | 7 |
| | Merkmale | 7 |
| | Nennenswerte symmetrische Verschlüsselungssysteme | 7 |
| | DES | 7 |
| | 3DES | 7 |
| | IDEA | 7 |
| | CAST | 7 |
| | RC4 | 7 |
| | RC5, RC5a, RC6 | 7 |
| | A5 | 7 |
| | Blowfish | 7 |
| | Twofish | 7 |
| | AES | 7 |
| | Asymmetrische Verschlüsselungsverfahren | 7 |
| | Merkmale | 7 |
| | Digitale Signatur | 7 |
| | Zertifikate | 7 |
| | Nennenswerte asymmetrische Verschlüsselungssysteme | 7 |
| | Diffie-Hellman | 7 |
| | RSA | 7 |
| | ElGamal | 7 |
| | Hybride Verschlüsselungsverfahren | 7 |
| | Merkmale | 7 |
| | Nenneswerte hybride Verschlüsselungssysteme | 8 |
| | IPsec | 8 |
| | TLS/SSL | 8 |
| | PGP | 8 |
| | Hash-Verfahren | 8 |
| | Merkmale | 8 |

| | | |
|-------|--|----|
| | Nennenswerte Hashsysteme | 8 |
| | MD2, MD4, MD5 | 8 |
| | SHA | 8 |
| | RIPEMD | 8 |
| 2.2 | E-Mail von Singh Manpreet | 8 |
| 2.2.1 | Allgemein E-Mail und Notification | 8 |
| | Senden | 8 |
| | Graphische Erklärung | 8 |
| | Empfangen | 8 |
| | IMAP | 8 |
| | POP | 8 |
| 2.2.2 | E-Mail | 8 |
| | Ursprung/Entstehung | 8 |
| | Bedeutung heute | 8 |
| | Zukünftig | 8 |
| | Probleme | 9 |
| | Kleine Probleme | 9 |
| | Große Probleme - Gefahren | 9 |
| | Sicherheit | 9 |
| | Versuche | 9 |
| | Was kann ich tun? | 9 |
| 2.3 | Oberfläche von Singh Manpreet | 9 |
| 2.3.1 | Allgemein User Interface (UI) | 9 |
| | Geschichte | 9 |
| | UIs | 9 |
| | Zukünftig | 9 |
| 2.3.2 | Grahpic User Interface (GUI) | 9 |
| | Bedeutung | 9 |
| | Wichtigkeit | 9 |
| | Vergleich GUI - Command Line Interface (CLI) | 9 |
| | Marktführende | 9 |
| | Wichtige Operating System GUIs | 9 |
| | Vor- und Nachteile | 9 |
| | Möglichkeiten der Realisierung | 10 |
| | Genauer | 10 |
| | Realisierung | 10 |
| | Graphikkarte oder Prozessor | 10 |
| 2.4 | Netzwerke von Ranalter Daniel | 10 |
| 2.4.1 | Grundlagen | 10 |
| | Der Host | 10 |
| | MAC-Adressen | 10 |
| | IP-Adressen | 10 |
| | Ports | 10 |
| | Schichtenmodel | 10 |
| | OSI | 10 |
| | TCP/IP | 10 |
| | Client-Server Verhältnis | 10 |
| 2.4.2 | Protokolle | 10 |
| | Address Resolution Protocol - ARP | 10 |
| | Sicherheitsaspekte | 10 |
| | Internet Protocol - IP | 10 |
| | IPv4 | 10 |
| | IPv6 | 10 |
| | User Datagram Protocol - UDP | 11 |
| | Transmission Control Protocol - TCP | 11 |
| | Dynamic Host Configuration Protocol - DHCP | 11 |
| | Domain Name System - DNS | 11 |
| | Internet Control Message Protocol - ICMP | 11 |

| | | |
|----------|---|-----------|
| | ICMP Echo Request/Response - Ping | 11 |
| | File Transport Protocol - FTP | 11 |
| | Simple Network Managing Prorocol - SNMP | 11 |
| | Management Information Base | 11 |
| | SNMPv2/SNMPv2c | 11 |
| | SNMPv3 | 11 |
| | Hypertext Transfer Protocol - HTTP | 11 |
| 2.4.3 | Netzwerksicherheit | 11 |
| 2.5 | Datenbank von Stojanovic Marko | 11 |
| 2.5.1 | Allgemeines | 11 |
| | Geschichte | 11 |
| | Definitionen | 11 |
| | Effizienz | 12 |
| | Funktionen | 12 |
| | Anwendungen | 12 |
| 2.5.2 | Datenbanksysteme | 12 |
| | Datenbankmanagementsysteme | 12 |
| | Datenbank | 12 |
| 2.5.3 | Relationales Datenbankmanagementsystem (RDBMS) | 12 |
| | Prinzip eines RDBMS | 12 |
| | Tabellen | 12 |
| | Alternative Datenbankmanagementsysteme | 12 |
| | Information Management System | 12 |
| | Netzwerkdatenbankmodell | 12 |
| | Hierarchisches Datenbankmodell | 12 |
| 2.5.4 | Zugriffe | 12 |
| | Zugriffsmöglichkeiten | 12 |
| | Sicherheit | 12 |
| | Gleichzeitige Zugriffe | 12 |
| 2.5.5 | Sprachen | 13 |
| | Verwaltungsgetrennte Sprachen | 13 |
| | Abfragen und Manipulieren der Daten | 13 |
| | Datenbankstruktur | 13 |
| | Berechtigungen | 13 |
| | SQL | 13 |
| 2.5.6 | SQLite | 13 |
| | Geschichte | 13 |
| | Eigenschaften | 13 |
| | Datentypen | 13 |
| | Syntax | 13 |
| | Befehle | 13 |
| | Vor- und Nachteile | 13 |
| | Vorteile | 13 |
| | Nachteile | 13 |
| 3 | Möglichkeiten der Realisierung Allgemein von Ranalter Daniel | 14 |
| 4 | Programmrealisierung | 15 |
| 4.1 | JobSystem von Porcic Alin und Ranalter Daniel | 15 |
| 4.2 | Notification von Singh Manpreet | 15 |
| 4.3 | Database von Stojanovic Marko | 15 |
| 4.3.1 | MAD-DB | 15 |
| | Erklärung | 15 |
| | Grafische Übersicht | 15 |
| 4.3.2 | Programmcode | 15 |
| 4.4 | Logging von Ranalter Daniel | 15 |
| 5 | User Manual von Procic Alin | 16 |

Kapitel 1

Einleitung von Stojanovic Marko

lorem ipsum

1.1 Aufgabenstellung

lorem ipsum

1.2 Aufteilung

lorem ipsum

Kapitel 2

Theorie zu den einzelnen Gebieten der Arbeit

2.1 Kryptologie von Porcic Alin

2.1.1 Allgemeines

lorem ipsum

2.1.2 Kryptoographie

lorem ipsum

Geschichte der Kryptographie

lorem ipsum

Klassische Kryptographie lorem ipsum

Moderne Kryptographie lorem ipsum

Ziele der Kryptographie

lorem ipsum

Methoden

lorem ipsum

2.1.3 Kryptoanalyse

lorem ipsum

Geschichte der Kryptoanalyse

lorem ipsum

Ziele der Kryptoanalyse

lorem ipsum

Methoden

lorem ipsum

2.1.4 Verschlüsselungsverfahren

lorem ipsum

Symmetrische Verschlüsselungsverfahren

lorem ipsum

Merkmale lorem ipsum

Nennenswerte symmetrische Verschlüsselungssysteme lorem ipsum

DES lorem ipsum

3DES lorem ipsum

IDEA lorem ipsum

CAST lorem ipsum

RC4 lorem ipsum

RC5, RC5a, RC6 lorem ipsum

A5 lorem ipsum

Blowfish lorem ipsum

Twofish lorem ipsum

AES lorem ipsum

Asymmetrische Verschlüsselungsverfahren

lorem ipsum

Merkmale lorem ipsum

Digitale Signatur lorem ipsum

Zertifikate lorem ipsum

Nennenswerte asymmetrische Verschlüsselungssysteme lorem ipsum

Diffie-Hellman lorem ipsum

RSA lorem ipsum

ElGamal lorem ipsum

Hybride Verschlüsselungsverfahren

lorem ipsum

Merkmale lorem ipsum

Nennenswerte hybride Verschlüsselungssysteme lorem ipsum

IPsec lorem ipsum

TLS/SSL lorem ipsum

PGP lorem ipsum

Hash-Verfahren

lorem ipsum

Merkmale lorem ipsum

Nennenswerte Hashsysteme lorem ipsum

MD2, MD4, MD5 lorem ipsum

SHA lorem ipsum

RIPEMD lorem ipsum

2.2 E-Mail von Singh Manpreet

lorem ipsum

2.2.1 Allgemein E-Mail und Notification

lorem ipsum

Senden

lorem ipsum

Graphische Erklärung lorem ipsum

Empfangen

lorem ipsum

IMAP lorem ipsum

POP lorem ipsum

2.2.2 E-Mail

lorem ipsum

Ursprung/Entstehung

lorem ipsum

Bedeutung heute

lorem ipsum

Zukünftig lorem ipsum

Probleme

lorem ipsum

Kleine Probleme lorem ipsum

Große Probleme - Gefahren lorem ipsum

Sicherheit

lorem ipsum

Versuche lorem ipsum

Was kann ich tun? lorem ipsum

2.3 Oberfläche von Singh Manpreet

lorem ipsum

2.3.1 Allgemein User Interface (UI)

lorem ipsum

Geschichte

lorem ipsum

UIs

lorem ipsum

Zukünftig

lorem ipsum

2.3.2 Graphical User Interface (GUI)

lorem ipsum

Bedeutung

lorem ipsum

Wichtigkeit

lorem ipsum

Vergleich GUI - Command Line Interface (CLI)

lorem ipsum

Marktführende lorem ipsum

Wichtige Operating System GUIs lorem ipsum

Vor- und Nachteile

lorem ipsum

Möglichkeiten der Realisierung

lorem ipsum

Genauer

lorem ipsum

Realisierung lorem ipsum

Graphikkarte oder Prozessor lorem ipsum

2.4 Netzwerke von Ranalter Daniel

lorem ipsum

2.4.1 Grundlagen

lorem ipsum

Der Host

MAC-Adressen lorem ipsum

IP-Adressen lorem ipsum

Ports lorem ipsum

Schichtenmodel

lorem ipsum

OSI lorem ipsum

TCP/IP lorem ipsum

Client-Server Verhältnis

lorem ipsum

2.4.2 Protokolle

lorem ipsum

Address Resolution Protocol - ARP

lorem ipsum

Sicherheitsaspekte lorem ipsum

Internet Protocol - IP

lorem ipsum

IPv4 lorem ipsum

IPv6

User Datagram Protocol - UDP

lorem ipsum

Transmission Control Protocol - TCP

lorem ipsum

Dynamic Host Configuration Protocol - DHCP

lorem ipsum

Domain Name System - DNS

lorem ipsum

Internet Control Message Protocol - ICMP

lorem ipsum

ICMP Echo Request/Response - Ping lorem ipsum

File Transport Protocol - FTP

lorem ipsum

Simple Network Managing Protocol - SNMP

lorem ipsum

Management Information Base lorem ipsum

SNMPv2/SNMPv2c lorem ipsum

SNMPv3 lorem ipsum

Hypertext Transfer Protocol - HTTP

lorem ipsum

2.4.3 Netzwerksicherheit

lorem ipsum

2.5 Datenbank von Stojanovic Marko

lorem ipsum

2.5.1 Allgemeines

lorem ipsum

Geschichte

lorem ipsum

Definitionen

lorem ipsum

Effizienz

lorem ipsum

Funktionen

lorem ipsum

Anwendungen

lorem ipsum

2.5.2 Datenbanksysteme

lorem ipsum

Datenbankmanagementsysteme

lorem ipsum

Datenbank

lorem ipsum

2.5.3 Relationales Datenbankmanagementsystem (RDBMS)

lorem ipsum

Prinzip eines RDBMS

lorem ipsum

Tabellen

lorem ipsum

Alternative Datenbankmanagementsysteme

lorem ipsum

Information Management System lorem ipsum

Netzwerkdatenbankmodell lorem ipsum

Hierarchisches Datenbankmodell lorem ipsum

2.5.4 Zugriffe

lorem ipsum

Zugriffsmöglichkeiten

lorem ipsum

Sicherheit

lorem ipsum

Gleichzeitige Zugriffe

lorem ipsum

2.5.5 Sprachen

lorem ipsum

Verwaltungsgetrennte Sprachen

lorem ipsum

Abfragen und Manipulieren der Daten lorem ipsum

Datenbankstruktur lorem ipsum

Berechtigungen lorem ipsum

SQL

lorem ipsum

2.5.6 SQLite

lorem ipsum

Geschichte

lorem ipsum

Eigenschaften

lorem ipsum

Datentypen

lorem ipsum

Syntax

lorem ipsum

Befehle

lorem ipsum

Vor- und Nachteile

lorem ipsum

Vorteile lorem ipsum

Nachteile lorem ipsum

Kapitel 3

Möglichkeiten der Realisierung Allgemein von Ranalter Daniel

lorem ipsum

Kapitel 4

Programmrealisierung

lorem ipsum

4.1 JobSystem von Porcic Alin und Ranalter Daniel

lorem ipsum

4.2 Notification von Singh Manpreet

lorem ipsum

4.3 Database von Stojanovic Marko

4.3.1 MAD-DB

lorem ipsum

Erklärung

lorem ipsum

Grafische Übersicht

lorem ipsum

4.3.2 Programmcode

lorem ipsum

4.4 Logging von Ranalter Daniel

lorem ipsum

Kapitel 5

User Manual von Procic Alin

lorem ipsum

Kapitel 6

Quellenverzeichnis

lorem ipsum