

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

14. Januar 2015

Zusammenfassung

Inhaltsverzeichnis

1	Aufgabenstellung	4
2	Theorie zu den einzelnen Gebieten der Arbeit	5
2.1	Wahl der Sprache	5
2.2	Kryptologie	5
2.2.1	Allgemeines	5
2.2.2	Kryprographie	5
	Geschichte der Kryptographie	5
	Klassische Kryptographie	5
	Moderne Kryptographie	5
	Ziele der Kryptographie	5
	Methoden	5
2.2.3	Kryptoanalyse	5
	Geschichte der Kryptoanalyse	5
	Ziele der Kryptoanalyse	5
	Methoden	6
2.2.4	Verschlüsselungsverfahren	6
	Symmetrische Verschlüsselungsverfahren	6
	Merkmale	6
	Nennenswerte symmetrische Verschlüsselungssysteme	6
	DES	6
	3DES	6
	IDEA	6
	CAST	6
	RC4	6
	RC5, RC5a, RC6	6
	A5	6
	Blowfish	6
	Twofish	6
	AES	6
	Asymmetrische Verschlüsselungsverfahren	6
	Merkmale	6
	Digitale Signatur	6
	Zertifikate	6
	Nennenswerte asymmetrische Verschlüsselungssysteme	6
	Diffie-Hellman	6
	RSA	6
	ElGamal	6
	Hybride Verschlüsselungsverfahren	6
	Merkmale	7
	Nenneswerte hybride Verschlüsselungssysteme	7
	IPsec	7
	TLS/SSL	7
	PGP	7
	Hash-Verfahren	7
	Merkmale	7
	Nennenswerte Hashsysteme	7

	MD2, MD4, MD5	7
	SHA	7
	RIPEMD	7
2.3	E-Mail	7
2.3.1	Allgemein E-Mail und Notification	7
	Senden	7
	Graphische Erklärung	7
	Empfangen	7
	IMAP	7
	POP	7
2.3.2	E-Mail	7
	Ursprung/Entstehung	7
	Bedeutung heute	7
	Zukünftig	8
	Probleme	8
	Kleine Probleme	8
	Große Probleme - Gefahren	8
	Sicherheit	8
	Versuche	8
	Was kann ich tun?	8
2.4	Oberfläche	8
2.4.1	Allgemein User Interface (UI)	8
	Geschichte	8
	UIs	8
	Zukünftig	8
2.4.2	Grahpic User Interface (GUI)	8
	Bedeutung	8
	Wichtigkeit	8
	Vergleich GUI - Command Line Interface (CLI)	8
	Marktführende	8
	Wichtige Operating System GUIs	8
	Vor- und Nachteile	9
	Möglichkeiten der Realisierung	9
	Genauer	9
	Realisierung	9
	Graphikkarte oder Prozessor	9
2.5	Netzwerke	9
2.5.1	Grundlagen	9
	Der Host	9
	MAC-Adressen	9
	IP-Adressen	9
	Ports	9
	Schichtenmodell	9
	OSI	9
	TCP/IP	9
	Client-Server Verhältnis	9
2.5.2	Protokolle	9
	Address Resolution Protocol - ARP	9
	Sicherheitsaspekte	9
	Internet Protocol - IP	9
	IPv4	9
	IPv6	10
	User Datagram Protocol - UDP	10
	Transmission Control Protocol - TCP	10
	Dynamic Host Configuration Protocol - DHCP	10
	Domain Name System - DNS	10
	Internet Control Message Protocol - ICMP	10
	ICMP Echo Request/Response - Ping	10

	File Transport Protocol - FTP	10
	Simple Network Managing Prorocol - SNMP	10
	Management Information Base	10
	SNMPv2/SNMPv2c	10
	SNMPv3	10
	Hypertext Transfer Protocol - HTTP	10
2.5.3	Netzwerksicherheit	10
2.6	Datenbank	10
2.6.1	Allgemeines	10
	Geschichte	10
	Definitionen	10
	Effizienz	11
	Funktionen	11
	Anwendungen	11
2.6.2	Datenbanksysteme	11
	Datenbankmanagementsysteme	11
	Datenbank	11
2.6.3	Relationales Datenbankmanagementsystem (RDBMS)	11
	Prinzip eines RDBMS	11
	Tabellen	11
	Alternative Datenbankmanagementsysteme	11
	Information Management System	11
	Netzwerkdatenbankmodell	11
	Hierarchisches Datenbankmodell	11
2.6.4	Zugriffe	11
	Zugriffsmöglichkeiten	11
	Sicherheit	11
	Gleichzeitige Zugriffe	11
2.6.5	Sprachen	12
	Verwaltungsgetrennte Sprachen	12
	Abfragen und Manipulieren der Daten	12
	Datenbankstruktur	12
	Berechtigungen	12
	SQL	12
2.6.6	SQLite	12
	Geschichte	12
	Eigenschaften	12
	Datentypen	12
	Syntax	12
	Befehle	12
	Vor- und Nachteile	12
	Vorteile	12
	Nachteile	12
3	Programmrealisierung	13
3.1	JobSystem	13
3.2	Notification	13
3.3	Database	13
3.3.1	MAD-DB	13
	Erklärung	13
	Grafische Übersicht	13
3.3.2	Programmcode	13
3.4	Logging	13
4	Abbildungsverzeichnis	14
5	Quellenverzeichnis	15

Kapitel 1

Aufgabenstellung

lorem ipsum

Kapitel 2

Theorie zu den einzelnen Gebieten der Arbeit

2.1 Wahl der Sprache

lorem ipsum

2.2 Kryptologie

2.2.1 Allgemeines

lorem ipsum

2.2.2 Kryptographie

lorem ipsum

Geschichte der Kryptographie

lorem ipsum

Klassische Kryptographie lorem ipsum

Moderne Kryptographie lorem ipsum

Ziele der Kryptographie

lorem ipsum

Methoden

lorem ipsum

2.2.3 Kryptoanalyse

lorem ipsum

Geschichte der Kryptoanalyse

lorem ipsum

Ziele der Kryptoanalyse

lorem ipsum

Methoden

lorem ipsum

2.2.4 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

2.3 E-Mail

lorem ipsum

2.3.1 Allgemein E-Mail und Notification

lorem ipsum

Senden

lorem ipsum

Graphische Erklärung lorem ipsum

Empfangen

lorem ipsum

IMAP lorem ipsum

POP lorem ipsum

2.3.2 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

2.4 Oberfläche

lorem ipsum

2.4.1 Allgemein User Interface (UI)

lorem ipsum

Geschichte

lorem ipsum

UIs

lorem ipsum

Zukünftig

lorem ipsum

2.4.2 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

2.5 Netzwerke

lorem ipsum

2.5.1 Grundlagen

lorem ipsum

Der Host

MAC-Adressen lorem ipsum

IP-Adressen lorem ipsum

Ports lorem ipsum

Schichtenmodell

lorem ipsum

OSI lorem ipsum

TCP/IP lorem ipsum

Client-Server Verhältnis

lorem ipsum

2.5.2 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

2.5.3 Netzwerksicherheit

lorem ipsum

2.6 Datenbank

lorem ipsum

2.6.1 Allgemeines

lorem ipsum

Geschichte

lorem ipsum

Definitionen

lorem ipsum

Effizienz

lorem ipsum

Funktionen

lorem ipsum

Anwendungen

lorem ipsum

2.6.2 Datenbanksysteme

lorem ipsum

Datenbankmanagementsysteme

lorem ipsum

Datenbank

lorem ipsum

2.6.3 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

2.6.4 Zugriffe

lorem ipsum

Zugriffsmöglichkeiten

lorem ipsum

Sicherheit

lorem ipsum

Gleichzeitige Zugriffe

lorem ipsum

2.6.5 Sprachen

lorem ipsum

Verwaltungsgetrennte Sprachen

lorem ipsum

Abfragen und Manipulieren der Daten lorem ipsum

Datenbankstruktur lorem ipsum

Berechtigungen lorem ipsum

SQL

lorem ipsum

2.6.6 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

Programmrealisierung

lorem ipsum

3.1 JobSystem

lorem ipsum

3.2 Notification

lorem ipsum

3.3 Database

3.3.1 MAD-DB

lorem ipsum

Erklärung

lorem ipsum

Grafische Übersicht

lorem ipsum

3.3.2 Programmcode

lorem ipsum

3.4 Logging

lorem ipsum

Kapitel 4

Abbildungsverzeichnis

lorem ipsum

Kapitel 5

Quellenverzeichnis

lorem ipsum