

Inhaltsverzeichnis

1	Einleitung und Motivation	13
1.1	Defizite bei der Konfiguration virtueller privater Netze (VPN)	13
1.2	Beiträge der Arbeit	16
1.3	Übersicht	16
2	Grundlagen: VPN-Konfiguration und strukturierte Peer-to-Peer-Systeme	19
2.1	Sicherheitsziele und Bedrohungen in paketorientierten Netzen	19
2.2	VPN-Szenarien	21
2.2.1	VPN von Firmen & Nichtregierungsorganisationen	21
2.2.2	VPN von Behörden und Militär	23
2.2.3	Privat eingesetzte VPN	24
2.3	Kryptographische Protokolle zur Absicherung von VPN	24
2.3.1	SSL, TLS und DTLS	24
2.3.2	Die IPsec-Protokollfamilie	25
2.3.3	Weitere kryptographische Protokolle	27
2.4	Strukturierte Peer-to-Peer Systeme	27
2.4.1	Verteilte Hash-Tabellen	28
2.4.2	SkipNet und Skip-Graphen	29
2.4.3	Peer-to-Peer-basierter Multicast	30
2.4.4	Netzwerkkoordinatensysteme	31
2.4.5	Spezielle Angriffe auf Peer-to-Peer-Systeme	32
3	Stand von Wissenschaft und Technik	35
3.1	Anforderungen an VPN-Autokonfigurationssysteme	35
3.1.1	Funktionale Anforderungen	35
3.1.2	Nichtfunktionale Anforderungen	37
3.1.3	Sicherheitsanforderungen	37
3.1.4	Anforderungen in Bezug auf die Verfügbarkeit	39
3.2	Existierende Systeme zur Autokonfiguration von VPN	41
3.2.1	Zentralisierte VPN-Konfigurationssysteme	42
3.2.2	Dezentrale VPN-Konfigurationssysteme	46
3.2.3	Vollständig verteilte VPN-Konfigurationssysteme	53
3.3	Overlay-Netze zur Steigerung von Robustheit und Verfügbarkeit	60
3.3.1	Robuste Overlay-Netze	60
3.3.2	Sabotageschutz von Netzwerkdiensten durch Overlay-Netze	61
3.4	Strukturierte Overlay-Netze für den Datentransport	61
3.4.1	Transport in Netzen mit garantierter, direkter Kommunikationsmöglichkeit	62

3.4.2	Indirekte Knotenanbindung durch Supernodes	62
3.4.3	Ansätze für Mobile Ad-hoc-Netze (MANET)	62
3.5	Fazit	64
4	Secure OverLay for IPsec Discovery (SOLID)	67
4.1	Grundlegende Prinzipien und Annahmen der VPN-Autokonfiguration	67
4.1.1	Netzstruktur	67
4.1.2	Annahmen	69
4.1.3	Kernfunktionen	69
4.1.4	Angreifermodell	70
4.2	Bootstrapping	71
4.3	Adresszuweisung	73
4.4	Discovery	74
4.4.1	Verteilte Datenbank oder direkte Abbildung	74
4.4.2	Struktur des Peer-to-Peer-Netzes	75
4.4.3	Querverbindungen auf Basis von Stichproben	76
4.5	Routing und Paketweiterleitung	82
4.5.1	Routing-Metrik	83
4.5.2	Routing-Mechanismen	84
4.5.3	Abkürzungsalgorithmen	85
4.5.4	Mechanismen zur Paketweiterleitung	89
4.5.5	Fazit	91
4.6	Topologiekontrolle	91
4.6.1	Divergenz zwischen Transportnetz- und VPN-Routing	92
4.6.2	Abhören von Kontrollinformationen zur Beschleunigung der Routing-Konvergenz	93
4.6.3	Overlay-Wiederherstellung nach Netzpartitionierungen	94
4.6.4	Anpassung an die Transportnetzumgebung	97
4.6.5	Fazit	99
4.7	Multicast-Routing	99
4.7.1	Topologien für die Verteilung von Multicast-Daten	99
4.7.2	Optimierungsmaßnahmen	101
4.8	Fazit	102
5	Betrachtungen zur Sabotageresistenz	103
5.1	Modellierung von VPN	103
5.2	Abschätzung der Bedrohung durch externe DoS-Angriffe	104
5.3	Schutz vor externen DoS-Angriffen	110
5.3.1	Optimale VPN-Topologien	110
5.3.2	Schutz durch Verfügbarkeitszonen	110
5.4	Schutz gegen interne DoS-Angriffe	118
5.4.1	Garantierte Vorhersagen der Grenzen interner DoS-Angriffe	119
5.4.2	Reaktive Regelung von Datenflüssen	120
5.5	Verfügbarkeitszonen in SOLID-VPN	121
5.5.1	Bootstrapping und Verbindungsaufbau	121
5.5.2	Topologiekontrolle und Routing	122

5.6	Fazit	123
6	Implementierung	125
6.1	Zusätzliche funktionale Anforderungen	125
6.2	Einbettung in Simulator & Prototyp	126
6.3	Überblick über die Software-Architektur	127
6.4	Bootstrapping	128
6.5	Adresszuweisung	131
6.6	Discovery und Topologiekontrolle	132
6.7	Routing und Paketweiterleitung	133
6.7.1	Eingesetzte Protokollarchitektur	134
6.7.2	Routing-Regeln und -Tabellen	135
6.7.3	Weiterleitung von Multicast-Verkehr	137
6.7.4	NAT-Traversal mit IKE-Mediation	137
6.8	Fazit	138
7	Evaluierung & Diskussion	141
7.1	Qualitative Diskussion	141
7.1.1	Umsetzung funktionaler Anforderungen	141
7.1.2	Nichtfunktionale Eigenschaften	143
7.1.3	Erfüllung der Sicherheits- und Verfügbarkeitsanforderungen	146
7.2	Quantitativ evaluierte Topologien und Szenarien	155
7.2.1	Struktur des Labornetzes	156
7.2.2	VPN mit direkter Konnektivität	156
7.2.3	Verschachtelte VPN-Topologien	157
7.2.4	Gewählte Standardparameter	157
7.3	Evaluierung des Prototypen	159
7.3.1	Reaktiver Aufbau von Sicherheitsbeziehungen	159
7.3.2	Erzeugter Verwaltungsaufwand	161
7.4	Netzwerksimulationen	162
7.4.1	Statische Overlay-Eigenschaften	162
7.4.2	Einfügen und Entfernen von Knoten	167
7.4.3	Verhalten bei Transportnetz-Partitionierungen	171
7.4.4	Verhalten bei partiellen Ausfällen	174
7.4.5	Sabotageresistenz	176
7.5	Fazit	183
8	Resümee	187
8.1	Zusammenfassung	187
8.2	Ausblick	189
A	Weiterführende Messungen	193
A.1	Verzögerung der IPsec-Schlüsselaushandlung	193
A.2	Häufigkeit der Verletzung der Dreiecksungleichung bei Verzögerungszeiten	194
	Literaturverzeichnis	195

Abkürzungsverzeichnis	213
Stichwortverzeichnis	215