

# **Sicherheit in Wireless LANs**

**von**

**Cornelius Höchel-Winter**

Inhaltsverzeichnis

<b><u>INHALTSVERZEICHNIS</u></b>		<b><u>I</u></b>
<b><u>1</u></b>	<b><u>MOTIVATION</u></b>	<b><u>1</u></b>
1.1	Gefährdungspotentiale von Funknetzen	3
1.1.1	Physikalische Aspekte	3
1.1.2	Netzwerktechnik	4
1.1.3	Übertragungstechnik	5
1.1.4	Betriebliche Aspekte	7
<b><u>2</u></b>	<b><u>DER STANDARD UND SEINE ERWEITERUNGEN</u></b>	<b><u>9</u></b>
2.1	Überblick	9
2.2	Frame Formate	12
2.3	Infrastruktur- und Ad-hoc-Modus	15
<b><u>3</u></b>	<b><u>SICHERHEITSTECHNIK AUF LAYER 2</u></b>	<b><u>17</u></b>
3.1	Der erste Wurf ...	17
3.1.1	WEP	17
3.1.2	Authentisierung	25
3.1.3	Verbindungsaufbau im WLAN	29
3.2	... war zu kurz	32
3.2.1	Angriffsszenarien	32
3.2.2	Tools	45
<b><u>4</u></b>	<b><u>DIE NEUEN SICHERHEITSSTANDARDS</u></b>	<b><u>50</u></b>
4.1	Ein erweiterter Anforderungskatalog	50
4.2	Die neuen Kryptografieverfahren	54
4.2.1	CCMP	54
4.2.2	TKIP	60
4.2.3	WPA	64
4.2.4	Vergleich der Frameformate	65
4.3	Authentisierung	66

4.3.1	IEEE 802.1X	66
4.3.2	802.1X-Integration in WLANs	73
4.3.3	Pre-Shared Keys	74
4.4	Schlüsselverwaltung	75
4.5	Robust Security Network	81
4.5.1	Scanning	83
4.5.2	Roaming	85
4.5.3	IEEE 802.11F	87
4.5.4	Sicherheitsklassen und Migration	91
4.6	Zusammenfassung des Frame-Austauschs	96

## **5 STRUKTURIERTE FUNKNETZE** **100**

5.1	Die Rolle des Distribution System	100
5.2	Distribution System hinter einer Firewall	105
5.3	Distribution System als VPN	107
5.4	Die Rolle des Clients	109
5.4.1	Notebooks	109
5.4.2	PDAs	110
5.4.3	Peripheriegeräte	111
5.4.4	Öffentliche WLANs	112
5.5	Fazit und Ausblick	113

## **ANHANG** **115**

A	Konstruktion eines gültigen CRC für gefälschte Frames	115
B	Detailprotokolle von Frame-Abfolgen	116
B.1	Anmeldung an einem „Open System“	116
B.2	Anmeldung an einem „Closed System“	126

## **ABBILDUNGSVERZEICHNIS** **136**

## **STICHWORTVERZEICHNIS** **139**

## **LITERATUR** **142**