Clemens Herrmann

Attacken auf die Sicherheitsmechanismen des Wi-Fi Protected Access Industriestandards

Diplomarbeit

GRIN

Bibliografische Information der Deutschen Nationalbibliothek:

Die Deutsche Bibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de/ abrufbar.

Impressum:

Copyright © 2009 GRIN Verlag
ISBN: 9783640307951

Clemens Herrmann

Attacken auf die Sicherheitsmechanismen des Wi-Fi Protected Access Industriestandards

GRIN Verlag

FH CAMPUS WIEN
UNIVERSITY OF APPLIED SCIENCES
> TECHNIK UND MANAGEMENT
DIPLOM-STUDIUM:
> INFORMATIONSTECHNOLOGIEN UND TELEKOMMUNIKATION

Diplomarbeit

Attacken auf die Sicherheitsmechanismen des WiFi Protected Access Industriestandards

ausgeführt am

Fachhochschul-Studiengang
Informationstechnologien und Telekommunikation

durch
Clemens Herrmann

Kurzfassung

In dieser Diplomarbeit werden die WLAN-Verschlüsselungsverfahren des „Wi-Fi Protected Access“-Industriestandards in ihrer Funktionsweise detailliert erklärt und auf ihre Sicherheit hin untersucht. Zahlreiche teilweise bisher unzureichend oder nur spärlich dokumentierte Angriffe auf RC4-basierte WLAN-Sicherheitsverfahren werden genau beschrieben. Weiters wird auch ein Ansatz für eine neuartige Angriffsstrategie auf WiFi Protected Access präsentiert, welche mit vorberechneten Tabellen arbeitet. Es fanden sich Methoden, die Größe der dafür notwendigen Wertetabelle stark zu reduzieren und dadurch die theoretische Durchführbarkeit eines derartigen Angriffes zu erleichtern. Die effizientesten der erläuterten Attacken wurden in einer Testumgebung praktisch durchgeführt. Abschließend werden verschiedene Vorkehrungen zum Schutz vor Bedrohungen aufgelistet. Die Arbeit richtet sich sowohl an mit der Thematik nur eingeschränkt vertraute LeserInnen, als auch an IT-SicherheitsexpertInnen.

Abstract

In this thesis the security of cryptographic techniques of the WiFi Protected Access industry standard for WLANs is investigated. The functionality of RC4-based security mechanisms is explained in detail. Various vulnerabilites and attacks on these mechanisms are described, some of which could not found to be sufficiently documented before. A theoretical scenario for a novel attack strategy on WiFi Protected Access is presented, which operates with tables of pre-computed values as a base for an attack. Measures were found to reduce the size of charts necessary and thus facilitating the theoretical feasibility of such an attack. The most efficient of the discussed attacks are executed in a test environment. To conclude, different measures for threat protection are specified. The thesis is directed both at readers whose familiarity with the subject area is limited and at IT-security experts.

Abkürzungsverzeichnis

AAD	Additional Authentication Data
ACS	Access Control Server
AES	Advanced Encryption Standard
AP	Access Point
ARP	Address Resolution Protocol
ASCII	American Standard Code for Information Interchange
BSSID	Basic Service Set Identifier
CBC-MAC	Cipher Block Chaining – Message Authentication Code
CCMP	Counter Mode With Cipher Block Chaining – Message Authentication Code Protocol
CHAP	Challenge Handshake Authentication Protocol
CM	Counter Mode
CRC	Cyclic Redundancy Check
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DoS	Denial of Service
EAP	Extensible Authentication Protocol
EAP-FAST	EAP-Flexible Authentication via Secure Tunneling
EAPoL	Extensible Authentication Protocol over Local Area Networks
EIV	Extended Initialization Vector
ESSID	Extended Service Set Identifier
FCS	Frame Check Sequence
FMS	Fluhrer-Mantin-Shamir
GMK	Groupwise Master Key
GTK	Groupwise Transient Key
HEX	Hexadecimal
IAS	Internet Authentication Service
ICV	Integrity Check Value
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
IPX	Internetwork Packet Exchange
IV	Initialization Vector
KSA	Key Scheduling Algorithmus
LAN	Local Area Network
LEAP	Lightweight Extensible Authentication Protocol

MAC	Media Access Control
MD5	Message Digest 5
MIC	Message Integrity Code
MPDU	Media Access Control Protocol Data Unit
MSB	Most Significant Bit
MSDU	Media Access Control Service Data Unit
NIC	Network Interface Card
NIST	National Institute for Standards and Technology
PEAP	Protected Extensible Authentication Protocol
PMK	Pairwise Master Key
PN	Packet Number
PPK	Per-Packet Key
PPP	Point-to-Point Protocol
PRNG	Pseudo-Random Number Generator
PSK	Pre-Shared Key
PTK	Pairwise Transient Key
PTW	Pyshkin-Tews-Weinmann
QoS	Quality of Service
RADIUS	Remote Authentication Dial-In User Service
RC4	Ron's Code 4
SNAP	Sub-Network Access Protocol
SSID	Service Set Identifier
SSL	Secure Socket Layer
TCP	Transmission Control Protocol
TID	Traffic Identifier
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
TMTO	Time-Memory Tradeoff
TTLS	Tunneled Transport Layer Security
VAP	Virtual Access Point
WEP	Wired Equivalent Privacy
Wi-Fi	Wireless Fidelity
WLAN	Wireless Local Area Network
WPA	WiFi Protected Access

Schlagwörter

WLAN-Sicherheit
IT-Security
WEP
WPA
WPA2
802.11i
WPA tabellarischer Angriff

Inhaltsverzeichnis