# DiscoSec: Ein leichtgewichtiges, DoS-resistentes Security Service Pack für IEEE 802.11 Netze

## Beitrag für den Communications-Software-Preis

Matthias Wilhelm, Paul Pichota
Betreuer: Ivan Martinovic und Jens B. Schmitt

{m_wilhel,p_pichot,martinovic,jschmitt}@cs.uni-kl.de

Distributed Computer Systems Lab (disco)
Technische Universität Kaiserslautern

---

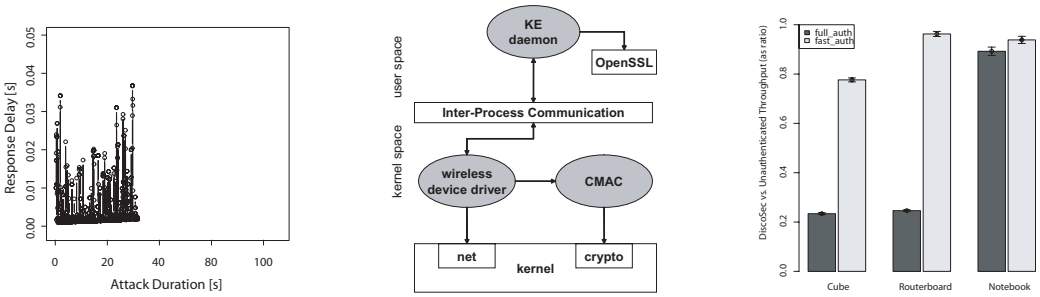
**Zusammenfassung** *DiscoSec* bietet also erster Open-Source WLAN-Treiber Schutz vor einer Vielzahl von weitverbreiteten Angriffen gegen den IEEE 802.11 MAC Layer. Durch ein innovatives Design mit Fokus auf Leistungsfähigkeit sowie einer effizienten Implementierung konnten die zunächst widersprüchlichen Zielsetzungen von Leistung und Sicherheit vereint werden. Das System bietet so einen verlässlichen Schutz von Drahtloskommunikation von Beginn an, ohne auf einen hohen Durchsatz verzichten zu müssen.

## 1 Praxisrelevanz der Software

Drahtlose Netze sind durch ihre besonderen Eigenschaften verwundbarer gegen böswillige Angreifer als kabelgebundene Systeme. Zu diesen Besonderheiten zählen unter anderem die Broadcast-Natur des Mediums, durch die jeder in Reichweite die Kommunikation abhören und auch eigene Nachrichten einbringen kann, wie auch der zentralen Verwaltungsinstanz eines Netzes im Infrastrukturmodus, dem Access Point ($AP$), dessen Funktionsfähigkeit sicherheitskritisch ist. Durch Designfehler im 802.11 Protokoll sind diese Merkmale leicht angreifbar. So kann aufgrund mangelndem Schutz die Urheberadresse eines Frames gefälscht werden, wodurch die Verwaltungsfunktionen effektiv angegriffen werden können, von einfachen Flooding-Attacken bis hin zu mehrstufigen Angriffen wie z.B. Rogue APs [2].

Der bekannte Standard IEEE 802.11i [1] widmet sich dem Problem der Vertraulichkeit und Entitäten-Authentizität von Nachrichten. Eine Reihe von bekannten Angriffen wird aber von diesem Standard nicht behandelt. Besonders kritisch ist der weiterhin fehlende Schutz von Management-Diensten und damit vor allem die Möglichkeit von Angriffen gegen die Verfügbarkeit von Access Points. Hier zu nennen sind Denial of Service (DoS) Angriffe, die darauf zielen einzelne Funktionen oder gar die komplette Funktionsfähigkeit des APs zu beeinträchtigen (siehe Abbildung 1a), sowie einer Reihe von Impersonifikationsattacken, deren Auswirkungen von der Unterbrechung von Verbindungen bis hin zum Brechen von weiteren Sicherheitszielen wie Authentizität oder Vertraulichkeit reichen. Für diese Problematik soll der Standard IEEE 802.11w Verbesserung bringen, aber die Verabschiedung dieses Standards ist erst für Dezember 2009 geplant[1].

[1] http://www.ieee802.org/11/Reports/802.11_Timelines.htm




(a) DoS-Attacke (b) Architektur (c) Leistungsbetrachtung

Abbildung 1: Teil (a) zeigt die Auswirkungen einer DoS-Attacke auf einen Access Point, der so bereits nach kurzer Zeit keinerlei Dienste mehr erbringen kann. Teil (b) stellt die Systemarchitektur von DiscoSec dar. Teil (c) zeigt die experimentellen Ergebnisse auf verschiedenen Hardwareplattformen (324MHz MIPS, 266MHz bzw. 1333MHz x86).

Diese Lücke füllt DiscoSec [3]. Durch die Verwendung unseres verbesserten Treibers für WLAN-Geräte werden zwischen den teilnehmenden Stationen und dem Access Point gemeinsame Schlüssel ausgehandelt, die es ermöglichen, die rechtmäßige Urheberschaft eines gesendeten Frames zu beweisen. Dadurch kann das Vertrauen in die Authentizität des Frames wiederhergestellt werden und ein Angreifer hat keine Möglichkeit mehr unter falschem Namen in die Kommunikation einzugreifen, was die gefährlichsten Attacken auf heutige 802.11 Netzwerke entschärft. DiscoSec ist der erste voll funktionsfähige Treiber für WLAN-Geräte, der diesen Schutz bietet und der auch auf kommerziell erhältlichen Standardplattformen für Access Points betrieben werden kann. Der Betrieb erfolgt völlig transparent, also ohne Interaktion des Benutzers, nur die Installation des Treibers ist notwendig um die Kommunikation zu schützen.

## 2 Neuigkeit und Verbesserungswert

Durch eine auf Leistung ausgerichtete Architektur und Implementierung bietet DiscoSec Sicherheit ohne auf Performanz verzichten zu müssen. Dieser Schutz ist kombinierbar mit anderen Sicherheitsmechanismen wie z.B. 802.11i, dessen aufwendige Initialisierung mit DiscoSec effektiv geschützt werden kann. Experimente mit dem verbesserten Treiber zeigen, dass auch auf handelsüblicher, leistungsschwacher Hardware ein effektiver Schutz möglich ist (siehe Abbildung 1c). So liegt die Abnahme des Durchsatzes bei unseren Messungen für schwache Hardware bei nur 22%, für Access Points mit mehr Rechenleistung liegt dieser Wert sogar bei nur 6%. Dies wird durch die Verwendung von performanten und bewährten Sicherheitsbausteinen wie Linux Crypto API oder OpenSSL erreicht, sowie der hardwarenahen Implementierung, die direkt im Kernel durchgeführt wurde. Neue kryptographische Primitive wie ein auf elliptischen Kurven basierender Diffie-Hellman Schlüsselaustausch (*ECDH* [4]) oder Message Authentication Codes unter Verwendung des AES Blockciphers (*AES-CMAC* [5]) wurden mit verschiedenen Alternativen evaluiert und aufgrund ihrer Leistungsfähigkeit ausgewählt.

Zu den bereitgestellten Schutzfunktionen zählen die Urheber-Authentisierung von Management Frames auf Grundlage des Headers (*fast_ auth*) oder des ganzen Frames (*full_ auth*),

sowie der Schutz vor Wiedereinspielung von aufgezeichneten Nachrichten (replay protection) und die verbesserte Fairness bei der Anmeldung zum Netzwerk. Der Zustandsautomat von IEEE 802.11 erfährt keine strukturellen Veränderungen, nur die bereits im Protokoll definierten Nachrichten werden durch Sicherheitsinformationen erweitert. So bleibt unser System komplett kompatibel zum Standard und damit auch zu bereits im Betrieb befindlichen Netzinfrastrukturen. Durch eine modulare Architektur (die in Abbildung 1b dargestellt ist) kann DiscoSec leicht an zukünftige Erfordernisse und Entwicklungen angepasst werden. Des Weiteren stehen den Betreibern von Access Points eine Vielzahl von Parametern und Konfigurationen zur Verfügung, um das Softwaresystem an ihre Erfordernisse und Möglichkeiten anzupassen. So kann z.B. der Schlüsselaustausch vom Access Point auf eine leistungsstärkere Maschine im drahtgebundenen Backbone des Netzes ausgelagert werden, um eine größere Zahl von Anmeldungen pro Sekunde zu ermöglichen.

## 3 Organisatorisches, Verfügbarkeit und Systemvorraussetzungen

Bei dieser Arbeit handelt es sich um eine studentische Gruppenarbeit (Projektarbeit), die an der AG Verteilte Systeme der Technischen Universität Kaiserslautern von zwei Studenten innerhalb eines Semesters erarbeitet wurde. Der Quellcode ist offen und zum Download erhältlich unter der Adresse *disco.cs.uni-kl.de/content/downloads*.

In der aktuellen Version benötigt DiscoSec ein Linux-System mit einer minimalen Kernelversion von 2.6.14, um von den neu in den Kernel eingeflossenen kryptographischen Primitiven zu profitieren. OpenSSL wird mindestens in Version 0.9.8 für ECDH-Unterstützung benötigt. Da DiscoSec auf MadWifi Version 0.9.2 basiert werden im Moment nur WLAN-Geräte mit Atheros-Chipsatz unterstützt, die zu dieser Version kompatibel sind[2]. Die Software wurde unter der x86 sowie der MIPS-Rechnerarchitektur getestet, prinzipiell kann DiscoSec auf allen Plattformen betrieben werden, auf denen die hier genannten Softwarekomponenten zur Verfügung stehen.

## Literatur


1. IEEE 802.11i/D10.0. Security Enhancements, Amendment 6 to IEEE Standard for Information Technology. IEEE Standard, April 2004.
2. J. Bellardo and S. Savage. 802.11 Denial-of-Service attacks: Real Vulnerabilities and Practical Solutions. In *Proceedings of the USENIX Security Symposium*, pages 15–28, August 2003.
3. I. Martinovic, P. Pichota, M. Wilhelm, F. A. Zdarsky, and J. B. Schmitt. Design, Implementation, and Performance Analysis of DiscoSec – Service Pack for Securing WLANs. In *9th IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (WOWMOM 2008)*, Newport Beach, CA, USA, June 2008.
4. SECG. Elliptic Curve Cryptography, Standards for Efficient Cryptographic Group. Available at www.secg.org/collateral/sec2.pdf, (last accessed 13.03.2008).
5. J. Song, R. Poovendran, J. Lee, and T. Iwata. The AES-CMAC Algorithm. RFC 4493 (Informational), June 2006.


[2] Eine Liste ist abrufbar unter http://madwifi-project.org/wiki/Chipsets