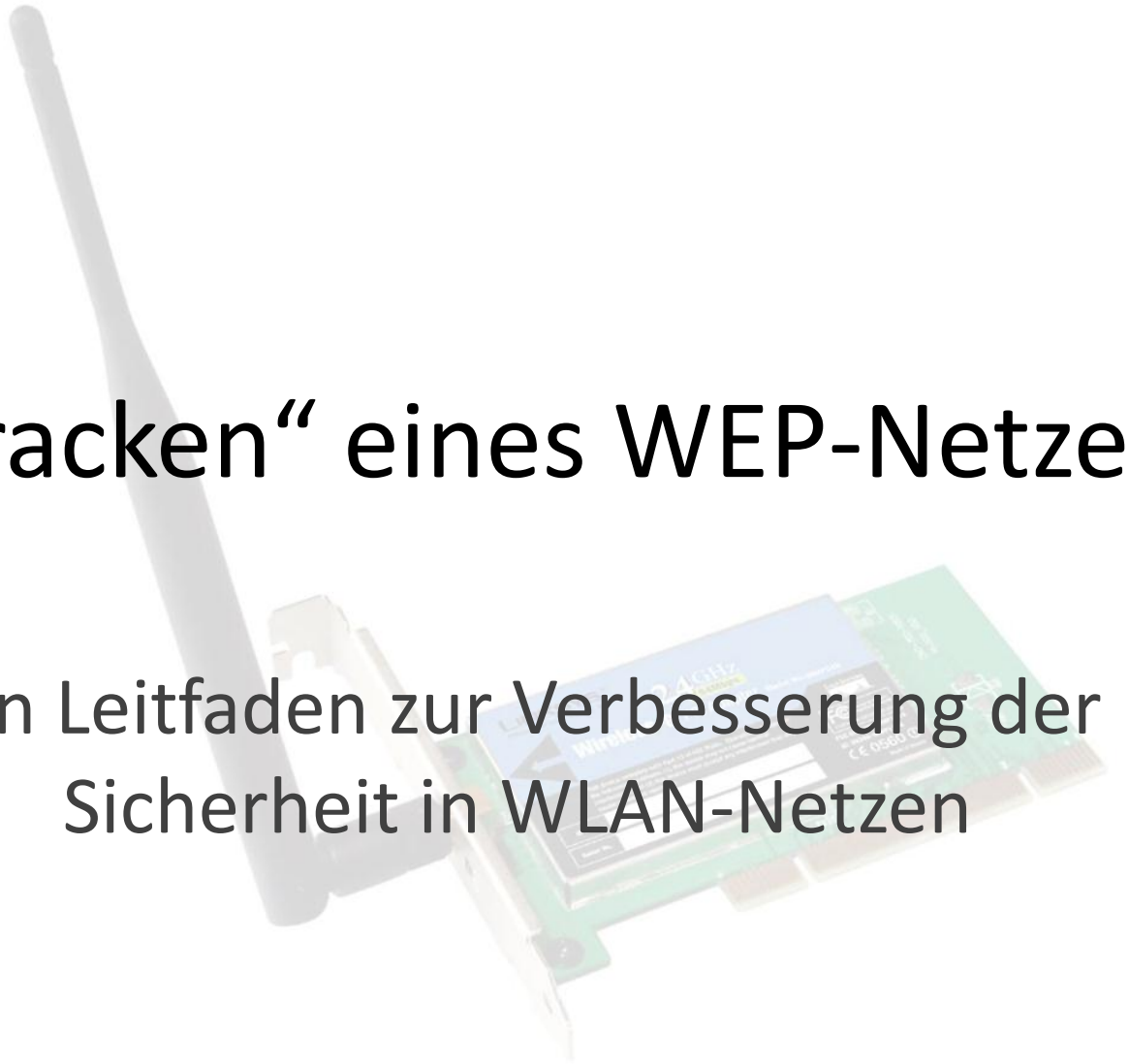


„Cracken“ eines WEP-Netzes

Ein Leitfaden zur Verbesserung der Sicherheit in WLAN-Netzen

2010 By Christian Stankowic, http://www.stankowic-development.net.

Rechtssauschluss

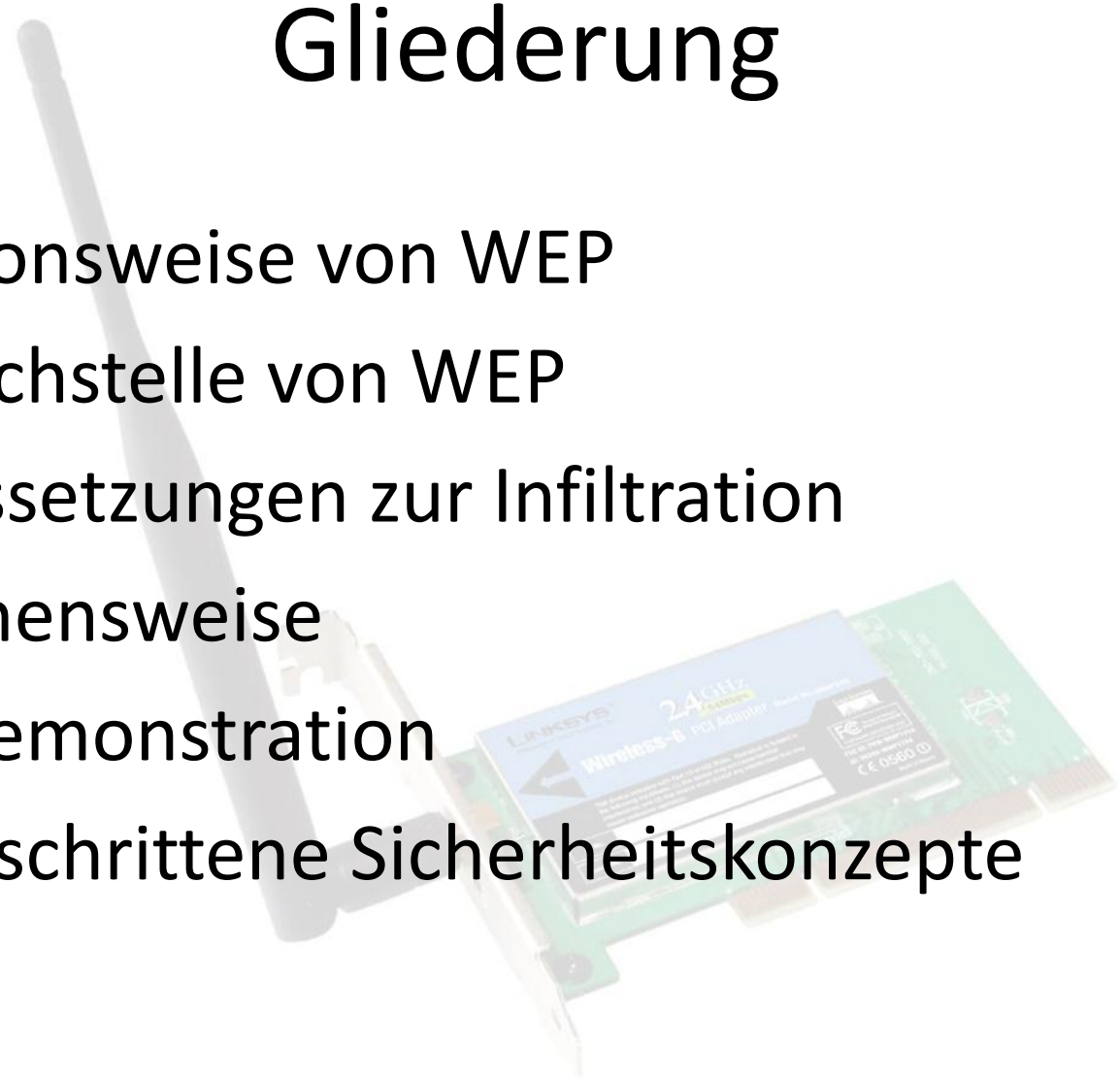
Die folgenden Informationen können für illegale Zwecke missbraucht werden. Legal ist das später geschilderte Vorgehen nur für Sicherheitschecks am eigenen Netzwerk – oder auch an fremden Netzwerken, sofern eine schriftliche Erlaubnis vorliegt.

Das unautorisierte Angreifen von Netzwerken ist eine Straftat und wird zivilstrafrechtlich verfolgt. Das Bestrafungskonzept reicht von Geld- bis hin zu Freiheitsstrafen.

2010 By Christian Stankowic, http://www.stankowic-development.net.

Gliederung

- Funktionsweise von WEP
- Schwachstelle von WEP
- Voraussetzungen zur Infiltration
- Vorgehensweise
- Live-Demonstration
- Fortgeschrittene Sicherheitskonzepte



2010 By Christian Stankowic, http://www.stankowic-development.net.

Funktionsweise und Schwachstelle von WEP

2010 By Christian Stankowic, http://www.stankowic-development.net.

Authentifizierung

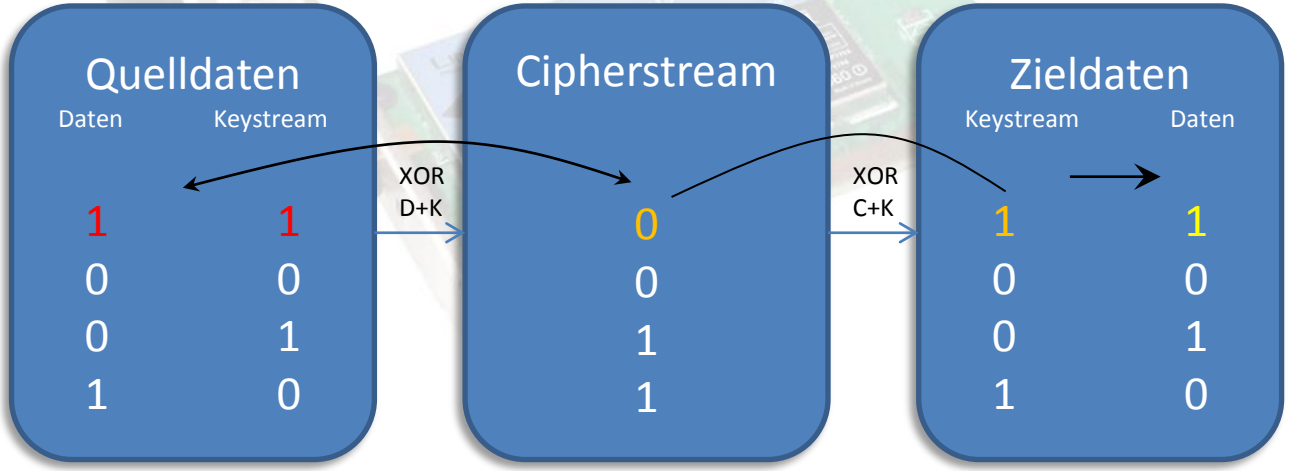
- ***Open System Authentification***
  - Key wird zur Verschlüsselung der Nachrichten und zur Authentifizierung genutzt
  - Stimmt der Key nicht, ist eine Kommunikation mit dem Netzwerk nicht möglich
- ***Shared Key Authentification***
  - Authentifizierung über Challenge-Response mit geheimen Schlüssel
  - Stimmt das Ergebnis → Authentifizierung erfolgreich

2010 By Christian Stankowic, http://www.stankowic-development.net.

Funktionsweise

- XOR-Verknüpfung des Nutzstroms mit einem zufälligen Datenstrom (*RC4-Algorithmus*)
- Ein generierter 24bit-Initalisierungsvektor verknüpft mit dem Schlüssel, berechnet mit RC4 ergibt den Keystream

A	B	XOR
0	0	0
0	1	1
1	0	1
1	1	0



2010 By Christian Stankowic, http://www.stankowic-development.net.

Schwachstelle

- Zu kurzer Initalisierungsvektor (*24 bit*)
- Durch das Sammeln von Paketen können schnell aus IVs der Key gewonnen werden
- Auch bei *Shared Key Authentification* leicht eine Authentifizierung möglich, da Challenge, IV und Response leicht mitgeschnitten werden können.

2010 By Christian Stankowic, http://www.stankowic-development.net.

Voraussetzungen zur Infiltration

- Ein Client im Netzwerk – zum Auslesen und „*re-injecten*“ eines ARP-Requests
- Informationen zum Netzwerk: BSSID, ESSID und Kanal des WLAN-Netzwerkes
- WLAN-Karte mit im Treiber implementierter Monitoring-/Promiscous Mode- und Injection-Funktionalität
- Installiertes Linux mit *aircrack-ng* / *Backtrack*

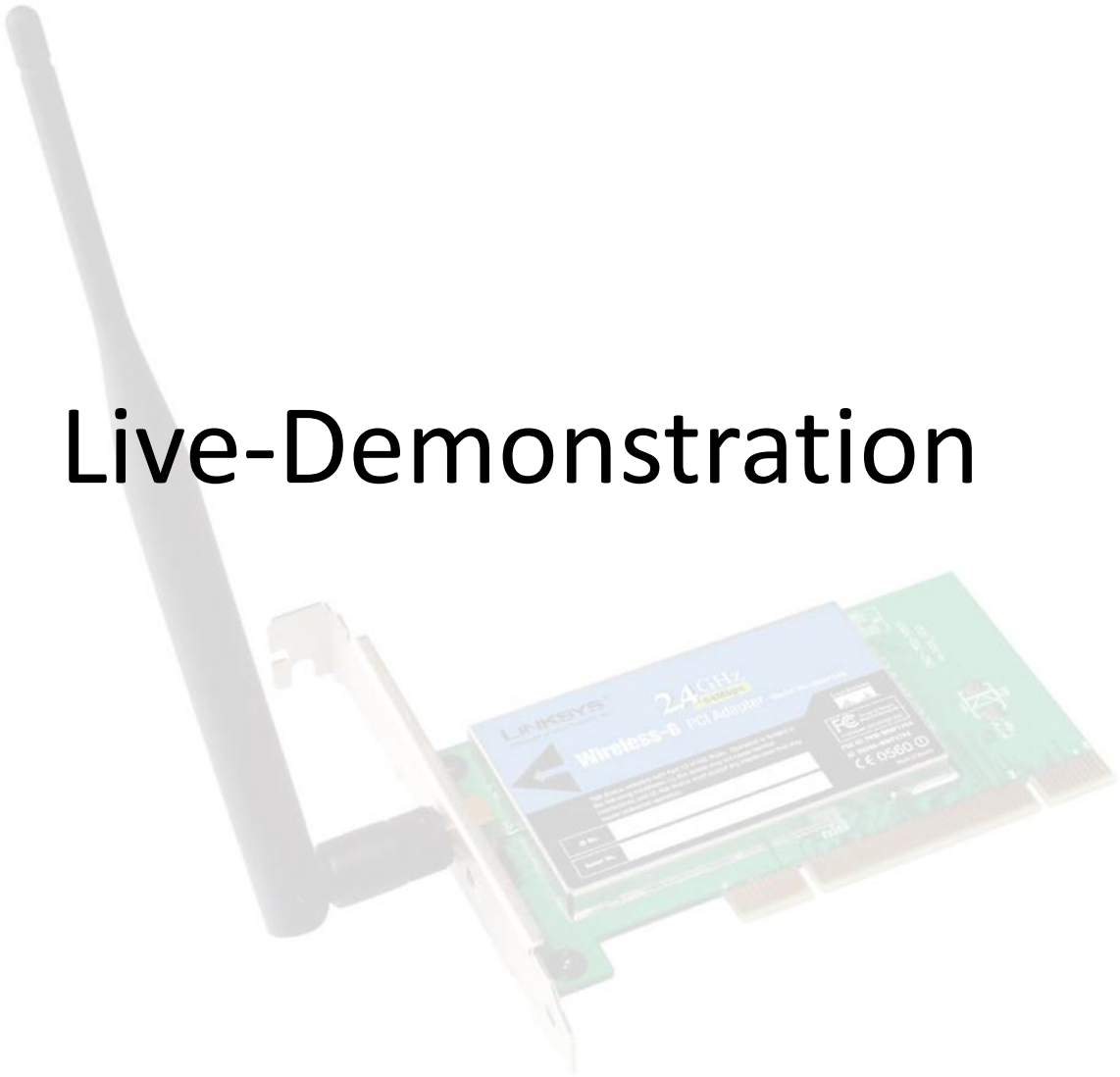
2010 By Christian Stankowic, http://www.stankowic-development.net.

Vorgehensweise

1. Monitoring-Modus aktivieren um gesamten Netzverkehr „*mitzuhören*“ → Netz erforschen
2. Injections erproben
3. Authentifizierung vortäuschen (*ggf. MAC-Filter umgehen*)
4. Sammeln von Initalisierungsvektoren (*IVs*), Beschleunigung durch Injection von ARPRs
5. Cracken des Keys durch Berechnung mithilfe der gesammelten IVs

2010 By Christian Stankowic, http://www.stankowic-development.net.

Live-Demonstration



2010 By Christian Stankowic, http://www.stankowic-development.net.

Fortgeschrittene Sicherheitskonzepte

- WPA2-Verschlüsselung (*AES-basierend*)
- Möglichst langer Pre-Shared Key mit vielen Sonderzeichen und Zahlen-/Buchstaben-Kombinationen - oder besser: **RADIUS-Server**
- Authentifizierung mittels EAP
- Access-Point mit Einbruchsdetektierung (*IDS*)
- **…oder am besten gar kein WLAN ☺**

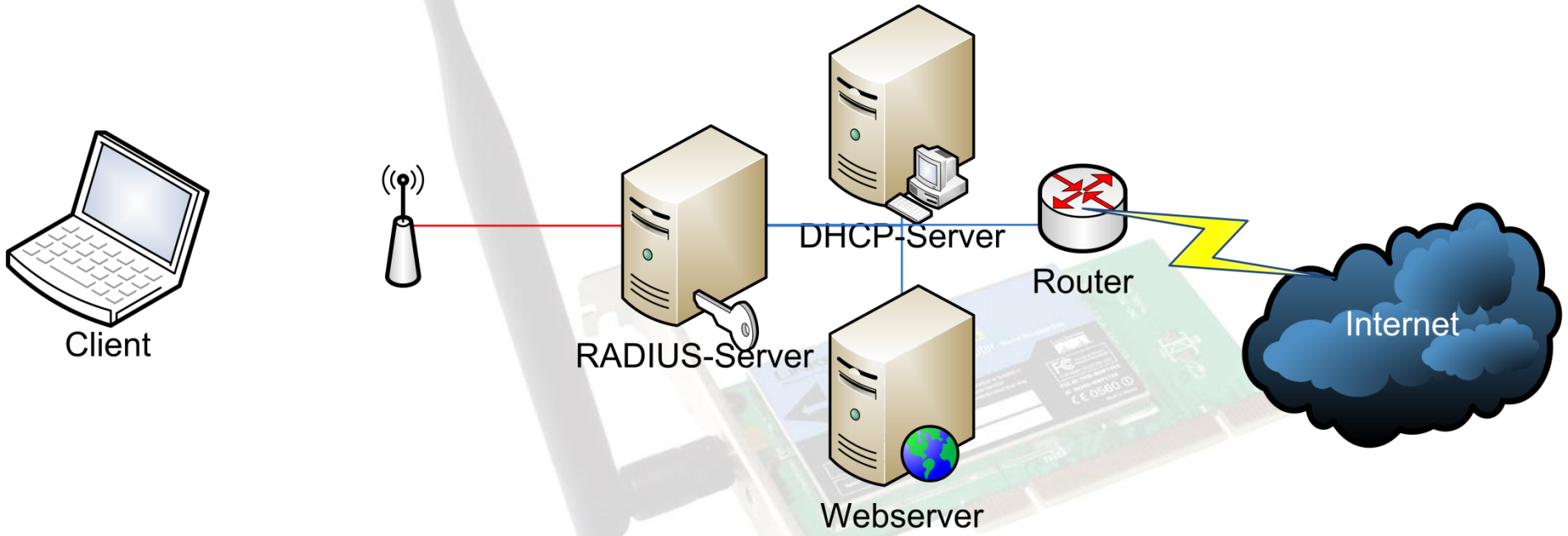
2010 By Christian Stankowic, http://www.stankowic-development.net.

RADIUS-Server

- **Remote Authentification Dial-In User Service**
- Client-Server-Protokoll zur Authentifizierung für Einwahl-Verbindungen, ermöglicht Zugangsmanagement
- Unterstützt ISDN, VPN, Modem und WLAN
- Möglichkeiten: Benutzerdefinierter Key für Benutzer, automatische Konfiguration der Clients, an LDAP/AD koppelbar,…

2010 By Christian Stankowic, http://www.stankowic-development.net.

Beispielaufbau



2010 By Christian Stankowic, http://www.stankowic-development.net.

Internetverweise

- http://www.aircrack-ng.org – Aircrack Software-Suite, Download und Informationen
- http://www.backtrack-linux.org – Backtrack Linux Live-CD mit zahlreichen Sicherheitsutilities
- http://wiki.christian-stankowic.de/doku.php?id=computer:netzwerk:wep-key_knacken – Ausführlicher Artikel zur Thematik auf meinem Wiki

2010 By Christian Stankowic, http://www.stankowic-development.net.

Vielen Dank für Ihre/Eure Aufmerksamkeit

2010 By Christian Stankowic, http://www.stankowic-development.net.