

# Sécurité wireless

# **1 Wi-Fi**

## ***1.1 Matériel & usage***

## ***1.2 Normes Wi-Fi***

## ***1.3 Les modes de fonctionnement***

## ***1.4 Configuration de clients ou de points d'accès sous Linux***

## ***1.5 Protocoles de sécurisation***

### **1.5.1 WEP**

### **1.5.2 WPA**

### **1.5.3 WPA2**

## ***1.6 Attaques***

### **1.6.1 Sniffing**

### **1.6.2 Spoofing**

### **1.6.3 Injection de trafic**

### **1.6.4 Flood & attaques radio**

### **1.6.5 Attaques sur les PSK**

## ***1.7 Sécurisation***

### **1.7.1 Sécurisation physique**

### **1.7.2 Visibilité du réseau**

### **1.7.3 Filtrage par adresse MAC**

### **1.7.4 Chiffrement**

## 1.7.5 Authentication 802.1x

## **2 Bluetooth**

### ***2.1 Matériel & usage***

### ***2.2 Pile protocolaire***

### ***2.3 Modes de communication & Topologies réseau***

### ***2.4 Protocoles usuels***

#### **2.4.1 HCI**

#### **2.4.2 L2CAP**

#### **2.4.3 RFCOMM**

#### **2.4.4 SDP**

#### **2.4.5 OBEX**

### ***2.5 Audit Bluetooth***

#### **2.5.1 Prises d'information HCI & SDP**

#### **2.5.2 Scan RFCOMM**

### ***2.6 Attaques & sécurisation***

#### **2.6.1 Blueprinting**

#### **2.6.2 Snarfing**

#### **2.6.3 BlueBug**

#### **2.6.4 BlueSmack**

## **3 GSM**

### ***3.1 Matériel & usage***

### ***3.2 Infrastructure GSM***

#### **3.2.1 Terminaux**

#### **3.2.2 BTS**

#### **3.2.3 BSC**

#### **3.2.4 HLR**

#### **3.2.5 VLR**

### ***3.3 Protocoles radio***

#### **3.3.1 Canaux**

#### **3.3.2 Authentification**

#### **3.3.3 Chiffrement**

### ***3.4 Attaques & sécurisation***

#### **3.4.1 Géolocalisation**

#### **3.4.2 Déni de service**

#### **3.4.3 Ecoute**

#### **3.4.4 Spoofing & redirection**

## **4 RFID**

### ***4.1 Matériel & usage***

### ***4.2 Normes ISO***

#### **4.2.1 ISO 14443 A & B**

#### **4.2.2 ISO 15693**

### ***4.3 Protocoles standards***

#### **4.3.1 HID**

#### **4.3.2 Mifare**

#### **4.3.3 Felica**

### ***4.4 Attaques & sécurisation RFID***

#### **4.4.1 Lecture distante**

#### **4.4.2 Attaques par relai**

#### **4.4.3 Emulation lecteur ou tag**

#### **4.4.4 Attaques cryptographiques**