



PO Box 64070  
Highlands North  
2037  
admin@telspace.co.za  
Landline Telephone: (011) 875-4319  
Fax: (011) 802-6683

**Telspace Systems Wireless Security Training – Bluetooth and Wireless Hacking 101**

Dear Client

Due to popular demand from our clients, Telspace Systems has decided to introduce ethical hacking training courses to South Africa on IT Security topics, ranging from Wireless and Bluetooth Hacking through to Web Application Hacking.

We would like to invite you to participate in our training session on the 25th and 26th February 2009.

Please find the training details in the below document, detailing Wireless and Bluetooth Hacking 101. Wireless Hacking will be held on Day 1, while Bluetooth Hacking will be held on Day 2.

Telspace Systems provides very practical and hands-on training sessions. We only have space for approximately 15 applicants during each training session, which allows for a more personal training atmosphere. Therefore, it is best to book early for guaranteed availability.

As of yet, the venue has not yet been confirmed, but will be in due course.

The total cost for the 2-day training on Hacking Wireless and Bluetooth 101 is R7490 excluding VAT per person. This includes training, course material, lunch, coffee and tea breaks.

If you have any queries regarding this specific training course, please feel free to contact us.

Kind regards

Ilva Pieterse  
Telspace Systems  
Sales Director  
Web: [www.telspace.co.za](http://www.telspace.co.za)  
Office: 011-875-4319  
Cell: 082-556-8529  
Email: [ilva@telspace.co.za](mailto:ilva@telspace.co.za)

## **Introduction to Telspace Systems**

Telspace Systems provides top level IT security solutions in various sectors locally and internationally.

Telspace Systems has, and always will, focus on vendor independent reporting. We also pride ourselves in being one of the only IT security companies in South Africa to present at international level.

Our client database is broad and includes companies in many different industries.

A few of the organisations and companies that we have serviced include:

- Various South African government departments
- Banking institutions
- Telecommunications providers throughout Africa
- Petroleum and logistics companies
- Mining institutions
- Radio stations and broadcasting companies
- Various airlines worldwide
- South African law firms
- Recruitment companies
- Internet service providers

### **Oday advisories**

Telspace Systems also regularly releases brand new (0day) IT security advisories as part of the “give back to open source” scheme. This is IT Security innovation at its best. A few of our releases include:

- Serious vulnerabilities in Article Dashboard
- Serious vulnerabilities in Iware Professional
- Various commercial software flaws found by Telspace Systems Research
- ActiveX component vulnerabilities

All of our research and releases are co-ordinated with the vendor and are part of a responsible disclosure effort.

### **BEE connections**

Telspace Systems also maintains strategic partnerships with BEE companies, such as Business Connexion Namibia, which allows us to expand through Africa and service the needs of clients throughout Africa. More about this agreement can be obtained at <http://www.telspace.co.za/press-020.php>

## Telspace Systems Competence and Exposure

Telspace Systems regularly presents at high level government and internationally-recognised security conferences. We are often interviewed locally and internationally by magazines, radio, television and newspapers.

A few of our latest (2007/2008) include:

- *702 Talk Radio* – David O’Sullivan’s morning show addressing the Government’s R400 million loss to cybercrime in 2008 – **interviewee**
- *Classic fM* – The Internet Economy with Reuben Goldberg – **interviewee**
- *SecTor 2008* – Toronto, Canada – **speaker and trainer**
- *ITWeb Security Summit 2008* – Johannesburg, South Africa – **speaker**
- *Hack in the Box 2008* – Dubai – **speaker and trainer**
- *SecTor 2007* – Toronto, Canada – **speaker**
- *The Truth Behind Big Screen Hacks* – BBC TV “Click” – **interviewee**
- *Hack In the Box 2007* – Dubai, UAE – **speaker** – (<http://conference.hitb.org/>)
- *Hack In the Box 2007* – Kuala Lumpur, Malaysia – **speaker**
- *iWeek magazine* – **regular writer** – ([www.iweek.co.za](http://www.iweek.co.za))
- *PMR Africa* (government magazine) – **regular writer**
- *CEO magazine* – **author**
- *ITWeb Industry Insights (2007/2008)* – **author**
- Local and international newspapers (Sunday Times, New Strait times etc) – **regular writers**
- *Mobileworld magazine* – Malaysia – Hacking the Bluetooth Stack
- *Combating Cybercrime in the SADC Region* – CESPAM Executive Training Programme – Cape Town – **speaker**
- *Business Zone* – International Cyber Terrorism – **speaker**
- *Information Security Practice* – Information Security workshop – **presenter**
- *Combating Financial Crimes in Africa* – Marcus Evans – **speaker**
- Published in various local and international websites such as Secunia (<http://secunia.com/>)

### **Training courses:**

Telspace Systems also offers a range of training courses that have been presented all around the world as well as locally:

- Bluetooth & Wireless Hacking 101
- Hands on Hacking Unlimited in conjunction with Zone-h
- Web Application Hacking 101

## Wireless and Bluetooth Hacking 101

### **Training brief:**

Wireless networks are continually growing in our modern world and society.

This 2-day course aims to demystify wireless network security and inform attendees on how to improve wireless LAN security and Bluetooth security.

This will be achieved via theory and practical. Attendees will first obtain detailed theoretical analysis of different wireless security schemas (i.e. Theory), thereafter have hands on experience in how the attacks are performed (i.e. practical).

Attendees will also be issued with challenges in the form of wireless hacking.

### **Who should attend this course?**

- General IT security specialists and administrators
- IT security specialists who are interested in Wireless hacking specifically
- Security Officers for organizations and companies
- Wireless Network Administrators
- Any individual who may be interested in these topics

### **Contents of the course:**

- Introduction to Wireless Hacking
- Wireless Protocols and Architecture
- Network Mapping
- Methodology for securing wireless networks
- Wireless hacking tools and attacks
- Defending against wireless hacking
- Introduction to Bluetooth
- Bluetooth vulnerabilities overview
- Bluetooth hacking tools and techniques
- Defending against Bluetooth attacks

### **Course Duration – 2 Days**

#### **Prerequisites:**

Basic knowledge of Wireless networks.

Participants must bring their own laptop with CDROM device (N.B for bootable software).

Participants must have administrative rights to install software on their laptop.

## **Day 1 Breakdown – Wireless Hacking – 25 February 2009**

### **Introduction to Wireless Hacking:**

- Wireless and its technology usage
- Wireless networking breakdown
- Security of wireless and progression
- What is wardriving?
- Attacking wireless brief

### **Wireless Protocols and Architecture:**

- Analysis of various wireless protocols
- Wireless architecture and design
- 802.11 Protocol Analysis

### **Network Mapping and Methodology for securing wireless networks:**

- Discovery of wireless networks
- Antenna variations
- Monitoring the wireless network, including packet analysis
- Various toolsets including Netstumbler, Kismet, the Aero suites and so forth

### **Wireless hacking tools and attacks:**

- Traffic injection tools
- Spoofing
- Flooding
- Aircrack and Aero suite of tools
- Airsnort
- WEP hacking cracking
- WPA, WPA2 hacking techniques
- Frame generation
- Defeating MAC Filtering
- Fake access points
- Other attacks

### **Defending against wireless hacking:**

- Site layout and planning
- Improving your wireless systems against hacker attacks
- Filtering

## Day 2 – Breakdown – Bluetooth Hacking – 26 February 2009

### Introduction to Bluetooth:

- What is Bluetooth?
- What does it allow for?
- How Bluetooth works
- Bluetooth data rates
- Bluetooth ranges and specifications
- Introduction Bluetooth security (Scatternets)
- Latest developments with Bluetooth

### Bluetooth vulnerabilities overview:

- The Snarfing attack
- The Bluebug attack
- The backdoor attack
- Bluechop
- Bluedump
- Bluebump
- Bluesmack
- The social engineering factor
- Bluetooth viruses
- Bluetooth implementation problems

### Bluetooth hacking tools and techniques:

- BTscan , Bluestumbler , Bluescan , BT Browser
- Bluesnarf
- Bluebug
- Bloover II
- Carwhisperer
- Blueprinting (SDP tool)
- Brute force discovery – Redfang
- Optimising range of Bluetooth attacks

### Defending against Bluetooth attacks:

- Bluetooth recommendations
- Standard organizations practice
- The future for Bluetooth security and implementations

**Training signup form:**

**Training Course: Bluetooth and Wireless Hacking 101**

Today's Date: \_\_\_\_\_

Cost: R7 490 Excl VAT, per person.

Client name (Company): \_\_\_\_\_

Client contact number: \_\_\_\_\_

Client address:

---

---

Number of participants: \_\_\_\_

Participants full names:

---

---

**Company or persons responsible for settling the account:**

Full name: \_\_\_\_\_

Signature: \_\_\_\_\_ Position: \_\_\_\_\_

Authorised relevant parties:

Full Name: \_\_\_\_\_

Signature: \_\_\_\_\_ Position: \_\_\_\_\_

Please fax this entire document to: 011-802-6683 as soon as possible.  
Payment should be made prior to the training seats being issued.  
Please give 2 weeks notice for cancellation.