

# The OSWA-Assistant™

"Assisting Wireless Auditors"  
or....  
"Why Should I Use This Toolkit??"

**Julian Ho**

OSSA, OSWA, OPST, CISSP, SISP, MAISP, CCNA, A+  
OSSA Certified Trainer #CT18274101  
OSWA Certified Trainer #OW126H110  
OPST Certified Trainer #A12V583

## About Us...

- Chief Operations Officer, ThinkSECURE Pte Ltd.
- 10+ years of Security and Network Experience with StarHub, Standard Chartered Bank (London & HK), Sony Partners Limited (USA), KPMG Consulting, Western Digital, et al.
- Original designer & implementor of security and operations for one of AsiaPac's largest hotspot deployments: StarHub's Wireless Hotzones in Suntec Convention Centre and Changi Airport Terminals 1 & 2, totaling approximately 100+ networked devices, covering an area of at least 180,000m<sup>2</sup> (28 FIFA-regulation soccer fields).
- Co-Creator: BlackOPS: HackAttack 2004 (Aug 2004)  
AIRRAID Wireless Tournament (Aug 2005)  
AIRRAID2 (Mar 2008, Bangkok)
- ThinkSECURE ([www.securitystartshere.org](http://www.securitystartshere.org)):
  - Purely technical org doing **practical technical** IT-Security Certification & R&D
  - Certifying body for accredited technical IT-Security Certifications:

**OSSA : Organizational Systems Security Analyst**

**OSWA : Organizational Systems Wireless Auditor**



## Some Background

### Is It Hollywood or Real Life...?

#### Report: Singapore teen faces 3 years' jail for tapping into another's wireless Internet

The Associated Press

Published November 12, 2006

SINGAPORE—A Singaporean teenager has been charged with tapping into some of the nation's wireless Internet lines, a move the nation's security forces say is growing as it reaches for more security.

But, the teenager, 17, is the first person to be charged with tapping into the country's wireless Internet lines, the Straits Times reported.

The report says the teenager was charged with tapping into a government-owned wireless network and accessing it from a computer at his home.

The newspaper said a judge said the teenager faced a maximum penalty of three years in jail.

## Some Background

### Is It Hollywood or Real Life...?

#### S'pore: Second person charged with Wi-Fi tapping

By The Associated Press Staff, Singapore, Nov 12, 2006 at 11:11 AM

SINGAPORE—A second person in the island-state has been prosecuted for illegally tapping into secured personal Wi-Fi networks.

A young man, 19, was charged on Thursday with tapping into a wireless network at a private home, the Singapore Police Department said. The man was charged with tapping into a wireless network at a private home, the Singapore Police Department said.

A 19-year-old man was charged with tapping into a wireless network at a private home, the Singapore Police Department said. The man was charged with tapping into a wireless network at a private home, the Singapore Police Department said.

The police said the man was charged with tapping into a wireless network at a private home, the Singapore Police Department said. The man was charged with tapping into a wireless network at a private home, the Singapore Police Department said.

The police said the man was charged with tapping into a wireless network at a private home, the Singapore Police Department said. The man was charged with tapping into a wireless network at a private home, the Singapore Police Department said.

## Some Background

### Is It Hollywood or Real Life...?

#### T.J. Maxx data theft likely due to wireless 'wardriving'

by JEFFREY HARRINGTON | 11/10/2012 11:20:45 AM | 1 COMMENT

With the potential of Wi-Fi theft, Bluetooth, and other IoT wireless, for security auditors, loss data is more than the million credit and debit card users who had shopped at the company's retail locations was stolen and sold to fraudsters.

Still, a recent article in the Wall Street Journal reporting a wireless data sniffing tactic known as "wardriving" and the consequences of neglecting wireless security protocol known as Wi-Fi Protected Privacy, as the article has quoted a number of operational security security measures, and also the risk was pulled off real-world solutions.

It's likely that the cyberattack on Maxx who stole millions of customer records from TJX stumbled across a vulnerable store location while driving through a shopping centre from their car using a laptop, a television set, and an 802.11g wireless LAN adapter.

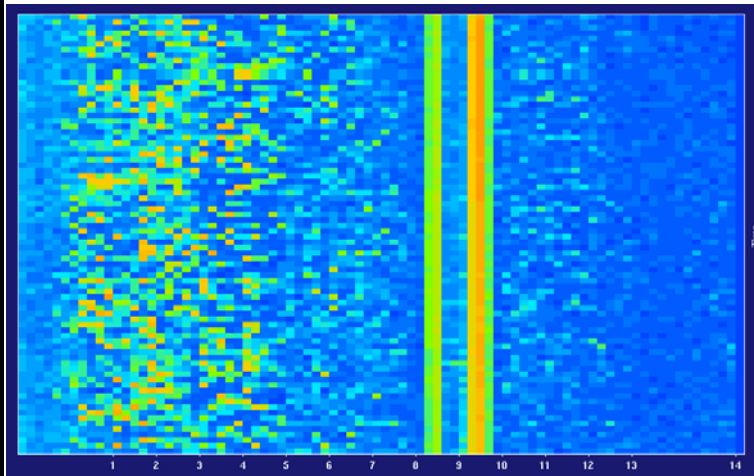
## Wireless Auditing Misconceptions

- Wireless ethernet is like wired ethernet so how you audit is the same.
- I use Ethereal / Wireshark to sniff on a regular basis - if it works for wired ethernet, it must work for wireless ethernet, right?
- All wireless cards are created equal so it doesn't matter what card i use for auditing.
- Hackers must be in the same area as my AP to break in.
- The newer wireless security standards mean you can't get into my network anymore.
- I don't get any results, it must be that the tool is broken.

## What Makes A Great Wireless Auditor?

- Understanding the technology's fundamentals. For wireless, this means Radio Frequency.

## What Makes A Great Wireless Auditor?



## What Makes A Great Wireless Auditor?

- Understanding the technology's fundamentals. For wireless, this means Radio Frequency.
- Next understand the higher layer protocols encoded within the RF energy pulse.

```
IEEE 802.11
Type/Subtype: Probe Response (5)
Frame Control: 0x0050 (Normal)
Version: 0
Type: Management Frame (0)
Subtype: 5
Flags: 0x00
DS status: Not leaving DS or network is operating in AD-HOC mode (To DS: 0 From DS: 0) (0x00)
.... 0... = More Fragments: This is the last fragment
.... 1... = Retry: Frame is being retransmitted
...0 .... = Pwr Mgt: STA will stay up
...0 .... = More Data: no data buffered
...0 .... = WEP Flag: WEP is disabled
...0 .... = Order Flag: Not strictly ordered
Duration: 324
Destination address: 00:0e:2e:c7:e6:b0 (00:0e:2e:c7:e6:b0)
Source address: 00:90:cc:cd:39:07 (00:90:cc:cd:39:07)
BSS ID: 00:90:cc:cd:39:07 (00:90:cc:cd:39:07)
Fragment number: 0
Sequence number: 2443
IEEE 802.11 wireless LAN management frame
Fixed parameters (12 bytes)
Tagged parameters (35 bytes)
SSID parameter set: "micio"
Tag number: 0 (SSID parameter set)
Tag length: 5
Tag interpretation: micio
Supported rates: 1.0(0) 2.0(0) 5.5(0) 11.0(0) 6.0 12.0 24.0 36.0
Tag number: 1 (Supported Rates)
Tag length: 8
Tag interpretation: Supported rates: 1.0(0) 2.0(0) 5.5(0) 11.0(0) 6.0 12.0 24.0 36.0 [Mbit/sec]
DS Parameter set: current channel: 1
Tag number: 3 (DS Parameter set)
Tag length: 1
Tag interpretation: current channel: 1
Country information: Country Code: FR, Any Environment
Tag number: 7 (Country Information)
Tag length: 6
Tag interpretation: Country Code: FR, Any Environment
Start channel: 1, Channels: 13, Max Tx Power: 20 dbm
ERP information: no non-ERP STAs, use protection, short or long preambles
Tag number: 42 (ERP Information)
Tag length: 1
Tag interpretation: ERP info: 0x0 (no non-ERP STAs, use protection, short or long preambles)
Extended supported rates: 9.0 18.0 48.0 54.0
Tag number: 50 (Extended Supported Rates)
Tag length: 4
Tag interpretation: Supported rates: 9.0 18.0 48.0 54.0 [Mbit/sec]
RSN information
Tag number: 48 (RSN Information)
Tag length: 20
Tag interpretation: RSN IE, version 1
Tag interpretation: Multicast cipher suites: AES (CCM)
Tag interpretation: # of unicast cipher suites: 1
Tag interpretation: unicast cipher suite 1: AES (CCM)
Tag interpretation: # of auth key management suites: 1
Tag interpretation: auth key management suite 1: PSK
RSN Capabilities: 0x0000
.... 1... = RSN pre-auth capabilities: Transmitter supports pre-authentication
.... 0... = RSN no pairwise capabilities: Transmitter can support WEP default key 0 simultaneously with pairwise key
.... 00... = RSN PTKSA replay counter capabilities: 1 replay counter per PTKSA/GTKSA/STAKEYS (0x0000)
.... 0000... = RSN GTKSA replay counter capabilities: 1 replay counter per PTKSA/GTKSA/STAKEYS (0x0000)
Vendor specific
```

## What Makes A Great Wireless Auditor?

- Understanding the technology's fundamentals. For wireless, this means Radio Frequency.
- Next understand the higher layer protocols encoded within the RF energy pulse.
- Never assume you've seen everything. Arrogance is the IT-security professional's downfall.
- Doing an audit is a state of mind, i.e. always questioning. Why do i see this result? What are the possible causes? Is there something i am overlooking?
- **Practical and technical** training & certification is important for acquiring the correct skills and mindset. You need the expertise to use audit tools effectively. More on this later.

## Professional Problems

- "Unable to load software on company machine thanks to corporate security policy / enforcement. :( "
- "Can't format my laptop hard-drive coz it's the company's machine."
- "More than one person shares this laptop, I can't risk repartitioning and losing their data!"
- "I don't know a thing about Linux !!  
How to install??? :P "



## Non-techie Problems

- "I have a wireless network at home - but how do i know it is secure??"
- "I heard people say to 'secure' my access point so I got my friend to do it for me. Am i secure now?"
- "All this talk about wireless security is bullsh\*t - who is interested in a small fry like me with only 1 small access point??"
- I only connect to my company with a cable - they have no wireless so no problem, right??
- "Wireless? Security? What's that?"



©2007 ThinkSECURE Pte Ltd; All Rights Reserved; No copying, storage, transmission or reproduction allowed without the express, written consent of the copyright owner.

## Help Is On The Way!

- Introducing the **OSWA-Assistant™** !
- This Wireless Auditing Software Toolkit is the official "assistant" for all **Organizational System Wireless Auditor™** (OSWA) professionals with the following key features:

**OS-independent, standalone, bootable CDROM**

**Audits 802.11 (WiFi), Bluetooth and RFID**

**For Pros: Logically Designed Menu System; Tools all centrally located**

**For Non-Techs: ActivityMap™ Web-based Help System**

**...and COMPLETELY FREE DOWNLOAD !  
(effective use of course, depends on training...)**

©2007 ThinkSECURE Pte Ltd; All Rights Reserved; No copying, storage, transmission or reproduction allowed without the express, written consent of the copyright owner.



በሃይማኖት ላይ

[illegible]

© 2004 Blackwell Publishing Ltd, *Journal of Internal Medicine* 255: 102–110

to build the software, go to <http://www.ccs.cmu.edu/~cs262/lectures/11/11.html> - lecture 11 - 5.11 - COC means to be - when you need to be sure you're OK

- 247 -

- That's 2 categories for our toolkit when everyone else has only 1!

- ©2007 Think SEC URE Pte Ltd. All Rights Reserved. No copying, storage, transmission or reproduction allowed without the express, written consent of the copyright owner.



## Features

### OS-independent, bootable CDROM

- The OS & tools are contained entirely in a self-booting CDROM.
- Just open up CD drive, insert CD & power-on your laptop or PC, like so...
- ISO image publicly downloadable at :  
**<http://oswa-assistant.securitystartshere.org>**
- Just download and use K3B, Nero, Sonic or other CD-burning software to burn the image to a standard 700MB CD.
- Look Ma, no formatting, partitioning, hard drive loading required!

©2007 ThinkSECURE Pte Ltd. All Rights Reserved; No copying, storage, transmission or reproduction allowed without the express, written consent of the copyright owner.

## Features

### Audits 802.11 (WiFi), Bluetooth and RFID

- WiFi - contains both infrastructure **and** client auditing tools; many people don't realize auditing wireless client security is an absolute must & overlook it!
- Bluetooth - audit the security of your PDA/cellphone/PC Bluetooth stack & configuration.
- RFID - test the security of the tag data structure and data-input validation mechanisms (if any!)
- Bonus: MoocherHunter™ on-board. Gives the ability to hunt unauthorized users of a wireless network. No other LiveCD has this feature.

©2007 ThinkSECURE Pte Ltd. All Rights Reserved; No copying, storage, transmission or reproduction allowed without the express, written consent of the copyright owner.

## Features

### Loaded with Wireless Tools (ver 0.9.0.5e) :

#### 802.11

- Aircrack-ng 1.0b2 suite
- Airtart
- Airtort
- Airtort
- AP-Hopper
- AP-Radar
- AP-Utils
- Asleep
- ChopChop
- CoWPAtty
- HostAPD
- Hotspotter
- Karma
- Kismet
- Leapcracker
- MDK3-v4
- MoolichHunter™
- Probemapper™
- SSIDsniff
- Wardrive
- Wavemon
- WEPlab
- Wi-Find
- Wi-Spy Tools
- WifiTap
- WifiZoo
- WPA-attack (Attacker)
- WPA Supplicant
- Wireless Extensions & Tools package

#### BLUETOOTH

- Bluebugger
- Bluediving
- Blueprint
- Bluescanner
- Bluesnarfer
- BT-Audit
- Btfs
- Btscanner
- Carwhisperer
- Ghettoooth
- Obexpush-dos
- HIDattack
- Redfang
- T-Bear
- Ussp-push
- Bluez Bluetooth Stack with hcitool/hcidconfig

#### RFID

- Rfidump
- Rfidtool

©2007 ThinkSECURE Pte Ltd. All Rights Reserved. No copying, storage, transmission or reproduction allowed without the express, written consent of the copyright owner.

## Features

### Redesigned Logical Menu & Tool Layout

- Other LiveCDs suffer from "Geek-itis": trying to get everything under the sun onto a CD regardless of relevancy plus their developers assume that people who use it are Linux gurus.
- Problem: no thought paid to usability or focus; menus non-intuitive & tools scattered all over (like a Windows default install)
- Usability should not be confined to people who spend more time with Linux than they do breathing air. Many auditors are not Linux freaks and just want to get the job done, not search for where all the stuff is! (that's just plain irritating as hell!)
- We've taken the time to debug, compile and make everything under **/usr/local/apps** with subdirs for **/wifi**, **/bluetooth** & **/rfid**.
- Our menus are intuitively labelled as shown in the demo...

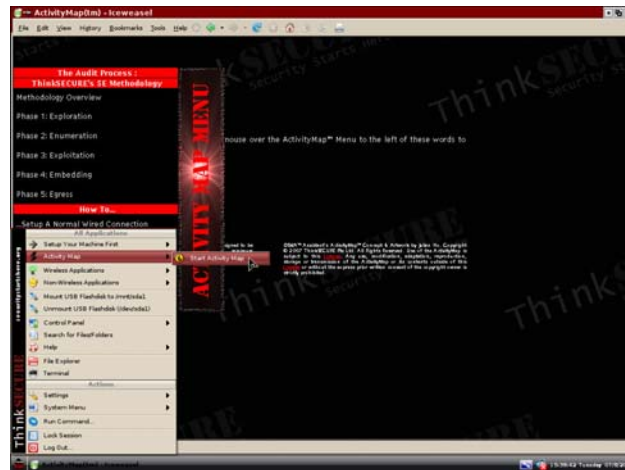
©2007 ThinkSECURE Pte Ltd. All Rights Reserved. No copying, storage, transmission or reproduction allowed without the express, written consent of the copyright owner.

## Features

### ActivityMap™ Web-based Help System

- "Geek-itis" again! Not everyone knows a professional wireless auditor or can afford to engage one. But they still own and run access points!
- Let's give the people the ability to conduct basic wireless audits by following a logical organized sequence of steps.
- Balancing act between too little and too much info.
- ActivityMap™ allows them to test their own systems without giving them the info/steps on how to engage others using active methods.
- If you need a professional to do advanced work or analysis, call in a certified **Organizational Systems Wireless Auditor™ (OSWA)**.

## Features



## Hardware Support

- Documentation is in the CD's / directory.
- We're looking at chipsets, not brands.
- Our website support & FAQ page gives you information on what wireless cards we've tested to work. (various modes)
- Running the toolkit: the more RAM the better; at least 1GB recommended, 2GB rocks! Also, CDROM operating profile (e.g. spin-up/down) & read speed very important!
- You can email us if you find any other hardware which works with tools inside the CD.
- LiveUSB version will be out on 8th August !

## Legal Stuff

- Base OS is GPLed and wireless tools are any one of the following: GPL (and its variants) or "free-to-use" license.
- ActivityMap™ has its own license. You can use it in personal or commercial/work capacity so long as it is only used together with the OSWA-Assistant™.
- MoocherHunter™ is licensed for use with OSWA-Assistant™ only.
- Bottom Line: you can download and use the CD in it's entirety for your work or personal home auditing, and can share it with your friends and colleagues (e.g. burn them a copy).
- When using the CD, users are legally bound not to use the toolkit for unauthorized purposes.

## Last Words

- Like any tool, how good the toolkit performs really boils down to the skill of the user; a bad carpenter can make a \$20,000 hammer look worthless.
- With the ActivityMap™, we try to mitigate the lack of knowledge and skill on the part of the non-technical person so that they can effect a basic wireless audit at home.
- At work & in organizations, this is no substitute for a certified **technical** security professional who is well versed in **practical** understanding of Radio Frequency and wireless protocol details and how to manipulate and take advantage of them.
- IT Pros: The tool is in your hands, now learn how to use it effectively - check out the **Organizational Systems Wireless Auditor™** Certification & Training course at :  
<http://oswa.securitystartshere.org>  
The 3-day certification course with practical exam on day 4 is internationally accredited by ThinkSECURE.