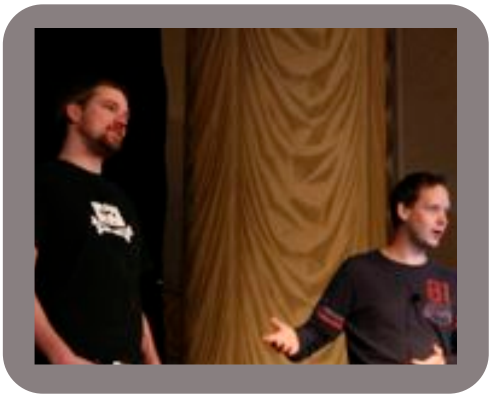
HITBSECCONF2009 – MALAYSIA

CONFERENCE KIT

Hack In The Box (M) Sdn. Bhd.
Suite 26.3, Level 26, Menara IMC,
No. 8 Jalan Sultan Ismail,
502050 Kuala Lumpur,
Malaysia

Tel: +603-20394724
Fax: +603-20318359
Site: http://www.hackinthebox.org || http://conference.hackinthebox.org/

HITBSecConf2009 - Malaysia



Venue:
Crowne Plaza Mutiara
Jalan Sultan Ismail,
Kuala Lumpur, Malaysia

5th & 6th October 2009

4 Tracks of Hands on Technical Training Sessions

7th & 8th October 2009

Triple Track Security Conference featuring HITB Lab Sessions

Lock Picking Village

HAM Radio Village

Capture The Flag Competition

Technology Showcase

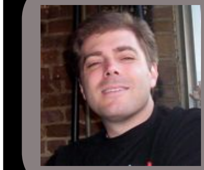
The Keynote Speakers

KEYNOTE 1 - Joe Grand
(President, Grand Idea Studio)

Joe Grand (aka Kingpin) is an electrical engineer, hardware hacker, and president of Grand Idea Studio, Inc., where he specializes in the invention, design, and licensing of consumer products and modules for electronics hobbyists. He is a former member of the legendary hacker collective L0pht Heavy Industries and has spent almost two decades finding security flaws in hardware devices and educating engineers on how to increase the security of their designs.

KEYNOTE 2 - Rop Gonggrijp
(Hacker and Activist)

Rop founded the hacker magazine Hack-Tic in 1989 and was believed to be a major security threat by authorities in The Netherlands as well as in the USA. In 1993, he founded XS4ALL. It was the first ISP that offered access to the Internet for private individuals in the Netherlands. In 2006 he founded the organization "Wij vertrouwen stemcomputers niet" ("We do not trust voting computers") which campaigns against the use of electronic voting systems.



KEYNOTE 3 - Ed Skoudis
(Co-Founder, InGuardians)

Ed Skoudis is a co-founder and Senior Security Analyst with InGuardians, a Washington DC based information security consulting firm. Ed's expertise includes hacker attacks and defenses, the information security industry, and computer privacy issues. Ed is the author and primary instructor for the SANS courses Hacker Techniques, Exploits and Incident Handling and Network Penetration Testing.

KEYNOTE 4 - The Founders of WikiLeaks
(www.wikileaks.org)

Wikileaks is developing an uncensorable Wikipedia for untraceable mass document leaking and analysis. Our primary interest is in exposing oppressive regimes in Asia, the former Soviet bloc, Sub-Saharan Africa and the Middle East, but we are of assistance to people of nations who wish to reveal unethical behavior in their governments and corporations. We aim for maximum political impact.

Official Conference Website:
http://conference.hackinthebox.org/hitbsecconf2009kl/

Hands on Technical Training Sessions (October 5th & 6th)

TECH TRAINING 1 - Web Application (in)Security

Trainer: Marcus Pinto (Author, Web Application Hackers Handbook)

NGS performs penetration tests against some of the most high-profile sites on the internet, and has published the seminal papers in SQL Injection, Oracle Application Server, and many advisories on Web Application Software. This course will demonstrate the full NGS methodology for finding vulnerabilities in web applications, sharing techniques, tools, tips and tricks, and revealing the breakdown of vulnerabilities found on assessment by NGS.

With much of Web Application security now common knowledge, NGS pushes this subject to its new limits, sharing the techniques which make the difference between most methodologies and a deep hack. As well as the conventional attacks covered in this field, delegates will be able to try their hand at some more unique, in-depth attacks.

TECH TRAINING 2 - The Art of Network Based Forensics - Going Beyond Packet Data

Trainers: Meling Mudin (Founder, security.org.my) & Lee Chin Sheng (Independent Network Security Researcher)

This 2-days theory and practical training session will provide the attendees insight into network forensics. This includes the principle, knowledge and tools that are needed to be studied and acquired before adopting to the best practices of network forensics. Attendees will also learn how to use network forensics to compliment host-based forensics in order to answer questions that can't be provided by host-based forensics.

But, this is not all. Since we are going beyond packet data, we will combine practical network forensics technique with log analysis. This involves collection, analysis and correlation of logs from network devices such as firewalls, routers and proxy servers with the acquired network packet data. By merging the analysis of log files and packet data, we hope that forensics investigators will have a clearer picture of a network event.

Hands on Technical Training Sessions (October 5th & 6th)

TECH TRAINING 3 - The Exploit Laboratory 3.0
Trainers: Saumil Shah (Founder/CEO, Net-Square) & SK Chong (Security Consultant, SCAN Associates Bhd.)

Have you ever found yourself staring at a vulnerability advisory with some proof-of-concept snippets and wished the author had rather attached a working exploit with it? Have you wished you could analyze vulnerabilities and write your own exploits for them? Have you wanted to debug and exploit custom built applications and binaries? The Exploit Laboratory is an intense hands-on class for those wishing to dive into vulnerability analysis and exploit writing. The Exploit Laboratory starts off with a basic insight into system architecture, process execution, operating systems and error conditions. The class then quickly accelerates to analysing vulnerabilities with debuggers, reproducing reliable error conditions and writing working exploits for the same.

The Exploit Laboratory features popular third party applications and products as candidates for vulnerability analysis and exploitation, rather than building up on carefully simulated lab exercises. Most of the class time is spent working on lab exercises and examples. Lab examples and exercises used in this class cover both the Unix (Linux) and Microsoft Windows platforms, illustrating various error conditions such as stack overflows, heap overflows and format string bugs. The latter part of the class focuses on topics such as advanced “one-way” shellcode, multi-stage payloads, integrating your own exploits into frameworks such as Metasploit, bypassing protection mechanisms, etc.

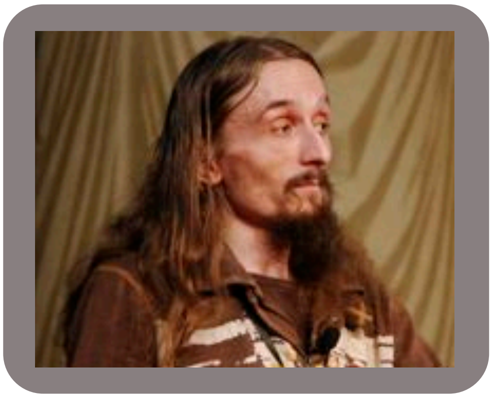
All this - delivered in a down-to-earth, learn-by-example methodology, by trainers who have been teaching advanced topics in computer security for over 8 years. This class is updated from the 2007 edition, featuring new content on heap overflows, abusing exception handlers and more hands-on examples based on recent vulnerabilities. The class features Mac OS X exploitation, for the first time. This class does NOT require knowledge of assembly language. A few concepts and a sharp mind is all you need.

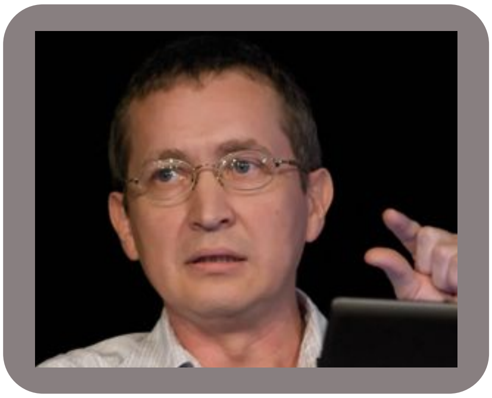
TECH TRAINING 4 - The Security of ASEAN Locks - FOR .GOV / LAW ENFORCEMENT ONLY
Trainers: Deviant Olam (TOOOL USA) & Babak Javadi (TOOOL USA)

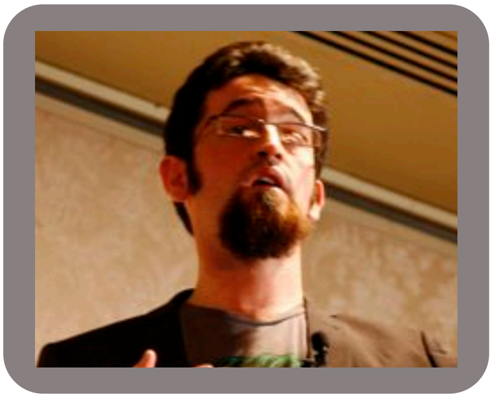
Physical security is an oft-overlooked component of data and system security in the technology world. While frequently forgotten, it is no less critical than timely patches, appropriate password policies, and proper user permissions. You can have the most hardened servers and network but that doesn't make the slightest difference if someone can gain direct access to a keyboard or, worse yet, march your hardware right out the door.

NOTE - This course will pay specific attention to the locks commonly-used in Malaysia and the rest of the Pacific Rim region. Rotating disk locks like those produced by SOLEX and their competitors will be analyzed, discussed, and experimented upon extensively.

Triple Track Conference (October 7th & 8th)





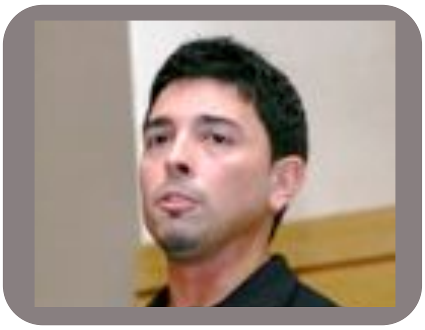


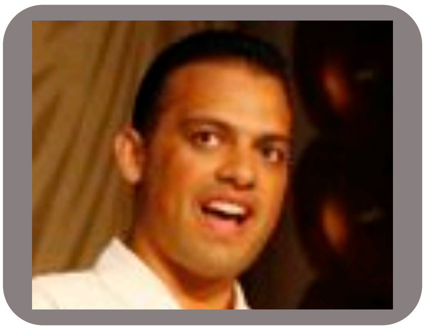
HITB Security Conference has routinely brought together some of the worlds' most well recognized security specialists and research presented at our events have routinely made headlines around the world. This year's conference will once again be run in the TRIPLE TRACK configuration and includes the hands-on HITB Labs session introduced in 2008.

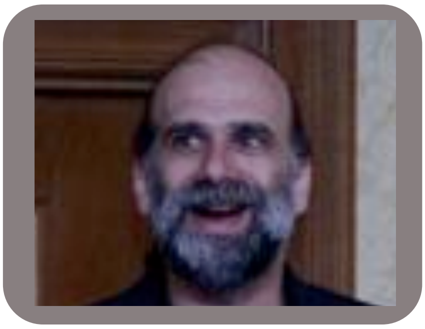
INVITED SPEAKERS

1.) Saumil Shah (Founder, Net-Square)
2.) Deviant Olam (TOOOL USA)
3.) Andrea Barisani (Chief Security Engineer, Inverse Path)
4.) Eric Michaud (TOOOL USA)
5.) Daniele Bianco (Hardware Hacker, Inverse Path)
6.) Babak Javadi (TOOOL USA)
7.) Meling Mudin (Founder, security.org.my)
8.) Job De Haas (Risecure)
9.) Lee Chin Sheng (Independent Security Researcher)
10.) Haroon Meer (Technical Director, Sensepost)

FULL SPEAKER LIST WILL BE ANNOUNCED IN AUGUST 2009







CALL FOR PAPERS

Got something new and cutting edge that you want the world to check out? We want talks that are technical and that discuss new and never before seen attack methods. Summaries not exceeding 1250 words should be submitted (in plain text format) to **cfp@hackinthebox.org** for review no later than 31st July 2009.

TOPICS

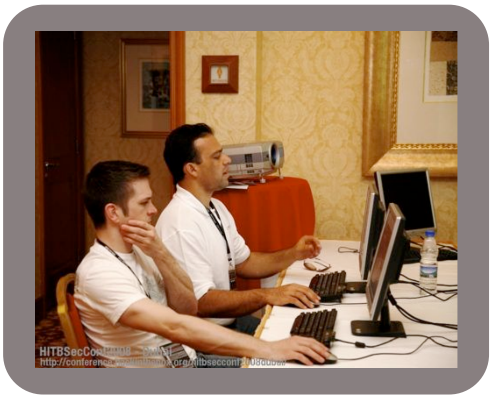
Topics of interest include, but are not limited to the following:

# 3G/4G Cellular Networks
# Apple / OS X security vulnerabilities
# SS7/Backbone telephony networks
# VoIP security
# Firewall technologies
# Intrusion detection
# Data Recovery
# Forensics and Incident Response
# HSDPA and CDMA Security
# WIMAX Security
# Identification and Entity Authentication
# Network Protocol and Analysis
# Smart Card and Physical Security
# Virus and Worms
# WLAN, GPS, HAM Radio, Satellite, RFID and Bluetooth Security
# Analysis of malicious code
# Applications of cryptographic techniques
# Network attack analysis
# File system security
# Security of Embedded Devices
# Hardware Side Channel Analysis

PLEASE NOTE

We do not accept product or vendor related pitches. If your talk involves an advert for a new product or service your company is offering, please do not submit.

Capture The Flag - Weapons of Mass Destruction



AN ALL NEW TEAM BASED ATTACK AND DEFENSE GAME!

The basic principle of CTF-WMD is similar to past CTF competitions held at Hack in The Box - attack and defend. Teams of 3 will have a set of daemons / services running on their machines and they need to exploit rival teams' daemons to get their flags. Submit the flag to obtain offensive points. Keep your daemons up and running to obtain defensive points.

In CTF-WMD, each team will manage a country and each country will start with the same number of population (also known as HP or HitPoints). Teams will need to launch warheads at rival countries or disable their warheads or utilities in order to gain offensive points. For defensive points, all the team needs to do is keep their utilities up.

There are 2 types of daemons.

- Warheads
- Utilities

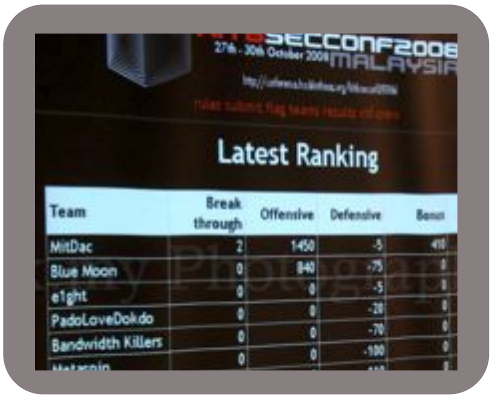
Warheads are inactive by default. Teams will need to crack a bunch of bonus binaries in order to obtain the launch codes for the warheads. Submit the launch codes to the score server and the score server will flag the designated nukes as active. Once a warhead(s) is active, they will automatically launch at a given interval (controlled by the score server). Each warhead carries different points. The harder it is to obtain the launch codes for the warhead, the more damage it'll do to the other teams. When a warhead hits another team's country, a number of population will be deducted from that country. Warheads can be disabled by hacking into them, capturing the flag and submitting them to the score server. When a team submits a rival team's warhead flag, the score server will disable said warhead and deem it unusable.

Utilities are defensive daemons. The only thing they do is regenerate the country's population. The more utilities you have up and running, the higher your regeneration multiplier is. When a team loses all utilities (flag captured by the enemy), population regeneration will drop to 0.

Winners will be determined according to the number of population they have left. If a team reaches 0 population before the game ends, the team is considered disqualified.

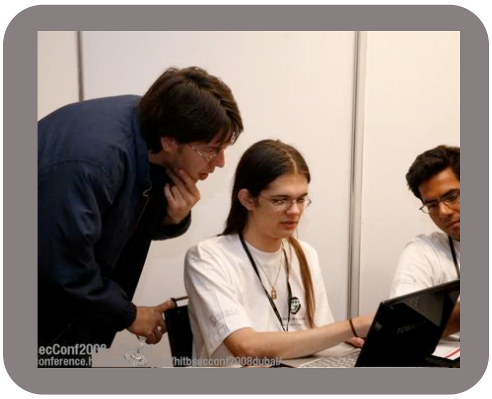
To register for Capture The Flag - Weapons of Mass Destruction, send an email to ctfinfo@hackinthebox.org with the following details:

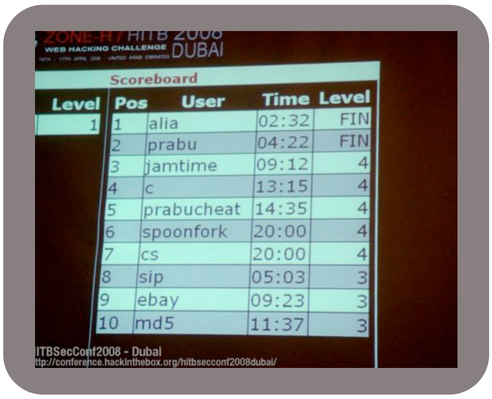
- Team Name
- Team Leaders Name / Handle + Email Address
- Team Members Names / Handle + Email Addresses


HITBSECCONF2008
27th - 30th October 2008 MALAYSIA

Latest Ranking

Team	Break through	Offensive	Defensive	Bonu
MitDac	2	1450	-5	410
Blue Moon	0	840	-75	0
e1ght	0	0	-5	0
PadoLoveDokdo	0	0	-20	0
Bandwidth Killers	0	0	-70	0
[illegible]	0	0	-100	0




ZONE-H / HITB 2008
WEB HACKING CHALLENGE
DUBAI

Scoreboard

Level
1

Pos	User	Time	Level
1	alia	02:32	FIN
2	prabu	04:22	FIN
3	jamtime	09:12	4
4	c	13:15	4
5	prabucheat	14:35	4
6	spoonfork	20:00	4
7	cs	20:00	4
8	sip	05:03	3
9	ebay	09:23	3
10	md5	11:37	3

HITBSecConf2008 - Dubai
http://conference.hackinthebox.org/hitbsecconf2008dubai/

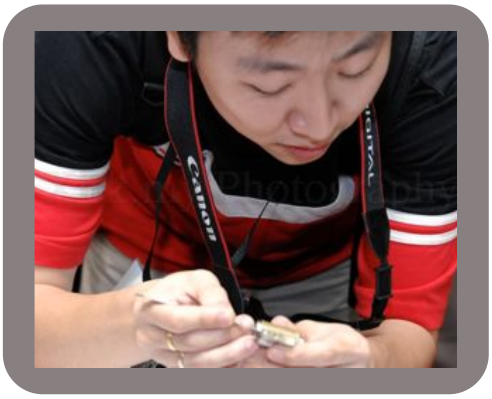
Lock Picking Village (LPV)

Set up and run by members from the The Open Organization of Lockpickers (TOOOL), attendees to this year's event will yet again get a chance to try their hand at picking, shimming, bumping, safecracking, and other physical security attacks.

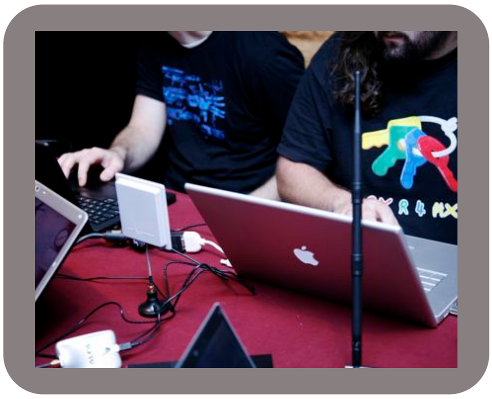
It has always been customary for TOOOL-sponsored physical security sessions to offer some degree of audience interaction and hands-on training. Sometimes this has taken the form of publicly-submitted locks being given on the spot security analysis, other times members of the general public with no lock-picking experience have been invited to attempt a bypass in order to demonstrate its ease.

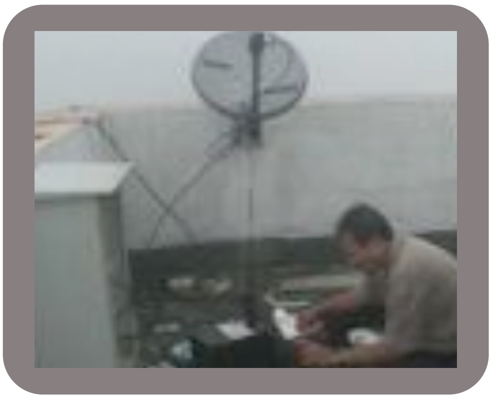
When sample locks and picks are made available, the public inevitably finds most equipment astonishingly easy to compromise and comes away with a better understanding of how to protect themselves. It is in this spirit of educational fun that The Open Organization of Lockpickers has begun to organize “Lockpick Villages” at security events around the world.

All who participate are guaranteed to have a good time and to come away with a healthier and more in-depth understanding of physical security hardware. For HITBSecConf2009 - Malaysia, TOOOL USA will be focusing on the security of ASEAN locks - as always attendees are encouraged to bring your own locks from home to have them tested :)



HAM Radio Village (HAM-RV)



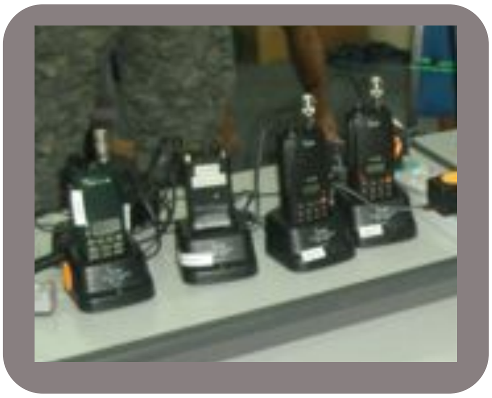


A brand new addition to the conference proceedings for 2009, the HAM Radio Village will be run by the Malaysian Amateur Radio Emergency Service Society - MARES, a non-profit, non-government organisation who's members consists of amateur radio enthusiast who volunteer to be at the ready to provide communication service in time of disaster when normal communication channels are either down or congested.

Amateur radio is defined by the Malaysian Telecommunications and Multimedia Commission (MCMC) as:

Radio communication service (covering both terrestrial and satellite) in which a station is use for the purpose of self training, intercommunication and techical investigation carried out by authorized persons who are interested in radio technique solely with a personal aim and without any pecuniary interest. Millions of radio amateurs communicate daily with each other directly or through relay systems.

Attendees will get a first hand insight into the equipment, licenses and examinations for those interested in getting into the world of amateur radio. Time and weather permitting, MARES will also showcase a LIVE COMMUNICATIONS FEED WITH THE INTERNATIONAL SPACE STATION (ISS) - space hacking anyone?



Price List

TRAINING + CONFERENCE – 5TH, 6TH, 7TH & 8TH OCTOBER

iTEM	TRAINER	PRICE (EARLY BIRD / NORMAL)
TT1 - Web Application (in)Security + Triple Track Security Conference	Marcus Pinto (Author, Web Application Hackers Handbook)	MYR 4098 / MYR 4798
TT2 - The Art of Network Based Forensics - Going Beyond Packet Data + Triple Track Security Conference	Meling Mudin (spoonfork) and Lee Chin Shing (geek00l)	MYR 4098 / MYR 4798
TT3 - The Exploit Laboratory 3.0 + Triple Track Security Conference	Saumil Shah (Net-Square) & SK Chong (Scan Associates)	MYR 4098 / MYR 4798
TT4 - The Security of ASEAN Locks (.GOV/LAW ENFORCEMENT ONLY) + Triple Track Security Conference	Deviant Olam & Babak Javadi (TOOOL USA)	MYR 5098 / MYR 5798

TRAINING ONLY – 5TH & 6TH OCTOBER

iTEM	TRAINER	PRICE (EARLY BIRD / NORMAL)
TT1 - Web Application (in)Security	Marcus Pinto (Author, Web Application Hackers Handbook)	MYR 3599 / MYR 3899
TT2 - The Art of Network Based Forensics - Going Beyond Packet Data	Meling Mudin (spoonfork) and Lee Chin Shing (geek00l)	MYR 3599 / MYR 3899
TT3 - The Exploit Laboratory 3.0	Saumil Shah (Net-Square) & SK Chong (Scan Associates)	MYR 3599 / MYR 3899
TT4 - The Security of ASEAN Locks (.GOV/LAW ENFORCEMENT ONLY)	Deviant Olam & Babak Javadi (TOOOL USA)	MYR 4599 / MYR 4899

CONFERENCE ONLY – 7TH & 8TH OCTOBER

EARLY BIRD	NORMAL PRICE	STUDENT PRICE	AT THE DOOR
MYR 499	MYR 899	** MYR 250 / MYR 499	MYR 1299

** STUDENT REGISTRATIONS

The student price of MYR250 is open to students who are studying in a **Malaysian institute of higher education (college/university)**. International students who are studying outside of Malaysia will still get to enjoy the conference at the early-bird rate of MYR499 regardless of their sign up date. Proof of your academic standing will be required when you check in on-site. You must bring a copy of your class schedule and a valid student ID in order to enjoy the associated student price. Failure to produce proof of your student status will result in a charge of the full on-site conference registration fee of MYR1299.

EARLY BIRD REGISTRATION ENDS ON 31ST JULY 2009
REGISTER ONLINE NOW

http://conference.hackinthebox.org/hitbsecconf2009kl/register/
http://conference.hitb.org/hitbsecconf2009kl/register/