Perth Technical Security Day 2009
Featured Talks and Topics

Event Details
Where: **2 Bradford Street, Mount Lawley, WA 6050**
When: **Friday 4 Dec 2009 from 9:15am to 4:30pm (Australia/Perth)**
Register: **http://eventarc.com/view/95/inagrual-aisa-perth-technical-security-day**

AISA Perth is proud to present the inaugural Technical Security Day in conjunction with ASIAL and Edith Cowan University. We are please to offer two streams of technical sessions. The morning will cover the best of web application security, where there will be two hands on workshops to choose from. Numbers are limited to these hands on sessions so be quick. In the afternoon we will be two technical case study sessions to choose from. Throughout the day we will be running a capture the flag competition with prizes on offer. Morning tea will be provided thanks to ECU. AISA members will be offered a light lunch and an invitation to our end of year drinks.

Interactive sessions by AISA members and supporters for the inaugural Perth Technical Security Day 2009 include:

Anatomy of an Attack: How Hackers Threaten Your Security

SOPHOS

Witness first-hand something which you definitely don't want to try at work: a live malware attack! Paul Ducklin will show you (on a secure and self-contained system) how cybercriminals combine multiple vectors of attack to pull off modern malware infections.

Paul Ducklin (Head of Technology, Asia Pacific, Sophos) is one of the world's leading security experts, and loves to share his knowledge. He is an entertaining and sought-after presenter world-wide. In 2009, he won the inaugural AusCERT Director's Award for Individual Excellence in Information Security.

Breaking Bad – Crypto and Web Applications

stratsec

Cryptography is often used as a method to protect data used by web applications, both during transmission and in storage, and for lots of things it's not meant to do.. However, cryptography is rarely implemented well and can often result in organisations having a false sense of security about the safety of their data. This two hour workshop will examine how & when cryptography can be used to secure data, common mistakes, pitfalls and examples of insecure implementations. Participants will also have an opportunity to complete a number of exercises demonstrating attacks against poorly-implemented cryptographic controls.

Web Application Security Assessment, A Guided Tour

OWASP
The Open Web Application Security Project

The local OWASP boys will be whipping out their flux capacitor to fit as much information as they possibly can into a 2 hour jam-packed session on web app security testing. By providing a flyby of the OWASP Testing Guide, David and Christian aim to demonstrate and explain how to detect security vulnerabilities in your own web applications, including: Cross Site Scripting; Injection Flaws; Cross Site Request Forgery and Session Management Flaws. Demonstrations will utilise a number of open source and freely available tools, including OWASP's own WebScarab. To provide a yoga-like flexibility to the session all materials and testing environments (an Ubuntu wrapped VMware virtual machine) will be provided to attendees, allowing you to either chase us rapidly down the rabbit hole of the OWASP Top 10, or to take your own time after the session... The perfect way to spend a lazy Sunday afternoon.

The Impact of Live Streaming of CCTV Footage on Crime, Communities and ICT Infrastructure

Surveillance in its many forms is an ever-increasing component of the lives of communities and the attempts to police them. Video surveillance is attractive to politicians and crime prevention officials, because it appears to present the possibility of improved crime prevention and response. This paper focuses on live streaming of closed circuit television (CCTV) footage and its technological implications, particularly relating infrastructure and data storage and integrity. In light of this, it also considers police and community perceptions of CCTV usage, and whether these are supported by academic research. The paper concludes with a discussion of the implications for police and the way they use and manage surveillance technologies for crime prevention and response.