



**'On the internet less than five per cent of crimes are actually reported, and in less than one per cent of crimes is anyone actually committed to stand trial.'**



## CYBER FUGITIVES ON THE RUN: NEW RESEARCH TRACKING DOWN INTERNET CRIMINALS

Unlike traditional criminals, these offenders don't leave fingerprints or DNA behind at the crime scene. That's why the perpetrators of internet crimes – such as 'denial of service' attacks that can wreak havoc on critical infrastructure – very often remain undetected.

Internet offenders can employ various methods to hide their identity, or steal the identity of others, to cover their cyber tracks.

Questions also remain as to whether Australian authorities can prosecute offenders who are based outside their judiciary.

"Compared to crimes in the real world, it's very hard to trace the criminals on the internet," says Professor Wanlei Zhou, researcher at the Faculty of Science and Technology, Deakin University.

"On the internet less than five per cent of crimes are actually reported, and in less than one per cent of crimes is anyone actually committed to stand trial."

Wanlei is working on new methods to trace those behind malicious cyber attacks, focusing his study on internet protocol (IP) packets.

All data sent through the internet is parcelled up into these IP packets, which includes information about the sender's unique IP address.

Internet criminals can change the source address in the IP packet, but Wanlei's work involves placing markers in the packet that criminals cannot see, let alone remove.

It is hoped these markers will allow internet crime fighters to reconstruct source addresses in IP packets that criminals have attempted to conceal.

"You will know exactly where the criminal has sent it from, so you can trace them," says Wanlei.

Wanlei and his colleagues, in Australia and overseas, are continuing to test the new technique, which he says could have far reaching consequences if it helps to reduce the rate of internet crime.

"Everybody now is using the internet, for banking, for commercial business, for government services. It's a very important part of our lives."



### REFERENCES:

Shui Yu, Wanlei Zhou and Robin Doss. 'Information Theory Based Detection against Network Behavior Mimicking DDoS Attacks', *IEEE Communication Letters*, Vol. 12, No. 4, pp. 319-321, April 2008.

Yang Xiang, Wanlei Zhou and Minyi Guo, *Flexible Deterministic Packet Marking: An IP Traceback System to Find the Real Source of Attacks*, Accepted by IEEE Transactions on Parallel and Distributed Systems, accepted 07/2008. In press.

### FURTHER INFORMATION:

Professor Wanlei Zhou, Acting Head of School, School of Information Technology

E: wanlei.zhou@deakin.edu.au

[www.deakin.edu.au/scitech/contact/zhou\\_w.php](http://www.deakin.edu.au/scitech/contact/zhou_w.php)[www.deakin.edu.au/scitech/les/research/rpa/palaeobiology/](http://www.deakin.edu.au/scitech/les/research/rpa/palaeobiology/)