



NEWS WHITE PAPERS POD/WEBCASTS DEMO SOFTWARE ARTICLES TOPICS EXPERT TIPS

 Search:

 Visit other TechTarget ANZ sites:
JOIN NOW
 CLICK FOR INSTANT ACCESS

Click here to join YOUR targeted online IT community NOW and gain access to member-only content across our 5 technology-specific sites... Free eNewsletter subscriptions too!

Webcast library
NOW OPEN

Home > Articles > Kiwicon in detail

Posted : Nov 21, 2007 | By: Patrick Gray

Kiwicon in detail

 Tools: [Print article](#) | [RSS Feeds](#)

 SHARE 

This past weekend's Kiwicon security conference in New Zealand was a cracker of an event, with around 200 delegates flocking to Victoria University in Wellington to learn all about the latest hacking techniques.

The conference kicked off with a presentation by Peter Gutmann, a researcher in the Department of Computer Science at the University of Auckland.

Gutmann, who helped write the PGP encryption package and is a bit of a legend in infosec circles, used his slot in the conference to explain why typical computer users are prone to making dumb decisions, ala phishing.

Over the course of his presentation, Gutmann highlighted the significant psychological differences between the people who write software and the people who use it.

It turns out the typical user interface -- of both operating system and security software - couldn't have been more bafflingly designed if it were deliberate. The absence of a padlock in a browser indicating an insecure connection to a phishing web-site, for example, has been clinically proven to be routinely ignored. People just can't perceive the absence of that little padlock.

Perhaps Microsoft, Symantec et al should consult the head shrinkers before their next service pack or point release. So there you go, the people who say Microsoft needs psychological help are actually right!

During the next presentation a gentleman named "Bogan", who works for a telco in New Zealand, told us that finding vulnerabilities and stupid design flaws in security software is actually quite handy when it comes to negotiating licensing deals with software vendors. If a software manufacturer wants to put up your support fees by \$20,000 PA, get to work finding bugs in their product. This talk showed us how we can save top dollars by embarrassing vendors into heavy discounts.

Next up a presentation by Declan Ingram of Security-Assessment.com showed us that little has changed in the world of intrusion detection and prevention.

Security operations centre staff still spend most of their time playing Xbox (because monitoring logs is no one's idea of a good time), the technology is prone to being interfered with through deliberately generated false alarms and the devices are commonly mis-configured. Sadly, it seems, many organisations are still unaware that intrusion detection systems can't detect attacks on encrypted services like SSL. If you can't decrypt the data then the IDS/IPS can't decrypt the data. Sounds sensible to us, but apparently some people just haven't learned.

Morgan Marquis-Boire of Security-Assessment.com (a company that provided a large number of speakers at the event) used his talk to paint a fairly spooky picture of the security of SCADA and x.25 networks. Because providers have been depreciating x.25 for years, no real effort has gone into securing it, and it's a connection type still used by many companies in the finance sector. Any CSO who witnessed Marquis-Boire's talk would probably rush back to the office and have a real think about what they can do to lock down their x.25 connections, if not ditch them completely.

Another Security-Assessment.com staffer, Nick Breese, then showed us how Playstation 3s can be used to crack passwords at breathtaking speed. When implementing an md5 algorithm on a Core 2 Duo scalar processor, he was able to run through around eight million iterations of the checksum in a second.

By optimising some code on the Playstation 3, which uses vector-based processing, his new figure was closer to 1.4 billion iterations a second. It was an interesting bit of research that shows us the days of conducting password recovery using standard computing equipment are surely numbered.

Vector-based processing is where it's at.

TechTarget ANZ will bring you a full write-up on Breese's talk in coming weeks.

In the most sensational presentation of the conference, security researcher Beau Butler showed us how Microsoft's completely half-arsed fix of a known issue - problems with Windows Proxy Autodiscovery - could be used by the more evil among us to seize control of vast numbers of workstations. Due to a bug in Microsoft's WPAD functionality, proxy auto-configuration requests frequently wind up popping out on to the Internet.

That means bad, bad people can load up your workstations with false proxy information. That's right, Butler had figured out a way to run a man-in-the-middle attack on hundreds of thousands, if not millions, of workstations in his home country. You'll be hearing more on this, but in the mean time it would make sense to configure a wpad server in your organisation to stop Microsoft's silly software from seeking proxy configuration files from evil hackers outside your organisation.

The day closed with bug hunter Brett Moore of Insomnia Security struggling through a fairly diabolical hangover to show the audience how to do all sorts of very clever things when exploiting memory bugs in Windows. This presentation went completely over TechTarget's head, but judging from the audience reaction, Moore is a very clever chap.

NEXT: [Day two of the Kiwicon conference](#)

White Papers

- Beating back blended spyware threats
- Branching out to protect remote offices
- Monitoring and Securing the Mobile Workforce
- Forrester's Guide to the Client Security Market
- Virtual criminology report

Related Articles

- Black Hat preview: get ready for the "Pwnie Awards"
- Should business prepare for collateral damage during Cyberwarfare?
- How Queensland Sugar fought off a denial of service attack
- Kiwis plan punishing anti-counterfeiting regime
- WhiteHat CTO rates MD5 hash vulnerability the Web's top security flaw

© 2010 TechTarget ANZ. All Rights Reserved. Designated trademarks and brands are the property of their respective owners. Use of this website constitutes acceptance of the TechTarget ANZ Terms and Conditions and Privacy Policy.

NEWS WHITE PAPERS POD/WEBCASTS DEMO SOFTWARE ARTICLES TOPICS EXPERT TIPS


 TechTarget ANZ sites: [SearchCIO.com.au](#) | [SearchNetworking.com.au](#) | [SearchSecurity.com.au](#) | [SearchStorage.com.au](#) | [SearchVoIP.com.au](#)

 WF Online community sites: [ElectricalSolutions](#) | [ElectronicsOnline](#) | [FoodProcessing](#) | [InMotionOnline](#) | [LabOnline](#) | [ProcessOnline](#) | [RadioComms](#) | [SafetySolutions](#) | [SustainabilityMatters](#) | [Voice&Data](#)

 Copyright © 2010 Westwick-Farrow Pty Ltd. All rights reserved.
[About Us](#) | [Contact Us](#) | [TechTarget](#)