



Comodo Cryptography Expert to Deliver Keynote speech at 4th ITNG Conference

Comodo Inc, March 01, 2007

URL: <http://www.pr9.net/business/ecommerce/5202march.html>

Dr Colin Walter's speech will focus on how solutions to side channel attacks are ineffective in real-world implementation.

PR9.NET March 01, 2007 - Jersey City, NJ - Comodo, a leading provider of Identity and Trust Assurance Management Solutions, is pleased to announce that Dr Colin Walter, Head of Cryptography at Comodo's Digital Trust Research Lab, will present the opening key note address at the 4th International Conference on Information Technology: New Generations (ITNG), 2- 4 April at the Orleans' Hotel, Las Vegas, Nevada (<http://www.itng.info>).

Dr Walter's speech, Counter Intelligence against Side Channel Attacks, focuses on inadequacies in existing counter measures to side channel attacks and emphasizes the need for extreme care and expertise when designing hardware for containing secret cryptographic keys.

In the field of cryptography, side channel attacks are the exploitation of weaknesses in physical devices used to deploy cryptographic systems allowing the attacker to decrypt sensitive data, such as private keys. For example, minute variations in timing, power, and electro-magnetic radiation can be used to reconstruct the secret keys used by a smartcard or cryptographic token when performing authentication.

The speech will show how "conventional wisdom" in the mathematical world about the security of counter measures such as data whitening, longer key lengths, and key blinding can be insufficient when deployed onto real-world hardware.

Dr. Colin Walter is the Head of Cryptography at Comodo CA and Chairman of Peripherals Working Group – Trusted Computing Group and Co-chair - Cryptographic Hardware and Embedded Systems. He has achieved international recognition in the design of hardware and algorithms for the implementation of RSA cryptography. A senior member of the IEEE, Colin is most well-known to the international community for his long term research into Montgomery modular multiplication. A selection of his papers are available on the Comodo website at <http://www.comodo.com/research/crypto/publications.html>

Full conference details and an itinerary can be found at the ITNG website (<http://www.itng.info>)

###

About Comodo Inc

Comodo, through its group of Internet security companies, is a leading Certification Authority and global provider of Identity and Trust Assurance services on the Internet. Comodo secures and authenticates online transactions and communications for over 1,000,000 business and millions of consumers. With a global presence in the US, UK, Ukraine, and India, Comodo offers businesses and consumers third-generation solutions for intelligent security and authentication technologies that create trust online. Comodo's technological expertise includes PKI digital certification, integrated authentication infrastructure services, regulatory compliance solutions and digital e-commerce services. The Comodo companies develop technologies that address critical authentication and security needs with proven and reliable solutions such as SSL certificates, Mutual Authentication solutions, PCI compliancy services, Desktop Security, Code signing certificates, identity and vulnerability management solutions.

Phone: 1 888 266 6361
FAX: 1 201 963 9003
Website: <http://www.comodogroup.com>
E-Mail: media-relations@comodo.com
Address: 525, Washington Blvd,
Jersey City
NJ 07310
USA