



Innovation in cryptography to drive new security protocols in chip manufacture

Comodo Inc, September 21, 2005

URL: <http://www.pr9.net/comp/science/2579september.html>

Comodo leads key industry cryptography conference to establish new processes for security in smart cards and credit cards worldwide

PR9.NET September 21, 2005 - New York. Comodo Inc., a global leader in Identity and Trust Assurance Management solutions announced today top line findings from the seventh annual CHES (Cryptographic Hardware and Embedded Systems) Conference in Edinburgh, Scotland. (See www.chesworkshop.org for details.) Comodo's Head of Cryptography, Dr. Colin Walter from Comodo's Digital Trust Lab was general chair for this year security conference under the umbrella of the International Association for Cryptographic Research, the IACR (www.iacr.org).

Conference Background

The conference was well attended by a mix of leading researchers from both academia and industry - representing prestigious companies and organizations such as IBM, Intel, Infineon, Siemens, Toshiba, Hitachi, Philips, NEC and Atmel. Delegates from key cryptography departments, such as Cambridge, Bristol, Louvain-la-Neuve and Leuven Universities, were also present.

With well over 200 delegates, CHES is probably the largest and most important forum for discussing the security and implementation aspects of the chips in credit and debit cards to ensure identity integrity. Three guest speakers gave a broader view of those topics within a secure and trusted global communication network. Thomas Wille from Philips Semiconductors talked about "Security of Identification Products: How to Manage", Ross Anderson from Cambridge University Computer Laboratory spoke on "What Identity Systems Can and Cannot Do" and Jim Ward from IBM, and president of the Trusted Computing Group, presented "Trusted Computing in Embedded Systems".

Summary of Conference Discussion

Overall, the main theme of the invited talks and surrounding discussion was how to balance freedom of information required for commerce with the equally demanding identity security needs of individuals and corporations.

So, for example, some challenging questions included whether "Douglas A MacKenzie" who bought a house twenty years ago is the same as the "Angus MacKenzie" that now wishes to sell the house? Will the same rules apply when this is applied to withdrawals from a bank account? Will economic or political pressures for secure solutions result in denial of personal rights?

These issues point to important new opportunities in protecting personal information as they "intersect" in the "open" commerce infrastructure.

Summary of Conference Conclusions

Exacerbating this challenging balancing act is the added reality that threats can come in ways and technologies not expected. For example, cloning of cards can be done using side channel attacks, which use variation in time, power or electro-magnetic radiation to determine the hidden secrets. When used internally, each bit of a secret key generates different EMR according to whether its value is 0 or 1. By interpreting these data correctly, fraudsters can obtain access to confidential information.

Some key conclusions and countermeasures were identified and included:

- * Investigation of new, potential side channel attacks, both against specific implementations and involving new concepts - so as to have remedial action in place.

- * Developing new algorithms to hide secret key bits to prevent the cloning of cards

There was acknowledgement that the challenge remains to develop further protocols for more effective hiding of the secret keys to mitigate the vulnerability of cards to attack.

###

About Dr. Colin Walter

Dr. Walter has made substantial progress in the discovery of implementation weaknesses of side channel attacks during his time at Comodo, and pioneered a number of solutions of which the Mist algorithm is a notable example, (randomizing the key processing for stronger security). Much of this work at the Comodo Digital Trust Research Laboratory has now been made public, and can be downloaded from <http://www.comodogroup.com/research/crypto/publications.html>

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

[PR9.NET - Your Free Press Release Service](#)