Cyber hacking could be a thing of the past

December 7 2009

Model Bombe code-breaking machine used at Bletchley Park during World War II to decipher messages transmitted by German forces using Enigma encoding machines.

(PhysOrg.com) -- High-profile websites are constantly under threat from hackers attempting to paralyse their websites but new research could make such attacks computationally impossible. This research will be one of the topics discussed at a major international conference on the theory and application of cryptology and information security in Japan this week.

Three papers by academics from Bristol University's Department of Computer Science will be presented at the ASIACRYPT conference in Tokyo [6 to 10 December].

Security notions and generic constructions for client puzzles will discuss the defence for websites against attackers who launch denial-of-service

attacks. Such attacks are becoming more common on the internet, with high-profile attacks taking place against many leading websites. The paper, from research by Bristol University academics, Paul Morrissey, Nigel Smart, Bogdan Warinschi and Liqun Chen from Hewlett-Packard Laboratories in Bristol, investigates a specific defence technique that aims to make performing such attacks computationally infeasible, while not overburdening the innocent user.

In joint research between Nigel Smart and Steve Williams at Bristol University; Benny Pinkas, University of Haifa, Israel and Thomas Schneider, Ruhr-University at Bochum, Germany, the team show that a procedure thought to be only theoretical can actually be implemented in practice. One goal of this collaboration, entitled *Secure two-party computation is practical*, is to ultimately allow for databases to compute on encrypted data. Future applications of this research could be for doctors to access centralised healthcare databases in a way that protects patient confidentiality.

In the final paper, *Foundations of non-malleable hash and one-way functions*, by Bogdan Warinschi from Bristol University; Alexandra Boldyreva and David Cash, Georgia Institute of Technology, USA and Marc Fischlin, Technical University in Darmstadt, Germany, the researchers consider foundational issues related to basic constructions in cryptography. This research is an important step in understanding the properties of a cryptographic object called a ”random oracle”. Such objects are a popular solution in constructing efficient cryptographic schemes, such as those used in a web browser.

Nigel Smart, Professor of Cryptology in the Department of Computer Science at the University of Bristol and co-author on two of the papers, said: “We are delighted to have such a strong presence at this year’s ASIACRYPT conference, especially as it was particularly hard to have papers accepted. Of 300 submissions, just over 40 were selected for

presentation at the conference."

More information:

• ASIACRYPT conference -- asiacrypt2009.cipher.risk.tsukuba.ac.jp/

The three papers being presented at ASIACRYPT 2009 are:

Paper: Security notions and generic constructions for client puzzles, Paul Morrissey, Nigel Smart, Bogdan Warinschi, Department of Computer Science at the University of Bristol and Liqun Chen from Hewlett-Packard Laboratories in Bristol.

Paper: Secure two-party computation is practical, Nigel Smart and Steve Williams, Department of Computer Science at the University of Bristol; Benny Pinkas, University of Haifa, Israel and Thomas Schneider, Ruhr-University at Bochum, Germany.

Paper: Foundations of non-malleable hash and one-way functions, Bogdan Warinschi, Department of Computer Science at the University of Bristol; Alexandra Boldyreva and David Cash, Georgia Institute of Technology, USA and Marc Fischlin, Technical University in Darmstadt, Germany.

Provided by University of Bristol (news : web)