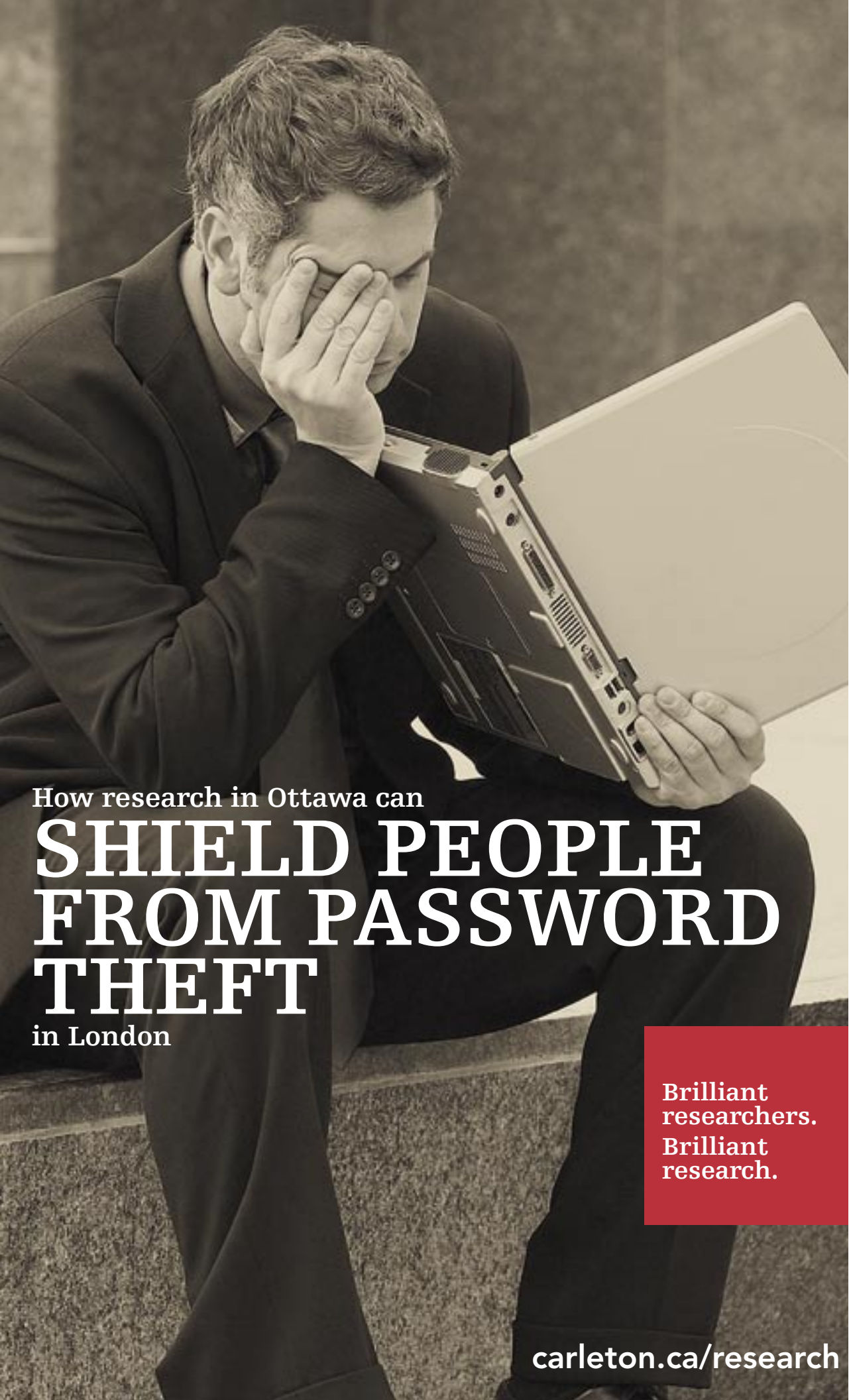

Carleton UNIVERSITY
Canada's Capital University

How research in Ottawa can

SHIELD PEOPLE FROM PASSWORD THEFT

in London

Brilliant researchers. Brilliant research.

Paul Van Oorschot, PhD
Carleton University's
Canada Research Chair in
Network and Software Security

carleton.ca/research

Brilliant researchers.
Brilliant research.

Research snapshot

Purpose
To identify the weaknesses in authentication and security systems that facilitate online identity theft.

Scope
To examine the online theft and exploitation of personal data such as bank account information and social insurance numbers.

Thesis
Existing mechanisms for authenticating personal identity are woefully inadequate and need to be improved.

Outcome
To make it harder to illegally gain access to, or exploit, online personal information and identification data, and thus to help protect individuals from identity theft.

Selected publications

- Chiasson, Sonia, P.C. Van Oorschot, Robert Biddle. "A Usability Study and Critique of Two Password Managers." *USENIX Security*, August 2006, Vancouver.
- Menezes, A.J., P.C. Van Oorschot, S. Vanstone, "Handbook of Applied Cryptography." *CRC Press*, 1996.

Grad student projects
Julie Thorpe,
second-year student,
PhD in Computer Science
Pass-thoughts: Authenticating With Our Minds

Mohammad Mannan,
second-year student,
PhD in Computer Science
Authentication and phishing, in the presence of untrusted computers

Honours
- 2001 J. Wesley Graham Medal in Computing and Innovation
- 2001-02 Program Chair, Internet Society Network and Distribution Systems Security Symposium (NDSS), San Diego
- 1993-01 Member of the Board of Directors, International Association for Cryptographic Research (IACR)

Carleton UNIVERSITY
Canada's Capital University

Phishing for answers: how to solve the problem of online identity theft

Ping! You receive an email that appears to be from your bank. The message claims that attempts have been made to break into the bank's computer system and asks for your help to prevent further intrusions. All you have to do is send along your online banking password so that the bank can authenticate your accounts. You type in the information and off goes your email… but not to your bank. Your online password is now in the hands of organized crime.

Is this scenario for real? Absolutely, according to Dr. Paul Van Oorschot, the Tier I Canada Research Chair in Network and Software Security at Carleton University. In fact, with the growth in the use of the internet by law-abiding citizens and criminals alike, it is a nightmare that will become more common in the future.

"The internet allows fraud to be automated, from a safe distance, which makes it especially attractive to organized crime as a potential source of income," he explains. "Given the billions of bytes of data that travel across virtual space daily, and the countless databases remotely accessible, the risk increases every day that an individual's personal identification information will be stolen. I wish to find ways to reduce this risk."

IDENTITY EASY TO STEAL

A leading international research scientist in computer and network security, Van Oorschot opened the Carleton Computer Security Lab in 2003. One of his projects is to identify the elements of authentication and information security systems that facilitate identity theft. By examining how information such as bank account, driver's license and social insurance numbers is harvested and exploited via the internet, his work illustrates that existing mechanisms for authenticating identity desperately need improvement. He hopes that his research will lead to new cost-effective security measures that make it much tougher to illegally access and exploit personal information.

Van Oorschot's research has found that some types of identity theft are facilitated by the continued use of conventional passwords for authentication. They are inexpensive to create, simple to use, and far too easy to steal. Criminals have a number of effective methods for stealing passwords. Phishing, for example, is a social engineering technique (i.e., a method for tricking individuals into giving up secrets): an authentic-looking email from a well-known financial institution requests passwords and other security information.

NEW WAYS TO AUTHENTICATE IDENTITY

To counter this type of theft, several enhanced security mechanisms are under development. These include the use of biometric passwords, multi-factor authentication, trusted hardware devices (those that perform "as you expect"), and schemes which cross-check trusted sources. In multi-factor authentication systems, one factor is typically a conventional password, while the second might be a time-dependent code created by a hand-held passcode generator. The challenges in making these alternatives practical include cost and user-friendliness.

Van Oorschot hopes, however, that cost-effective and stronger security measures will eventually be available to authenticate identity. His enthusiasm for his research seems boundless.

"My goal is to provide research solutions that positively impact the lives of others," he reflects. "My fifteen years in industry reinforced my desire to address concrete, practical problems. As a university researcher, I am in the privileged position of being able to solve research problems which may help many other people."

"My goal is to provide research solutions that positively impact the lives of others."

Canada Research Chairs
The Canada Research Chairs Program is designed to attract the best talent from Canada and around the world, helping universities achieve research excellence in natural sciences and engineering, health sciences, and social sciences and humanities.

Chairholders improve Canadians' depth of knowledge and quality of life, strengthen the country's international competitiveness, and help train the next generation of highly skilled people. When fully implemented, the program will support 2,000 research professorships across the country.

207-06 300 06 2006