Carleton
UNIVERSITY
Canada's Capital University

Designing a Stronger Backbone for Internet Security and to Protect Users

research.carleton.ca

Paul Van Oorschot, PhD, FRSC
Carleton University's Canada Research Chair in Authentication and Computer Security

Paul Van Oorschot Researches Defensive Software Technologies to Protect Computer Resources and Users

Internet banking in Canada is portrayed as being as safe as a giant time-lock vault. A major component is a security protocol with a high-level Secure Socket Layer (SSL) encryption technology to ensure a direct connection or 'hand shake' between a customer's browser and the bank's server. SSL also provides a means to verify that a message comes from the original source and is not altered.

An internationally recognized authority in computer security, Paul Van Oorschot investigates protective software technologies. He is renowned for his expertise in authentication mechanisms and infrastructure including SSL, passwords, certificate-based authentication and software architecture. As with any complex structure, software architecture – like the best designed buildings – must have a solid, stable and reliable foundation but one that is resilient, comprehensible and technologically and economically viable.

In an era plagued by identity theft, malicious computer software, and broad opportunities for social engineering that collectively open the door to hacker attacks, most people understand the need for security. Yet, defensive tools such as passwords were designed 40 years ago for desktop computer systems, which then offered a simple means to restrict who the authorized users were.

Passwords are here to stay as one user-facing dimension in multi-faceted frameworks, says Van Oorschot, even though the notion of computing has changed. Passwords and related safeguards were introduced in a world where the only users were experts and engineers. This has evolved now into an environment where users are non-experts from all backgrounds and age groups. Many mobile browsers, for example, do not currently offer the SSL-related security indicators and authentication certificate information that is available on desktops.

"We need to look at authentication mechanisms that are robust and user friendly on both mobile devices and desktop computers. One option involves Internet geo-location technologies as a supplement to password authentication."

Equally important is that software is installed on mobile devices and run by just about everyone – very few of whom are experts – and such users could inadvertently agree to install malware or apps with hidden (Trojan) functionality. One of Van Oorschot's research objectives is to examine operating system designs that provide protection by isolating mobile apps from each other and from the operating system itself while preserving all the rich advantages of the software components. Another area of interest is designing better password management tools.

THE RESEARCH

What I do

Advancing the understanding of authentication technologies and designing better software mechanisms including user identity management, authentication infrastructure for computer use, and security for mobile devices.

Why it matters

Mobile devices, including smartphones and tablets, now outstrip personal computer sales, and require specialized security features different from those designed principally for desktops.

What it will change

Stronger machine-to-machine and user authentication are an essential component to offset computer-related security threats.

THE RESEARCHER

2008-2013, Scientific Director and Principal Investigator, Natural Sciences and Engineering Research Council ISSNet, a network of 15 faculty professors in eight Canadian universities.

2013, Carleton University, Faculty Graduate Mentoring Award.

2011, Fellow, Royal Society of Canada, the national academy of sciences.

Co-author, Handbook of Applied Cryptography, (CRC Press, 2001), regarded as the standard reference for engineers and applied researchers in the field.

PARTNERS

Partnerships and collaborations have included NSERC ISSNet, CA Computer Associates, U.S.A.; Blackberry Ltd., Waterloo, ON; Trend Micro, Ottawa; Bell Canada, Montreal; and Microsoft Research, Redmond, WA.

research.carleton.ca

"Good architecture and design requires knowing how we will keep authentication and security features resilient without complicating things for the user."

Carleton UNIVERSITY
Canada's Capital University