Trinity College Dublin
Coláiste na Tríonóide, Baile Átha Cliath
The University of Dublin

Research Seminar

Passwords - A Guide to the Ruins and Lessons for Improvement

Cormac Herley
Microsoft Research

12-1pm Weds 26th Sept 2015

Abstract: We review some of our recent work on authentication and search for lessons on why problems here have proved so persistent. First, considering a user who has, not one but dozens of accounts to maintain, we find that the common advice (choose random passwords and one per account) is not merely difficult but impossible in the absence of memory aids. We show that weak passwords and password re-use, far from being shameful manifestations of user failings, are essential tools in allocating effort as portfolio size grows. Second, we examine the gap between the effort needed to withstand online and offline attacks, and find it to be enormous: probable safety occurring when a password resists 10^6 and 10^{14} guesses respectively. This implies that many common practices guarantee large-scale waste of user effort. These include exceeding the online while falling short of the offline threshold, and encouraging users to resist offline guessing at sites where passwords are stored plaintext or reversibly encrypted.

Finally, we seek lessons. How do we end up insisting on the necessity of things that prove impossible? Why do we keep getting things wrong? What will it take to move things forward?

Short Bio: Cormac Herley is a Principal Researcher at Microsoft Research, where he's been since 1999. His main current interests are data analysis problems, authentication and the economics of information security. He has published widely in signal and image processing, information theory, multimedia, networking and security. He is inventor of 70 or so US patents, and has shipped technologies used by hundreds of millions of users. He received the PhD degree from Columbia University, the MSEE from Georgia Tech, and the BE(Elect) from the National University of Ireland.

Venue: Seminar Room, Dunlop-Oriel House/CTVR.

Further Details: Doug Leith (doug.leith@tcd.ie)

CONNECT
Networks of the Future