Cryptography in the Wild: Password Managers

Kenny Paterson

Abstract: Cryptography is a fundamental enabling technology that underpins the information age: without it, we could not have online commerce, secure messaging, cloud computing and many other things that we have come to take for granted today. Cryptography rests on firm foundations in computer science and mathematics, but there is often a disconnect between those foundations and how cryptography gets used in practice – "in the wild", so to say. In this talk, I'll introduce recent work done in my research group that examines that disconnect in a particular context, namely cloud-based password managers. These are used by millions of people and are marketed as offering strong security, with terms like "Zero Knowledge Encryption" being common in the industry. I'll explain how we went about examining the security of password managers, how we worked with vendors to improve the security of their products, and why we do this kind of work. I'll also discuss what lies ahead in the broader space of "end to end encrypted applications", including password managers, cloud storage, messaging apps, and online collaboration systems.