Exploring the Use of Trusted Hardware in Mobile Apps

Jenny Blessing[1], Alastair Beresford[1], and Ross Anderson[1,2]

[1] University of Cambridge
[2] University of Edinburgh

Trusted hardware is one of the most promising tools to increase the real level of security provided to smartphone users. Both major mobile operating systems, Android and iOS, have provided some form of hardware-backed key storage for around a decade through Android KeyStore and iOS Secure Enclave respectively. Once encryption keys and other sensitive data are generated and/or stored within the secure enclave, they cannot be extracted or otherwise compromised even in the face of physical device access.

But trusted hardware is only useful if it is actually used. Despite the longstanding availability of secure hardware in mobile devices, it is not well understood how many developers actually take advantage of this type of secure storage. This is of particular relevance in smartphones, where hardware keystores are available at no marginal cost to the app developer.

In this talk, we will discuss preliminary results from a large-scale survey of secure hardware usage in Android applications. We explore how many apps use the KeyStore in practice, and which specific features they use. Our initial findings suggest that few apps outside of the most widely used and well-resourced use any form of secure hardware.

Of particular interest is examining how usage varies by app category. We find that applications in heavily-regulated sectors such as finance are more likely to use the KeyStore compared to, for instance, gaming apps, suggesting that secure hardware usage is linked to compliance. In the presentation, we will explore what this says about developers' and employers' motivations (or lack thereof) to prioritize security during the development process.

This work has broad implications for security economics, usability, and policy. Drawing on both our results and prior literature, we will conclude by discussing developer incentives to care about security and practical barriers to security tool adoption.