PhD Symposium

Towards An Authorization Framework For App Security Checking

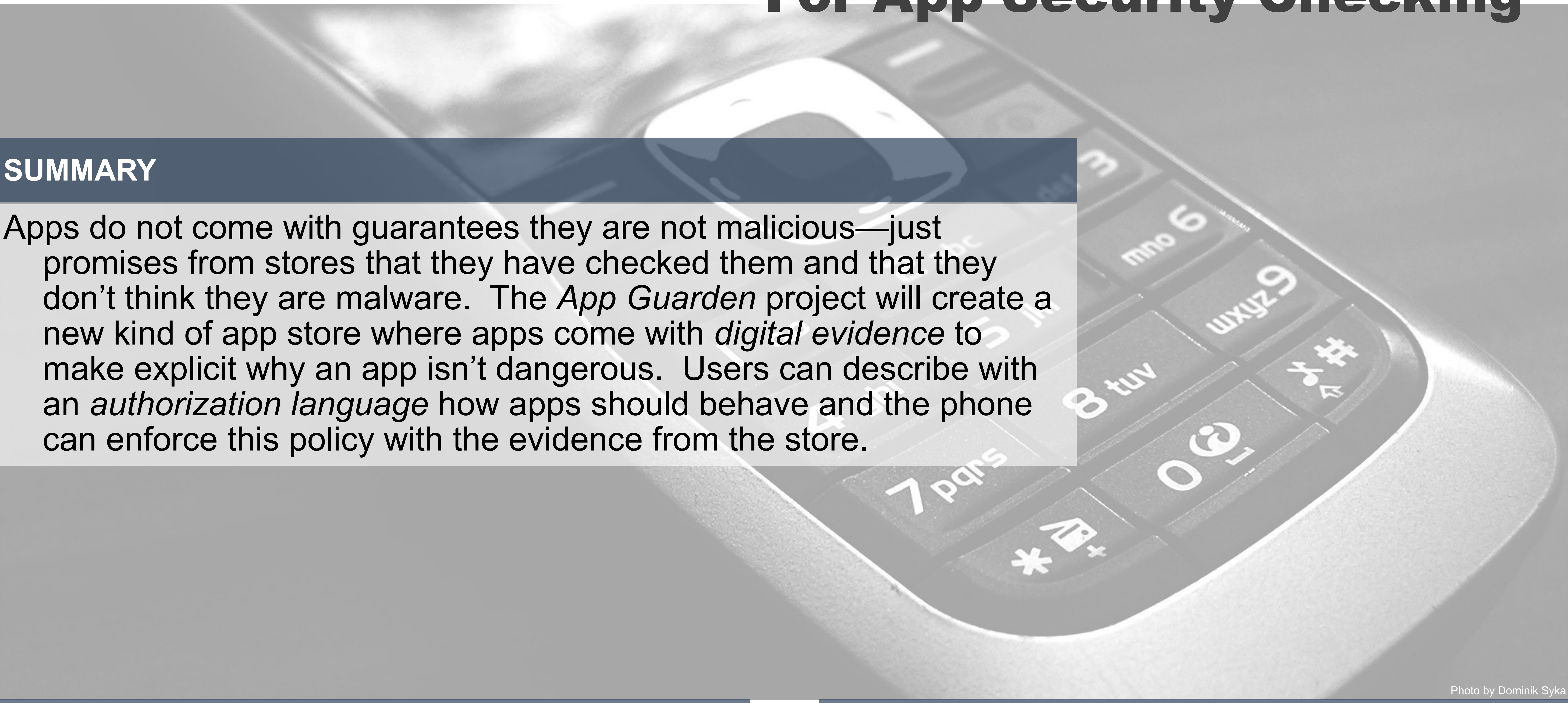


Photo by Dominik Syka

SUMMARY

Apps do not come with guarantees they are not malicious—just promises from stores that they have checked them and that they don't think they are malware. The *App Guarden* project will create a new kind of app store where apps come with *digital evidence* to make explicit why an app isn't dangerous. Users can describe with an *authorization language* how apps should behave and the phone can enforce this policy with the evidence from the store.

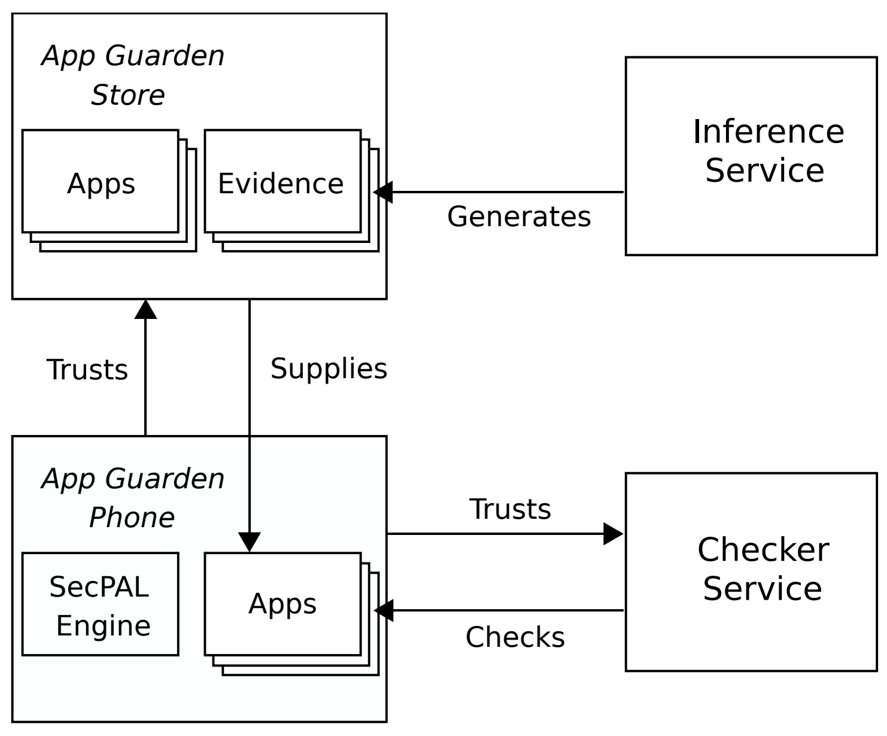
PROBLEM

Users trust the app stores not to supply them with malware but sometimes this trust is misplaced. Sometimes malware on mobile platforms isn't intentional: developers are not security specialists and sometimes make poor security decisions.

Our aim is to create a modified Android ecosystem where apps come with digital evidence for security and where users can say how they want apps to behave on their device.

APPROACH

We use the SecPAL authorization logic to see whether there is evidence to show that an app follows the user's policy for how their phone should behave.



Digital evidence will allow security properties to be shown and checked increasing trust that an app is secure. If evidence can't be produced we can use signed statements by trusted parties to attest the security properties.

RELATED WORK

The two biggest app stores do not say what security checks they do before selling an app; though they are believed to include static and dynamic analyses.

Other attempts to make apps more secure have included work on restricting app behaviour through fine-grained permissions; or by tracking and tainting data passed between applications.

Our approach adds to this by describing what an app is capable of and by giving a framework to describe and compare device policies.

STATUS AND FUTURE WORK

The project is at an early stage. We have started porting SecPAL and have begun exploring the device policies users have.

We want to evaluate these policies and see how effective they are at stopping malware on Android; and see whether enforcing a policy automatically reduces the inconvenience of manually authorising apps.

By formalising the device policies we hope to be able to describe the current device policies used by Apple and Google and compare them with each other.

Joseph Hallett

PhD duration: 3½ years.

http://groups.inf.ed.ac.uk/security/appguarden/Home.html