# A Summary of

### Resiliency of mobile OS security for secure personal ubiquitous computing

This Article was about a team creating a new security system for mobile operating systems. Actually it’s only for Android; which they don’t get to until the 2nd part. They named their Mobile OS Security Technique “DMOS” (Deep Mobile OS Security)

This security system has a few key parts, there’s an onion level defense mechanism that uses each layer of the system (user, application, kernel, framework, etc) to create defensive layers which will slow down and mess up attackers. Also It has role-based access control, which sandboxes data for better control. They also make “certified users” who can only access phones they’re certified in.

They use the term “**Cyber Resiliency**” a lot in this article, and it’s primary definition in this article seems to mean that the data is less mutable and difficult to access outside of *certified* user agents. Their techniques for resiliency use many specific keywords that are unnecessary and annoying. In order to asses their resiliency, they created some metrics for the measurement of *cyber resiliency*. 1st is that many assumptions should be solved to use the metrics beforehand. This doesn’t make sense, none of the authors appeared to be native English speakers, so maybe there was a translation error.

Besides the poor grammar, this project seems actually pretty neat. The point of the research and DMOS is to make the Android OS more resilient to attacks, locks anything out that shouldn’t be there. They tested against USB,SMS,SIM,SD and other acronyms for data transfers and the attacks were all blocked. They expect to be able to move these ideas to IoT after placing them in Android. It’s pretty neat.