Editorial: Security of Mobile Devices

We are a journal on embedded computing. Mobile devices such as mobile phones, tablets, and other devices are part of the embedded computing world. The recent push in India to use mobile wallets and mobile banking by the government has created a lot of concern among computer professionals and policy makers alike. Is it safe to link your bank account or do banking on your mobile devices? This is not a problem of a particular country that is trying to leapfrog its population into a digital economy without adding adequate technological, legal, and policy frameworks for the security of transactions over the mobile devices. It is more or less a problem for most countries around the world.

Looking into the technological challenges, we found that the security of mobile devices is quite weak, to say the least. As per DeviceAtlas [1], as of Q1 of 2017, in Australia, Android 6.0 was in approximately 65% of phones, whereas Lollipop and earlier versions are still in about 35% of phones. In Canada, the numbers are quite similar. On the other hand, in Brazil, only about 35% have moved to Marshmallow (i.e., 6.0), and in Argentina, even less, at about 25%. In India, 30% of phones have Marshmallow, and 70% have earlier versions Marshmallow. Moreover, in India, about 25% phones are using versions below Lollipop. Why are these statistics of interest? Recall that, in October 2016, a Linux kernel bug named “Dirty COW” (CVE-2016-5195) came out, and because Android is also based on the Linux kernel, it was found to have the problem. A number of exploits that could gain temporal root on Android versions below Marshmallow were found, and Google patched it in November 2016. Here comes the problem. A lot of people in countries like India do not get such patches or upgrades of Android versions for two reasons: first, cheap phone manufacturers often do not offer an “on the air” upgrade or fix in time; and second, even when offered, it costs 100MB or more data to accept the patch. There is no legal or regulatory framework to force the mobile carriers to offer this data for free, and data is expensive. This leads a large section of the population to not accept any “on the air” upgrade. In our lab, we created Dirty Cow exploits quite easily to obtain the most sensitive information out of Android phones where the fixes were not applied.

A quick glance at CVE Details [2] would reveal the extent of this versioning problem and the lack of cyber hygiene that originates from not receiving timely patches and version upgrades. In 2017, a total of 1,098 vulnerabilities in Android have been reported. Of them, 309 are privilege escalation vulnerabilities. Exploits of all of these are easily available, especially for criminals savvy in the dark web.

If you are doing banking on your Android device and you get hit by a malware that can escalate privilege, install a key logger, or even actually access various sensitive information on your phone, should you be doing banking on your phone? Those who urge the common people to do banking over their mobile devices should look at CVE Details [3] before giving ill-advised ideas to the not so technology-savvy population.

There are other problems such as QSEE (Qualcomm Secure Execution Environment) [4] vulnerability, which relates to Qualcomm processor-based mobile phones. QSEE is a secure execution environment where cryptographic computation is supposed to happen in a special hardware partition, which is not accessible directly by any application. It turns out, bugs existed that compromised the trust zone, so the untrusted zone can

have access to all of it. There goes all the secret keys and all the special arrangements for bootstrapping trust, and so on.

And then there is this—Google Play Store seems host many malicious applications, Trojans, and malware that exploit various vulnerabilities to exfiltrate data, install key loggers, and, in some cases, just brick the phone.

There is a lot more to this than we can discuss in an editorial. However, in India, there is also a push to use biometric authentication to enable banking. Since a nationwide collection of biometry of each individual launched for “unique identification”—and people were forced to link their bank account to this biometric identification—politicians want the people to start transacting for banking and payments just using fingerprints. We will discuss the dangers of this entire notion and the lack of security in the fingerprinting devices another time. However, given that mobile phones are being touted as the gateway to banking and payment, as embedded systems and security thereof is of utmost importance to help the unsuspecting population from being robbed of their money, we need to vigorously question this kind of move—no matter which country makes such attempts. We should also work on securing mobile devices and mobile banking and on finding better ways to protect the phones from malware and exploits, and we must also profoundly warn the public of the dangers until we can fix this once for all—if at all possible.

We would like to see some special issue proposals on security of mobile devices, mobile applications, mobile chipsets, the secure execution environments in mobile devices, and other topics relevant this issue. We as a community should enhance our efforts to make mobile devices safer for people, lest policy makers start pushing them to even vote in elections with their mobile devices.

In this last issue of Volume 16, we have one special issue section on “Secure and Fault Tolerant Embedded Computing” and a large number of regular articles. The articles range from real-time simulation support for cyber physical systems, synthesis of controllers, synthesis of application specific RTOS, better caching behavior prediction, and a variety of topics. A number of special issues are waiting around for Volume 17.

In closing Volume 16, I must thank the ACM publications office, especially Ms. Laura Lander for her incessant support and the tremendous help she renders to ACM publications, in particular to *TECS*. Ms. Jeyel Tecson left the journal assistant position in the middle of this volume after 3 years of great service, and Ms. Arriane Bustillo has taken over. We thank both of them for their help and service. Our production in charge Ms. Kelly Crooks has been as always a wonderful project manager, and we owe big thanks to her to keep the production process on time and painless.

We look forward to your continued indulgence in Volume 17 as well.

Sandeep K. Shukla

Indian Institute of Technology Kanpur

Editor-in-Chief

[1] <https://deviceatlas.com/blog/android-versions-market-share-2017>.

[2] http://www.cvedetails.com/product/19997/Google-Android.html?vendor_id=1224.

[3] http://www.cvedetails.com/vulnerability-list/vendor_id-1224/product_id-19997/opgpriv-1/Google-Android.html.

[4] <https://duo.com/blog/sixty-percent-of-enterprise-android-phones-affected-by-critical-qsee-vulnerability>.