The Last Byte

Security Begins at Home

Scott Davidson

■ **OF THE MANY** interesting articles in this issue of *IEEE Design&Test*, one particular article by Zhou et al. grabbed my attention. The article showed that hardware performance counters, which count instances of microarchitectural events, cannot distinguish between a system in normal operation and a system under attack. One reason given is the gap between the functional behavior of a system and the behavior at the microarchitectural level. Therefore, it is best to look for incursions at the functional level and distinguish good from any suspicious behavior there.

This advice applies not only to security experts but to all of us. Not long ago, social engineering, where someone tried to solicit security information like passwords from an insider, happened only to workers in large companies. Now, it happens even to your grandmother.

Emails purporting to be from a tech company saying your account will be terminated unless you follow a forged link and give information is social engineering. So are the calls supposedly from Social Security or the Internal Revenue Service. It is interesting to consider how we detect (or do not detect) this activity.

As in hardware security, we look for activity that does not meet our model of the world. When there is a big mismatch, we can easily discard the bogus mail. For instance, I do not own or use any Apple products, so emails telling me my Apple account is being discontinued do not have a lot of success. We expect big companies to send emails that are of a certain quality, so emails full of spelling errors can be deleted.

It is not always so easy, for instance, when mail supposedly comes from a company you do business with. Just as in hardware security, you need a model of what a real email looks like, and the more detailed the model the better you can detect forgeries. Those who understand email can look at full headers and see where the mail really came from. Those who understand the web and HTML can browse over the link to see where it goes. A less sophisticated user can get fooled in no time.

An even better model involves what information a representative from a genuine company has on you. A caller from the criminal “Windows Company” got asked what operating system I use. That made them hang up.

This saved me when someone supposedly from my bank called me at 2 A.M. and claimed someone was misusing my debit card. Almost plausible, right? But I had the presence of mind to ask this person to tell me my home address. When he claimed he wasn’t allowed to do so, I knew it was a scam, burned his ear off, and hung up. I am usually not in a good mood at 2 A.M., not since I got out of college anyway.

As attacks become more sophisticated, we will need AI apps that can understand the computing and financial environments of users, build models of them, and intercept and stop fraudulent attacks. Some spam filters do this already and call blockers like NoMoRobo do it for spam calls, but they are not very sophisticated. We must do better to protect all internet users. And if these apps can answer criminal calls and say nasty things to the criminal caller, all the better. ■

Digital Object Identifier 10.1109/MDAT.2021.3068237
Date of current version: 20 May 2021.

■ Direct questions and comments about this article to Scott Davidson; davidson.scott687@gmail.com; Twitter: @scottd687.

Copublished by the IEEE CEDA, IEEE CASS, IEEE SSCS, and TTTC