Security Engineering Question Sheet 5: Lectures 9 and 10

Prof. Ross Anderson & Yuvraj Patel

Here are a set of questions to help you think through the topics covered in lectures 9 and 10, on Hardware Security 2 and Operating Systems 1.

1. A Rowhammer attack requires the rapid access of rows within the CPU's Random Access Memory. However, all modern systems have caches that act as a fast buffer for frequently accessed memory. Does such a cache make a Rowhammer attack impossible, given that it typically reduces the rate of access to main memory?

2. In side channel attacks, what is the difference between ”Flush and Reload” and ”Prime and Probe”? Is one of these more general than the other?

3. To eliminate Spectre attacks, your boss suggests you buy a processor without a cache. How effective do you think this might be, how feasible, and would there be any disadvantage?

4. Does SGX eliminate Spectre attacks? If so, how? If not, what does SGX achieve? Is SGX only beneficial in a data centre, rather than on end-consumer hardware?

5. “All access control is just a matrix matching users to files, so capabilities and access control lists are exactly equivalent.” How accurate is this statement?

6. “The mandatory access control mechanisms in Android just serve to take control away from the user and place it in the platform holder's hands. Any benefit to the consumer is just an illusion.” How accurate is this statement?

7. Why would Apple only store biometrics in their own proprietary Secure Enclave, rather than using TrustZone and/or allowing access to the iOS kernel more generally? Does this really improve security?