COSC 4765
Computer Security

Name: Jacob Tuttle

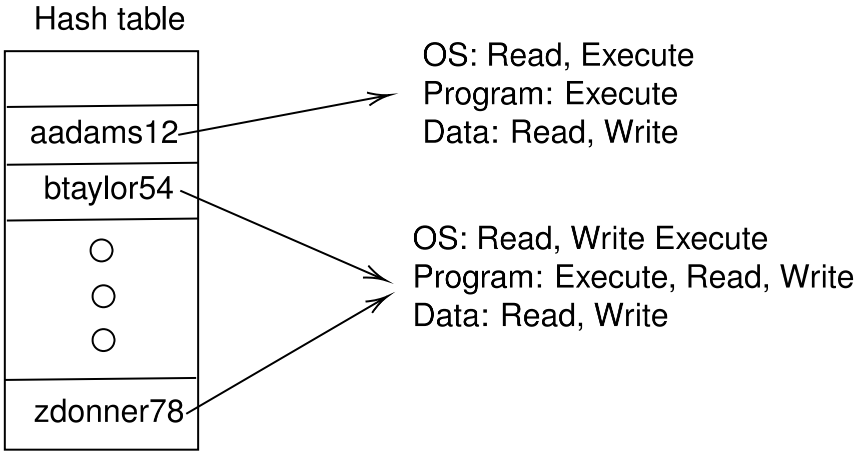
Homework 06

October 25, 2020

1. Large Scale Access Control

One of the largest limitation to using matrix based access control for a large organization is managing to find your way to the correct entry quickly. Even using some efficient sorting and searching system will require an increasing number of actions as the number of users grows into the hundreds of thousands. On top of that, storing all of that data, much of it repeated since there is a limited number of possible access right levels.

In order to build a data structure that allows for quick retrieval, let's try to leverage a hash table to do it. We can use the usernames to reference the users in a lockup table that points to the subset of possible rights they have access to.



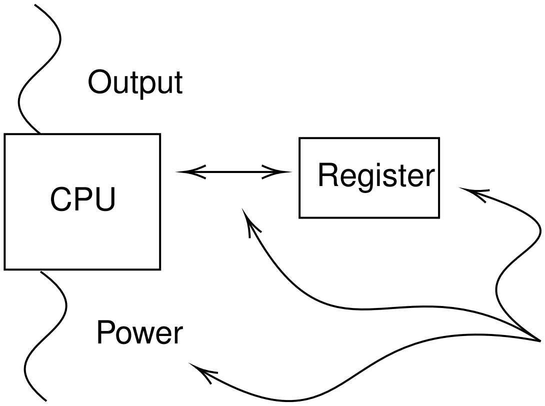
This will give us the ability to look up the access rights of a user in a single action. Since the lookup is stored in a hash table, we cut down a dozen or so operations to a single lookup. Then, since we simply point to one of the 512 possible subsets of access rights, we save repeating that information across hundreds of thousands of users.

Bonus

An implementation of this hash lookup is available here.

2. Side Channel Attacks

At the most basic level, a side channel attack tries to gain information about a system by measuring a byproduct of that system. For instance, modern CPUs draw electricity and power in expected ways depending on what kinds of operations it is performing. Two of the most famous side channel attacks exploited the concept of speculative execution and measured the delays that moving around bits on the computer would require.



An attacker can listen to any
of these places to get information
about the CPU and what its doing.