Steven M. Bellovin
https://www.cs.columbia.edu/~smb

Containers and their Limits

Containers

- Containers can be very useful
- However, they have their limitations
- Some of the most important use cases for containers run right into those limits

Walls and Doors

- Our security models depend on walls to contain the badness
- We need doors to communicate
  - A container is just a wall within a computer
- We're pretty good at building walls

Photo by Dominic Sherony via Wikimedia Commons

Actually, Our Walls Aren't Always Great

The Real Problem is our Doors

Picture source unknown

What's Wrong with Doors?

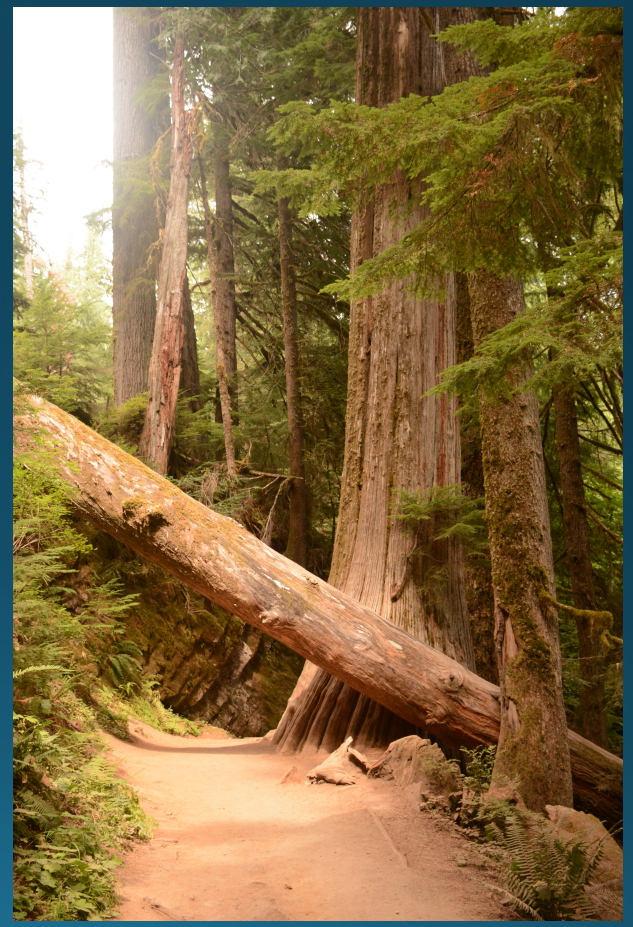
- Sometimes, the policies are wrong
- Sometimes, the implementations are wrong
- Sometimes, the necessary functionality *requires* dangerous policies or code

We Have to Talk to our Containers

- Imagine a web browser container
- We want to save files
- We want to send it URLs from email messages
- We want to click on mailto: URLs

We Have to Talk to our Containers

- Imagine a web browser container
- We want to save files
- We want to send it URLs from email messages
- We want to click on mailto: URLs
- No doors?
- If a tree falls in the forest and no one hears…



Limitations

- Containers can help prevent persistent attacks
- But…
  - Attackers (especially more sophisticated ones) can exploit doors to break out of the container and achieve persistence that way
  - Sometimes, important resources (e.g., Web encryption keys) have to be inside the container
  - If the container is insecure, the attacker can simply penetrate it anew each time it's closed and restarted
- Containers can help, but they're not a panacea
- They are software and they encapsulate software, and hence are subject to all of the ills appertaining thereto

Questions?