Threat models and Composable systems
Workshop on open source secure enclaves

Prakash Ramrakhyani
Arm Research
SSITH: System Security Integrated Through Hardware and Firmware

SSITH threat model classifies an exhaustive list (2800) of existing vulnerabilities into 7 categories. This threat model views the system as a whole.

This may be a useful way to define a threat model but there can be others.
Before we get to discussing more about threat models,
If you are asked to relate a secure system with one of these images, which one would you pick?
Security Perspectives

- Level of security depends on how cost of breaching security compares with perceived value of asset being secured.

- The same vulnerability may or may not be a problem depending upon the use case
  - Eg: Data from humidity/alkalinity sensors in a home owner’s lawn v/s sensors employed on a commercial farm

I contend that all the images on the previous slide are valid answers
Many factors influence the choices made in building a system and systems are often composed of components/elements arriving from different sources.

It may be useful to define threat models for individual components as well.

*(Note: Software layers are included under compute in this slide for simplicity.)*

**Threats on compute elements:**
Buffer errors, Crypto errors, Permissions and privileges, Information leakage, Numeric errors, Code Injection, Resource management

**Threats on memory elements:**
Unauthorized reads, Unauthorized writes, Replay attacks, Resource management

**Threats on I/O elements:**
Information leakage, Resource management
Differential Security

- Define security levels of system components based on susceptibility to various threat levels
  - Security level of the system is a function of the security level of individual components and how they have been glued together
- Users/use-cases specify what threats and vulnerabilities are relevant to them and the system is built based on requirements and budget
- Continuous monitoring of new threats and vulnerabilities to refine security levels
- Automation needed to scale.