Security/Privacy & Assured Autonomy

Howie Shrobe

MIT CSAIL

Panelists

- Tony Dahbura – Johns Hopkins
- Jeremy Daily -- Colorado State
- Greg Falco –MIT & Stanford
- Ryan Gerdes – Virginia Tech

Assured Autonomy

The expectation that a system entrusted to make decisions on its own, will with high probability:

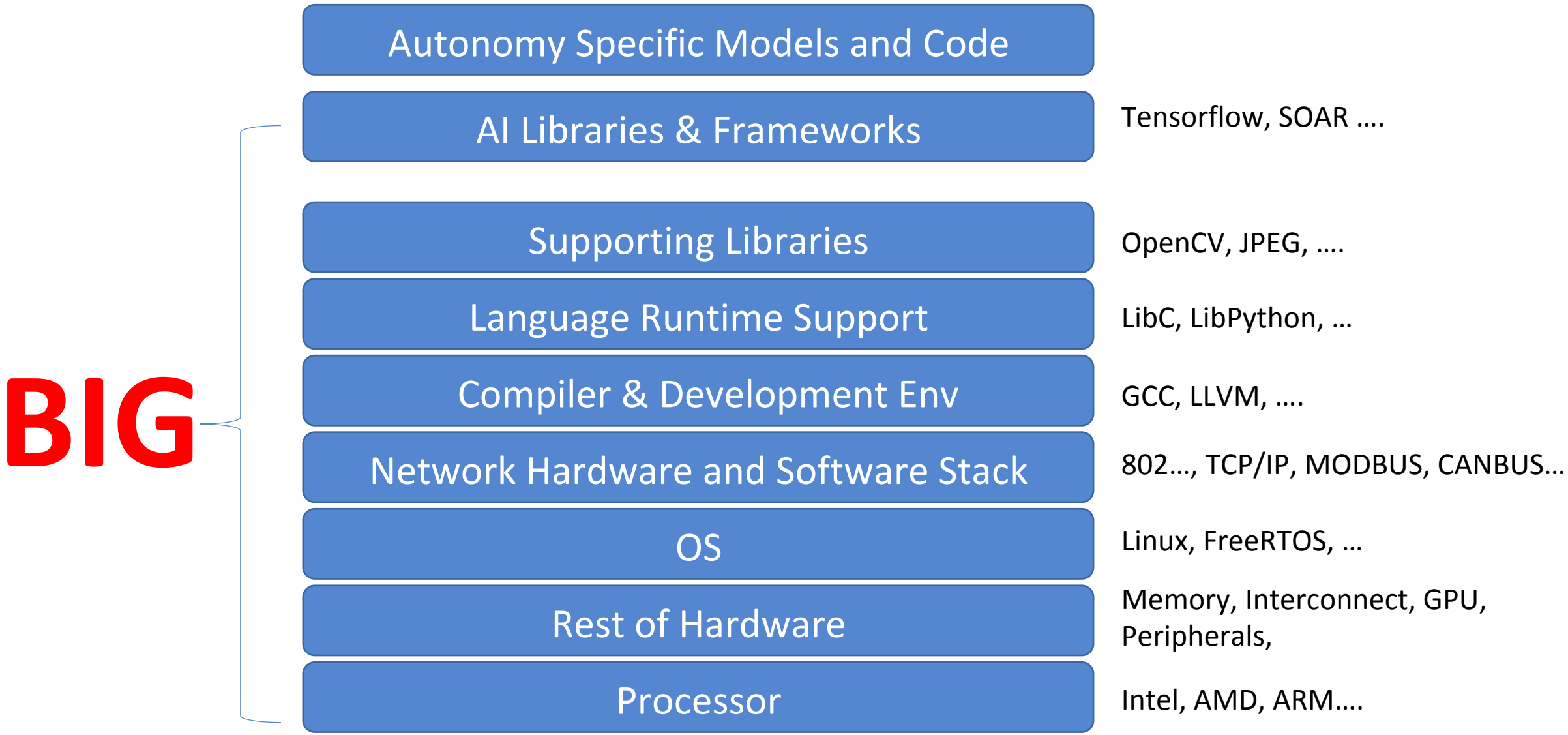
- Make good enough decisions to achieve (most of) its goals without causing (much) harm
- Be able to explain & justify those decision

- A secure system is one that will behave as designed and implemented even when under attack
  - Normally thought of as Confidentiality, Integrity and Availability
  - For Cyber-Physical systems must also include predictable timing, etc.

- Security is necessary condition for Assured Autonomy

Cars are (unsafe) rolling computers

An Autonomous System Stack



Tensorflow vulnerability list

Advisory Number	Type	Versions affected	Reported by	Additional Information
TFSA-2019-001	Null Pointer Dereference Error in Decoding GIF Files	<= 1.12	Baidu Security Lab	
TFSA-2018-006	Crafted Configuration File results in Invalid Memory Access	<= 1.7	Blade Team of Tencent	
TFSA-2018-005	Old Snappy Library Usage Resulting in Memcpy Parameter Overlap	<= 1.7	Blade Team of Tencent	
TFSA-2018-004	Checkpoint Meta File Out-of-Bounds Read	<= 1.7	Blade Team of Tencent	
TFSA-2018-003	TensorFlow Lite TOCO FlatBuffer Parsing Vulnerability	<= 1.7	Blade Team of Tencent	
TFSA-2018-002	GIF File Parsing Null Pointer Dereference Error	<= 1.5	Blade Team of Tencent	
TFSA-2018-001	BMP File Parser Out-of-bounds Read	<= 1.6	Blade Team of Tencent	

Summary

- If we want to have any confidence in an autonomous system then its necessary (but not sufficient) to guarantee that vulnerabilities cannot be exploited to change the reasoning of the autonomy software
  - All data must carry meta-data
  - Policies related to the meta-data must be systematically enforced
  - Enforcement must be done across all levels
  - A “belt and suspenders” approach is necessary
  - Prevention + Containment