Autonomous Systems: Setting the Stage

Matthew Merzbacher
ADSA 23 ~~ May 4, 2021

SWWC: Is Autonomous Security Possible?

- ➔ Tesla & Waymo (and others) are creating autonomous vehicles
  - ◆ Remove human from loop
  - ◆ Claim to reduce accidents & costs
- ➔ Can self-governing security systems reduce/replace the human-in-the-loop?
  - ◆ Respond to (unpredictable) real-world conditions automatically and independently
- ➔ Automation versus Autonomy
- ➔ Examples, Risks, Next Steps
- ➔ What can we do? What should we do?

Waymo to begin testing its driverless ride-hailing service on the streets of San Francisco with employees as riders.

[Source: Waymo, February 2021]

Automated is not the same as Autonomous

Automated	Autonomous
Constrained, Rigid	Self-Governed, Adaptive
Closed Environment	Open Environment (“Real World”)
Task-based	**Goal-based (or even Mission-based)**
More predictable	May have unexpected behavior
Fail Hard	Fail Gracefully
Easier to set requirements	Harder to set requirements
Easier to assess success	Harder to assess
Ready today	May never be fully ready

Real World Examples (Automated or Autonomous?)

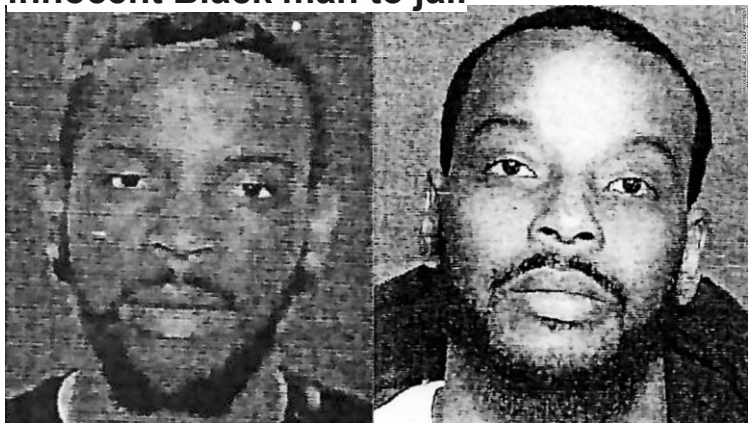
- ➔ Stock Trading / Smart Buildings
  - ◆ Execute a fixed (albeit complex) behavior
  - ◆ Other than recognizing panic, can usually default to “do nothing”
- ➔ Robotic manufacturing
  - ◆ Relies on a closed environment
- ➔ Voice Recognition & Response
  - ◆ Do these work for you?
- ➔ “Self-Driving” Navigation
  - ◆ Vacuums, Cars, Space Probes
- ➔ Autonomous TSOs
  - ◆ Is this bias?

[Source: *Crip Camp*, Netflix]

Needs and Concerns

- ➔ Data, Data, Data
- ➔ Goal-based autonomy will help handle emerging threats/conditions
- ➔ Need a measure of goal efficacy
  - ◆ Is it OK to measure task performance?
  - ◆ **Prescribing tasks kills autonomy**
- ➔ Pitfalls
  - ◆ Can we trust systems that we don't fully understand or that can adapt?
    - Tesla constantly monitoring and feeding back
    - We ***should*** consider that in security
  - ◆ How do we avoid bias?
  - ◆ Risks of testing on live systems

A false facial recognition match sent this innocent Black man to jail



[Source: CNN April 29, 2021]

A Few Specific Examples: Replacing/Reducing TSOs

- ➔ Should passengers self-validate their ID?
- ➔ Would you trust a robot to open and search your luggage?
- ➔ What about a terrorist's luggage?
- ➔ What about a robotic pat-down?

- ➔ Identify repetitive tasks for automation or autonomy to reduce cognitive load and vigilance decrement

What Next?

- ➔ Autonomous systems, even flawed, will outperform existing systems
- ➔ Start fielding and improving
  - Find “long-haul trucking” analogs
  - Add autonomy to existing systems
  - Broaden definition of “system” to include passenger, TSO, system, airport, everything!
  - Include vendors in assessment of performance and feedback in a comprehensive, honest, and validated manner
- ➔ Prepare for failure in many forms

NYPD has terminated its contract with the maker of a 'creepy' robot dog, following a fierce backlash over its use in policing

[source: Business Insider, April 29]