SEPTEMBER 2019

AUTONOMY AT SCALE

Intelligent Machines Advancing Technology to Improve our Future

noblis®

For the best of reasons

NOBLIS.ORG

TABLE OF CONTENTS

CHALLENGE: THE CYBERSECURITY ENVIRONMENT IN AUTONOMY AT SCALE

Sam Leestma

Autonomous machines are set for exponential growth—increasing both their footprint in new industries and their utilization in industries already leveraging autonomy. The future will see greater use of autonomous machines at scale for transportation, distribution of goods, military operations, and space exploration (Figure 1). As the use of autonomous technology grows, cybersecurity breaches of systems managing autonomous machine fleets and nodes will become a greater threat to individuals and to the security and functions of industries and nations as a whole. As space travel, mass transportation, food and goods distribution, and individual transportation become reliant on autonomous machines, the information about critical operations, logistics, and personal information will be trusted to systems operating mostly independent of human interaction. This dependence presents several key challenges in security design integration, the verification of security functionality, and the protection of operating systems and the metadata that they will rely on and produce.

Additional considerations must be made especially when examining the increased utilization of autonomous machines at scale for distribution of goods and food and transportation of people. Classified as critical infrastructure, these systems that can affect large portions of the population and require additional protections. Many protections surrounding current critical infrastructure systems (e.g., power grids, water facilities, telecommunications) rely on closed systems or security by obscurity. The far more open community of autonomous technology will have to be vigilant in detecting and mitigating threats. Monitoring and tracking the emergence of new threats and attack vectors will be critical to maintaining the viability of increased reliance on autonomy at scale (AaS).

Information about critical operations, logistics, and personal information will be trusted to systems operating mostly independent of human interaction.

Autonomous machines are also increasingly being used in military operations. Military services have leveraged drones for combat operations; the security and integrity of those autonomous machines will be important to preserve human safety. Special consideration will have to be paid for communications and protocols managing these machines to ensure decisions on hostile targets are accurate and effective against the threat. As the use of armed drones in active combat situations increases, the design must ensure the integrity of the protocols remain intact and function correctly.

Data Types and Critical Operations

To discuss protection mechanisms for application to autonomous systems and to define and validate levels of trust needed, we will need to explore the nature of the systems and the functions they support. The use cases affecting populations and the stability of nations, functions that support the movement and logistics of food and goods and the transportation of people present some of the most critical functions at scale. Autonomous nodes responsible for food and product distribution as well as mass transport will rely on systems that provide logistics and management of autonomous services (Figure 2). These centralized management systems will hold the information needed for their operation and their byproduct or metadata will draw the attention of unauthorized threat sources. As AaS becomes more integrated into the military and space industries, the security of nations will start to rely on the security and trust in operations of those autonomous systems and individual autonomous nodes.

The movement of food presents challenges because, if compromised, it can have national security and economic prosperity implications. The stability of a society relies heavily on the availability and integrity of the food supply, and the high assurance of the operations and security of systems that manage food distribution protects food supply safety. Those systems will need high availability to ensure populations have basic necessities. In examining the movement of goods, the availability of autonomous systems and nodes will be critical to organizations that leverage those technologies. A company's viability can tie directly to its ability to reliably move products to consumers. The movement of goods also presents a secondary concern. Companies that produce and distribute goods will focus on

Figure 1: Current and future implementations of autonomous machines at scale

maintaining the confidentiality of their logistical information. The movement, volume, and capacity of their distribution of products is integral to their strategic planning and corporate health. Loss of this material data can weaken a company. The challenge of metadata protection will be an important concern for companies as autonomous systems increasingly, process and store centralized logistical information.

Autonomous nodes that are responsible for food and product distribution as well as mass transport will rely on systems that provide logistics and management of autonomous services.

Space missions, by their nature, are operated by nation sponsors. They support coordinated international missions, transport commercial and national-interest satellites, carry equipment and goods for scientific experiments, and transport personnel. The large capital and human investment in space programs are critical to a nation and its security. Maintaining the integrity and availability of space missions involves all autonomous space machines reaching their intended locations and orbits. Conversely, the loss of that integrity or availability can result in the compromise of those autonomous space machines. Confidentiality of space missions (i.e., their flight contents, strategic operations, and goals for the sponsoring nation) will require protection to ensure the security of the nation states.

The military use case for autonomous machines includes military operations and transport of personnel and services. The military uses the critical logistical information produced and used by these systems to operate without the enemy's knowledge. Troop and equipment locations and movements are highly classified by the nature of their use. Additionally, the metadata used and produced by drones can contain military or intelligence information for target tracking and engagement, and the information about missions supported by drones can contain operations, their status, as well as logistical information about enemy combatants.

Threat Pairing for Critical Services

Each use case for AaS presents a unique threat profile based on the functionality and data present. Within each of the critical services, autonomous systems and their controllers use, produce, and store data and metadata. Each of these services and data elements will have multiple threat sources interested in exploiting it. Exercising vulnerabilities can produce losses in the confidentiality, availability, and integrity—elements of "trustworthiness" in most current discussions of autonomous systems. Myriad threat sources would find value in the theft of data, denial of services, and manipulation of the functionality or data used and processed on autonomous systems.

Simple threat sources such as script kiddies, whose motivation is accomplishment, notoriety, or simple mayhem, could apply to all use cases. The threat profiles for AaS for transportation of goods and services, military logistics, and space travel, however, are more targeted.

Figure 2: Data and metadata types present in autonomous systems

Each of these groups has unique motivations and each use case of autonomous machines and systems offers opportunities to advance their goals. Some implementations of AaS will support services that will mirror the importance of our critical infrastructure. Food transportation and goods distribution and logistics handled by autonomous machines will put these critical services into systems independent of human interaction. Food, medication, and critical equipment—fundamental to the wellbeing of citizens—will reside with systems that have multiple points of failure and access points that do not require human intervention to gain entry. Autonomous machine management systems will offer a single point or limited points of exploitation that can disrupt large scale critical services affecting large portions of a population. Hostile nations or economic criminals could have interest in denial of services or the integrity of the systems contents or the logistical operations. The use of autonomous machines for these services will mitigate the easiest point of attack from human coordinated physical attacks, to single nodes, to multi-point, to remote attacks that can affect fleets of nodes that are providing critical services.

As the operation and utilization of autonomous machines in more hostile and military environments will continue to increase, the threat profiles and the impact of compromises that those threat sources wish to achieve become more critical to the nations and individuals relying on those autonomous machines and systems. Successful attacks can result in loss of life and impact availability of critical supplies needed in dangerous situations. As the implementation of autonomous machines increases in the military community, the threat profiles can shift based on political and national or group lines. The shift to information warfare will result in more complex attacks on systems, which could expand to encompass autonomous machines and systems providing critical services. Physical attacks on single nodes will be replaced by cyber-attacks that can affect large swaths of military targets.

Physical attacks on single nodes will be replaced by cyber-attacks that can affect large swaths of military targets.

Known Cybersecurity Concerns

The infrastructure and systems in the AaS landscape face many current threats.

Many autonomous machines use Global Positioning Systems (GPS), a low-energy, unencrypted service susceptible to denial of service—intentional and unintentional—and vulnerable to snooping. As a core service that all autonomous systems rely on, GPS creates a single point of vulnerability with far-reaching consequences throughout the autonomous system.

Figure 3: Common autonomous machine hardware attacks

Sensor attacks, a form of exploit tricking sensors into giving false data, can affect the performance of autonomous machines and lead to widespread or isolated accidents resulting in traffic and route flow failures. Even isolated sensor attacks could result in the denial of service for critical operations. Sensor attacks on autonomous machines used for military operations can result in false target identification—and unintended human causalities. While these attacks generally result from physical tampering, sensors can also be manipulated by underlying hardware attacks (Figure 3).

Hardware attacks allow hackers, nation states, or any individual or group with access to the manufacturing or retrofitting processes to inject vulnerabilities into the hardware or firmware utilized by autonomous machines. This can result in complete compromise of the autonomous node or give the attacker the ability to affect services associated with the particular compromised piece of hardware.

Attacks on firmware updates can effect similar levels of compromise to those of hardware attacks. Firmware attacks can be accomplished through remote updates or from physical compromise of the onboard diagnostics (OBD) hardware ports present in an autonomous machine.

Remote Access such as Bluetooth and built-in Wi-Fi provides attackers with a vector to gain access to autonomous nodes. The system architecture of nodes and management systems vary greatly; each access point attack vector, if exploited, provides the ability to pivot and compromise a wide variance of a node that differs depending on the node (Figure 4). Once an attacker gains access, they may—depending on the architecture or security implementations present—install various viruses or malware, tracking software, or a wide array of unauthorized code. The impacts of these compromises can range from gaining complete control of a node, to monitoring the node, to degradation to the integrity of the node's operation.

Figure 4: Attack vectors applicable to autonomous systems and machines

CONNECTED VEHICLES: DETECTING AND VALIDATING AUTONOMOUS VEHICLE MISBEHAVIOR

By: Cory Krause

A significant factor in the success of the U.S. Department of Transportation's (USDOT's) Connected Vehicles program is the transmission of Basic Safety Messages (BSMs) between vehicles and infrastructure. BSMs are important, over-the-air messages that contain necessary vehicle data such as position, speed, acceleration and brake status. These BSMs can gather details about the traveling vehicle in real time and transmit this information to other vehicles and infrastructure devices in the area.

Such an open network poses certain risks regarding the reliability of the information contained within the BSMs. One possible threat comes from faulty sensors or components within the vehicle that could measure data erroneously and result in the transmission of inaccurate and/or unrealistic BSMs. Another possible threat comes from malicious third parties potentially hacking into the system and feeding misleading data while posing as a nearby trusted vehicle. Either scenario will result in BSMs that do not reflect the vehicle's actual behavior and can be considered misbehavior within the system. The accuracy of this data is an absolute necessity that carries the weight of a potential loss of life due to spoofed or inaccurate messages that misrepresent a vehicle's location and can cause a tragic collision.

Noblis is leading a USDOT project that creates an installable piece of code on connected and autonomous vehicles (CAVs) that detects BSMs in the area and determines their accuracy. This work includes several tasks:

- **Development of algorithms for detecting and qualifying misbehavior**
- **Creation of code, installable to the vehicle on-board units, that detects and flags incoming vehicle misbehavior**

- Testing of the code through the installation and trial of misbehavior in connected and autonomous vehicles (CAVs)
- Development of a formatting and reporting mechanism for credentialed hardware, which allows for credentials to be revoked from misbehaving devices

Noblis has developed software that reads a large amount of Basic Safety Messages (BSMs) over the air in a 300 to 500-meter area. Using these heterogeneous data points, we attempt to determine several pieces of important information—most notably, are the vehicles likely where they say they are, and is it physically possible that they are doing what they say they are doing. Many times, the spoofed messages resulting from hacking into the system are not realistic—whether because the hacker doesn't have an in-depth understanding of the system they are attacking or because they simply want to create havoc. Upon checking all the fields for realistic values (e.g., speed, acceleration, brake status), the software flags anything outside the realm of possibility. This could be a speed over 100 miles per hour or some wheels braking while accelerating. The software also handles the more complex task of determining location accuracy. By comparing latitude and longitude of all vehicles in a physical space and the surrounding area, we can use a low false-negative approach of removing and flagging the vehicles that could not be within the physical space.

The software then sends these flags to an authority that checks them and, if accurate, adds the devices to a credential revocation list that removes the ability for these devices to send messages in the future. In this way, whether it be through malevolency or malfunction, the devices can no longer impact the travel of those vehicles around them. The devices will then be checked by vendors and local transportation agencies to determine the problem.

Noblis is leading this effort of detecting and validating autonomous vehicle misbehavior through another autonomous system. Such forward-thinking approaches will likely be included in CAVs for years to come.

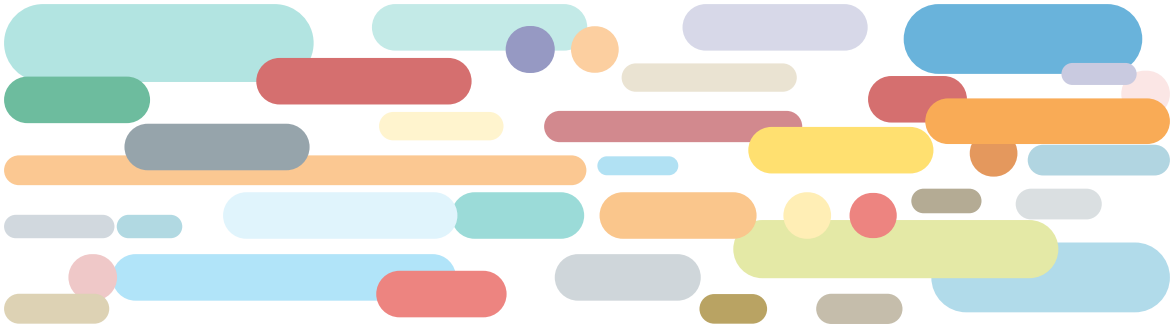
Securing Autonomy at Scale

Technical countermeasures will need to be developed and enhanced, and autonomous nodes and management systems will have to be retrofitted to include these security and redundancy implementations. To be resilient to unique threats and a wide range of large-scale attacks, the movement toward Autonomy at Scale (AaS) must prioritize security as a focal point in the progress of autonomous innovation. The use of security mechanisms and security function isolation needs to be employed with autonomous machines as fleets grow and become a critical part of the daily lives of individuals, governments, military, and commercial industries.

While current security mechanisms can and should be leveraged in the development and integration of these systems, new countermeasures to mitigate the unique threats to autonomous systems must also be developed. For example, the security challenges present in GPS systems will have to be analyzed, mitigated, and integrated to support AaS. The use of currently established security practices such as encryption, key infrastructure, hardware protections, and intrusion detection systems will need to be incorporated to ensure that not only autonomous nodes, but also control systems are protected. Supply chains for hardware and parts will need to be tightly monitored and managed. The sourcing of materials, chips, and technologies will have to be analyzed, and trusted partners must be established. Robust intrusion and anomaly detection will need to be in place and fine-tuned. Systems will need to detect allowable variance to position and operating status and have defined response conditions. These systems will have to be sufficiently redundant to ensure detection of small issues so that isolated anomalous conditions do not create widespread outages. Even small variations in coordinates and GPS position can create catastrophic consequences.

LOOKING FORWARD

As AaS creates a boon in productivity and consistency in transportation and logistics and as the community and businesses increase capacity and functionality in autonomous machine vehicles, new threats and opportunities to exploit critical functions in society will arise. Novel and increased thought needs to be given to the security considerations of these systems. The rapid progress and increased reliance on autonomous systems will quickly outpace the cybersecurity needs unless we pay special attention to current and upcoming challenges in securing these systems. Standards in architecture, security measures and compliance frameworks must be developed and integrated into the lifecycle of these autonomous nodes and systems. Throughout the history of information technology, functionality progress and innovation often take the lead. Leaving security as an afterthought has caused the loss of information to foreign adversaries, financial loss to cyber criminals, and loss of private information. In the case of AaS, the cost of lagging behind in security will manifest itself in dangerous breaches and exploits that can impact national security and safety.



ABOUT NOBLIS

Noblis is a nonprofit science, technology, and strategy organization that brings the best of scientific thought, management, and engineering expertise with a reputation for independence and objectivity. We work with a wide range of government and industry clients in the areas of national security, intelligence, transportation, healthcare, environmental sustainability, and enterprise engineering. Together with our wholly owned subsidiary, Noblis ESI, we solve difficult problems of national significance and support our clients' most critical missions.

NOBLIS.ORG

noblis®

For the best of reasons

703.610.2000 answers@noblis.org @NoblisInc