FORTRA

GUIDE *(Beyond Security)*

The Importance of Black Box Fuzzing in Key Industries

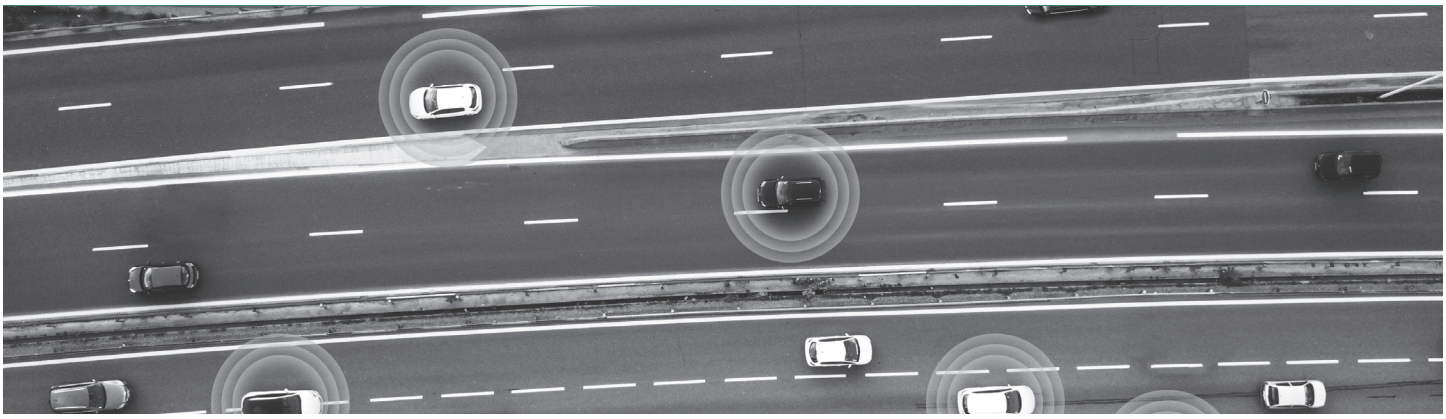
Fuzzing is key to protecting vital components of our connected lives – from smart cars and medical devices to airplanes and industrial control systems.

Introduction

Black box fuzzing has become an important tool in the dynamic application security testing (DAST) arsenal used by software developers and security professionals. For example, in its software development lifecycle (SDLC), Microsoft requires fuzzing at every interface of every product. As software drives more and more components of our daily lives, finding security vulnerabilities and addressing them before cyberattackers exploit them becomes increasingly important.

"Smart" devices and those on the Internet of Things (IoT) are particularly vulnerable. But not all vulnerabilities have equal impact. A connected refrigerator ordering 10 gallons of milk instead of one isn't a huge problem but self-driving cars that suddenly stop seeing obstacles could be catastrophic.

Any device or system that's operated by or with the use of software is vulnerable to attack. That's why companies began adding security to the entire SDLC, leading to security being "baked into" the process and the term secure software development lifecycle (SSDLC). But some industries present such a potential for disastrous problems that regulations require black box fuzzing to help ensure software security. In this guide, we'll look at four industries — automotive, aviation, medical devices, and industrial controls — where black box fuzzing is required or recommended and examine some of the possible consequences of non-compliance.



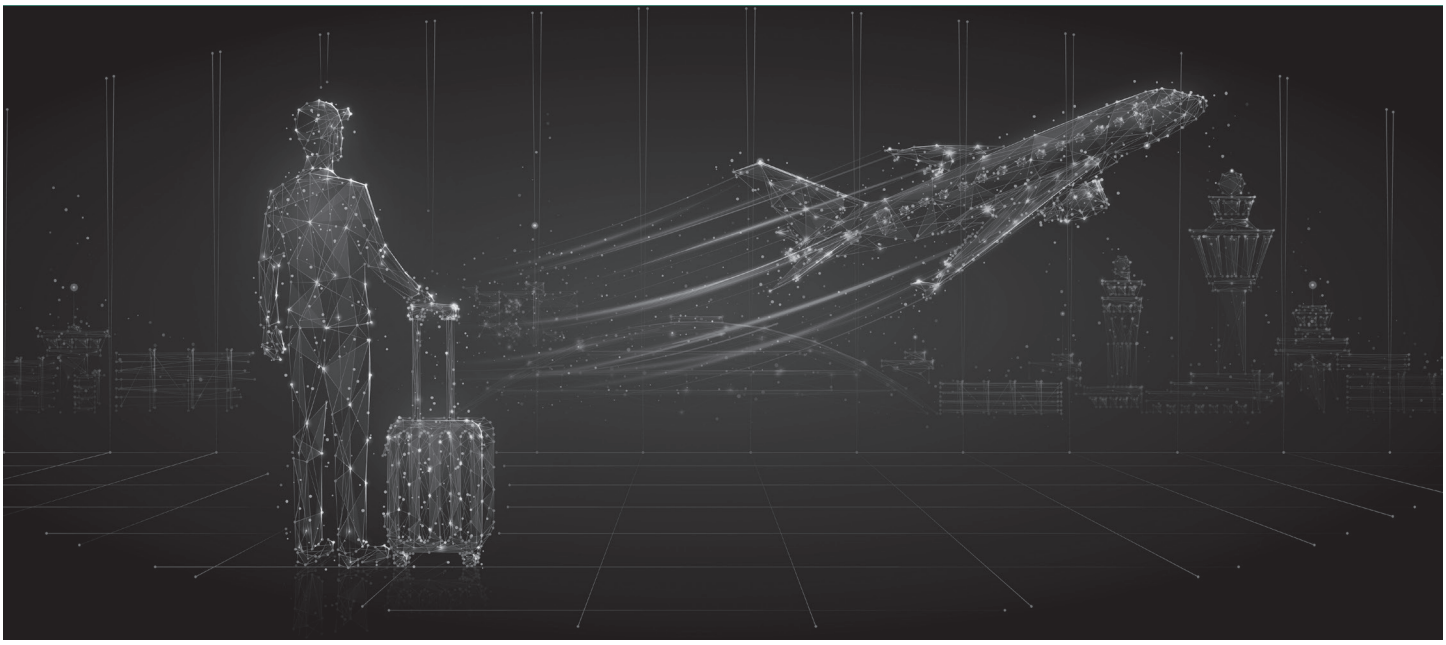
Securing Connected Cars – The Automotive Industry

Automotive technology has come a long way since the first Model T rolled off Henry Ford's Detroit assembly line in 1908. Unfortunately, recent automotive advancements have created tremendous opportunities for malicious hackers and other bad actors to cause harm. CANbus systems developed in the 1980s to facilitate communications between automotive systems are now present in most vehicles on the road. As auto engineers rushed to take advantage of the new technology, they didn't always consider the security implications, leaving a plethora of weaknesses in their wake. A simple online search reveals how-to information that can allow hackers to quickly and easily take control of key systems. In addition to CANbus systems, modern cars include info-tainment systems, satellite communications capabilities, Bluetooth connections, and more that all use some form of connectivity, making them vulnerable to exploitation. And perpetrators don't even need to be anywhere near the vehicle.

For example, about 82% of auto cybersecurity attacks around the globe were carried out remotely in 2021, according to a report from vehicle cybersecurity firm Upstream. And while car takeovers like the well-known Jeep incident in 2015 make splashy news, more than 40% of the attacks in 2021 targeted OEM back-end servers that store vehicle location data and can remotely control vehicle locks, ignition switches, and more. Attacks of this sort can give cybercriminals access to vehicles, or fleets of them, as well as OEM's company data. There are an estimated 125 million internet-connected cars on the road worldwide in 2022 but hardening those connections against outside intruders hasn't been as widespread. That's where black box fuzzing comes in, helping software developers and manufacturers use the same technique a criminal would to uncover vulnerabilities first and fix them before they can be exploited.

Looking forward, the number of connected cars is predicted to triple by 2035, making automotive cybersecurity very important. ISO/SAE 21434, the most recent standard released by the International Organization for Standardization (ISO) and Society of Automotive Engineers (SAE), calls for technology in electrical and electronic systems to prevent cyberattacks. It also requires vehicle and parts manufacturers to use processes that incorporate Security Design Principles, which direct software and application developers to consider possible attacks and prioritize information security. The UN Economic Commission for Europe (UNECE) has released similar standards, WP 29.R155 and R156. The idea is to address potential vulnerabilities throughout the SDLC rather than separating security into its own unit or leaving it until the end. It applies to both original equipment manufacturers and all others in the automotive supply chain. The ISO/SAE 21434 standard also requires manufacturers to continue to monitor vehicles for existing and unknown vulnerabilities for more than 10 years after the initial sale. One of the best ways to uncover unknown vulnerabilities as part of SSDLC is the use of fuzzing.

As an increasing majority of vehicles use connectivity to power internal systems and communicate with external networks, consumers won't have much opportunity to avoid vulnerable technology. They will, however, remain sensitive to highly publicized breaches that can damage a brand overnight. More importantly, perhaps, manufacturers, insurers, and others in the supply chain may find their own systems, proprietary designs, and private data compromised by attackers accessing vehicle system vulnerabilities that could have been uncovered with the use of black box fuzzing prior to release.



Protecting Planes and Passenger Data - The Aviation Industry

Safety protocols have long been built into aviation around the globe as government agencies seek to protect passengers and business interests work to secure assets and reputations. But as more systems have become automated and continuous connectivity on aircrafts and in airports is the norm, the size of the threat surface has increased significantly in recent years.

Onboard systems relay information back and forth within the plane while data also whizzes between aircraft and the ground, creating a huge potential for exploitable vulnerabilities. Because of the interconnectedness and international implications for any aviation incident, problems can quickly snowball to cause significant financial, reputational, and safety repercussions.

Regulation (EU) 2018/1139, the latest requirements from the European Union Aviation Safety Agency, mandates compliance with cybersecurity measures from software design through development and even instructions for secure operation later. The agency is also working on developing standards that encompass the risks associated with larger information ecosystems including air traffic control and the entire aviation supply chain.

Following the White House's Executive Order on Improving the Nation's Cybersecurity, issued in May 2021, the Federal Aviation Administration (FAA) has shifted to a Zero Trust approach for the aviation ecosystem. Like the European regulations and those in other industries, the FAA has called for SSDLC by including security protections and testing early in the design and development of systems rather than after deployment.

While fuzzing could be used to achieve the aims of many security regulations, ED-203A / DO-356A, the latest standards from European Organisation for Civil Aviation Electronics and the Radio Technical Commission for Aeronautics in the US, actually require it outright. Fuzzing is part of refutation tests and analysis called for in the standards.

As in the automotive sector, cybercriminals could certainly take over planes, causing them to crash. But modern criminals, even state-sponsored ones, seem much more intent on holding data for ransom, stealing proprietary information, and causing economic upheaval. Fuzz testing can help OEMs and others identify vulnerabilities and determine the efficacy of security solutions. With the aviation industry expected to generate 98 million terabytes of data by 2026, black box fuzzing can help meet regulatory requirements for hardening systems and protect against unforeseen exploits.

Shielding Medical Devices – The Healthcare Industry

The need for security in the automotive and aviation industries may have seemed clear and obvious from early in the industries' lifespans, yet technology as vital as that found in medical devices has only recently begun to be regarded in the same manner. The ever-increasing scourge of attacks on healthcare organizations shows that cybercriminals are well aware of the potential vulnerabilities in this industry. Individual devices can be hacked but the broader threat involves using device security flaws to breach networks and entire systems. The technological pivot necessary to continue providing care during the pandemic has also increased the opportunities for attack.

Vital data has been held for ransom in major hospital systems and small clinics have had their entire data chain wiped out by bad actors. In fact, the cost of data breaches in healthcare totaled $9.23 million, the highest of all industries, according to a 2021 report by IBM. Healthcare providers experienced 712 data breaches in 2021 with more than 80% of those caused by malicious external actors and unauthorized insider access, according to HIPAA Journal. Unfortunately, the industry has historically spent significantly less on cybersecurity than others.

Thankfully, the tides are beginning to turn. In 2022 the FDA released draft guidance on medical device cybersecurity that calls for a secure product development framework (SPDF) similar to SSDLC. It includes security by design, says cybersecurity is inseparable from device safety, and calls specifically for fuzz testing. The guidance directs manufacturers to retain evidence of testing and other aspects of risk management to show compliance.

In addition to the loss of data, poor care outcomes, and even death associated with healthcare cyberattacks, there's also the financial cost. Hospitals spend about 65% more per year on marketing in the two years following a data breach, according to a study published in the American Journal of Managed Care. The extra cost and effort to reassure a skittish public and repair the hospital's image come at a time when facilities are already overburdened with increasing costs, staffing problems, and pandemic-related concerns. Experts agree that simple measures like educating staff on secure passwords and limiting access to systems combined with powerful testing such as black box fuzzing, could significantly reduce the threat. As the FDA has noted, black box fuzzing has a key role to play in securing the nation's healthcare system and restoring the faith of patients.

Safeguarding Industrial Control Systems

Industrial control systems (ICS) are a key part of modern infrastructure, including water treatment, power generation and distribution, transportation, and chemical manufacturing facilities. The sheer complexity of these operations often requires machine control. However, ICS organizations, in search of efficiency, have opted for off-the-shelf software instead of creating systems in-house. This combination of critical operational technology and modern IT elements has opened the industry to the same threats as traditional IT environments. Attacks on ICS facilities began in 2010 with the Stuxnet worm and have only increased in number and expense around the globe. Attackers can easily find vulnerabilities by fuzzing unsecured systems.

Targeting critical infrastructure is highly attractive to cybercriminals precisely because of the potential for a large impact. A cyberattack that disrupts, debilitates, or disables such systems could be damaging to human life, the environment, supply chains, and more. The Colonial Pipeline ransomware attack in 2021 resulted in a ransom payment of $4.4 million but pipeline operations were halted temporarily, leading to gasoline shortages, price spikes, and panic across much of the eastern US. The White House issued its Executive Order on Improving the Nation's Cybersecurity shortly thereafter. Moves to secure US ICS are critical since the country is targeted by 69% of all critical national infrastructure attacks, according to Symantec. As a result of the order, the National Institute of Standards and Technology (NIST) published a list of minimum standards for software vendors and developers that included the call to "run a fuzzer" as part of DAST. NIST noted that fuzzer inputs frequently uncover bugs in software.

Of all the industries mentioned in this e-book, ICS and critical national infrastructure attacks have the highest potential to cause catastrophic problems for the greatest number of people. Black box fuzzing is a key tool in SSDLC and guarding against intrusion by cybercriminals who will definitely fuzz infrastructure systems looking for a way in.

Black Box Fuzzing – The Sensible Choice

When something as available and recommended as black box fuzzing exists, it must be considered in the face of the potential consequences of a cyberattack on any of the key industries mentioned here. Given the increasing boldness and escalating targets of cybercriminals, it's safe to assume that even a seemingly small breach or one against a minor target could simply be a trial run for something larger. State-actors, state-supported groups, and criminal gangs are all competing around the globe to cause as much financial, supply chain, and overall disruption as possible. Automated fuzzing used to hammer a system looking for a way in is a key tool for these bad actors. It just makes sense for software and system developers to employ the same tool, black box fuzzing, as part of a secure software development lifecycle to keep the bad guys out.

FORTRA

Fortra.com

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.