Tuesday, February 28, 2017

Hacking Robots Before Skynet

By Cesar Cerrudo (@cesarcer) and Lucas Apa (@lucasapa)

Robots are going mainstream in both private and public sectors - on military missions, performing surgery, building skyscrapers, assisting customers at stores, as healthcare attendants, as business assistants, and interacting closely with our families in a myriad of ways. Robots are already showing up in many of these roles today, and in the coming years they will become an ever more prominent part of our home and business lives. But similar to other new technologies, recent IOActive research has found robotic technologies to be highly insecure in a variety of ways that could pose serious threats to the people and organizations they operate in and around.

This blog post is intended to provide a brief overview of the full paper we've published based on this research, in which we discovered critical cybersecurity issues in several robots from multiple vendors. The goal is to make robots more secure and prevent vulnerabilities from being used maliciously by attackers to cause serious harm to businesses, consumers, and their surroundings. The paper contains more information about the research, findings, and cites many sources used in compiling the information presented in the paper and this post.

Robot Adoption and Cybersecurity

Robots are already showing up in thousands of homes and businesses. As many of these "smart" machines are self-propelled, it is important that they're secure, well protected, and not easy to hack. If not, instead of helpful resources they could quickly become dangerous tools capable of wreaking havoc and causing substantive harm to their surroundings and the humans they're designed to serve.

We're already experiencing some of the consequences of substantial cybersecurity problems with Internet of Things (IoT) devices that are impacting the Internet, companies and commerce, and individual consumers alike. Cybersecurity problems in robots could have a much greater impact. When you think of robots as computers with arms, legs, or wheels, they become kinetic IoT devices that, if hacked, can pose new serious threats we have never encountered before.

With this in mind, we decided to attempt to hack some of the more popular home, business, and industrial robots currently available on the market. Our goal was to assess the cybersecurity of current robots and determine potential consequences of possible cyberattacks. Our results show how insecure and susceptible current robot technology is to cyberattacks, confirming our initial suspicions.

Cybersecurity Problems in Today's Robots

We used our expertise in hacking computers and embedded devices to build a foundation of practical cyberattacks against robot ecosystems. A robot ecosystem is usually composed of the physical robot, an operating system, firmware, software, mobile/remote control applications, vendor Internet services, cloud services, networks, etc. The full ecosystem presents a huge attack surface with numerous options for cyberattacks.

We applied risk assessment and threat modeling tools to robot ecosystems to support our research efforts, allowing us to prioritize the critical and high cybersecurity risks for the robots we tested. We focused on assessing the most accessible components of robot ecosystems, such as mobile applications, operating systems, firmware images, and software. Although we didn't have all the

physical robots, it didn't impact our research results. We had access to the core components, which provide most of the functionality for the robots; we could say these components "bring them to life."

Our research covered home, business, and industrial robots, as well as the control software used by several other robots. The specific robot vendors evaluated in the research are identified in the published research paper.

We found nearly 50 cybersecurity vulnerabilities in the robot ecosystem components, many of which were common problems. While this may seem like a substantial number, it's important to note that our testing was not even a deep, extensive security audit, as that would have taken a much larger investment of time and resources. The goal for this work was to gain a high level sense of how insecure today's robots are, which we accomplished. We will continue researching this space and go deeper in future projects.

An explanation of each main cybersecurity issue discovered is available in the published research paper, but the following is a high-level (non-technical) list of what we found:

- Insecure Communications
- Authentication Issues
- Missing Authorization
- Weak Cryptography
- Privacy Issues
- Weak Default Configuration
- Vulnerable Open Source Robot Frameworks and Libraries

We observed a broad problem in the robotics community: researchers and enthusiasts use the same - or very similar - tools, software, and design practices worldwide. For example, it is common for robots born as research projects to become commercial products with no additional cybersecurity protections; the security posture of the final product remains the same as the research or prototype robot. This practice results in poor cybersecurity defenses, since research and prototype robots are often designed and built with few or no protections. This lack of cybersecurity in commercial robots was clearly evident in our research.

Cyberattacks on Robots

Our research uncovered both critical- and high-risk cybersecurity problems in many robot features. Some of them could be directly abused, and others introduced severe threats. Examples of some of the common robot features identified in the research as possible attack threats are as follows:

- Microphones and Cameras
- External Services Interaction
- Remote Control Applications
- Modular Extensibility
- Network Advertisement

- Connection Ports

A full list with descriptions for each is available in the published paper.

New technologies are typically prone to security problems, as vendors prioritize time-to-market over security testing. We have seen vendors struggling with a growing number of cybersecurity issues in multiple industries where products are growing more connected, including notably IoT and automotive in recent years. This is usually the result of not considering cybersecurity at the beginning of the product lifecycle; fixing vulnerabilities becomes more complex and expensive after a product is released.

The full paper provides an overview of the many implications of insecure robots as they become more prominent in home, business, industry, healthcare, and other applications. We've also included many recommendations in the paper for ways to design and build robotic technology more securely based on our findings.

Click here for more information on the research and to view the full paper for additional details and descriptions.