Hacking Robots Before Skynet[1]

Cesar Cerrudo (@cesarcer)

Chief Technology Officer, IOActive

Lucas Apa (@lucasapa)

Senior Security Consultant, IOActive

Research Preview

Robots are going mainstream. In the very near future robots will be everywhere, 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. Similar to other new technologies, we've found robot technology to be insecure in a variety of ways, and that insecurity could pose serious threats to the people, animals, and organizations they operate in and around.

This paper is based on our own research, in which we discovered critical cybersecurity issues in several robots from multiple vendors. While we assist the vendors in addressing the cybersecurity vulnerabilities identified, we want to describe the currently available technology, some of the threats posed by a compromised robot, and the types of cybersecurity issues we discovered. 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.

IOActive®

[1] https://en.wikipedia.org/wiki/Skynet_(Terminator)

Contents

Introduction

As electronic devices become smarter and the cost of cutting-edge technology decreases, we increasingly look to machines to help meet human needs, save lives, entertain, teach, and cure.

Enter the robot, an affordable and practical solution for today's business and personal needs.

Everyone is familiar with robots. In science fiction books and movies, they are often portrayed as mythological mechanical creations that can resemble animals or humans and assist society either by performing helpful tasks, or attempt to destroy it, as in the *Terminator* films.[2] Setting science fiction aside, real robots are being built and used worldwide now, and adoption is increasing rapidly.

The evidence of robots going mainstream is as compelling as it is staggering. Large investments are being made in robotic technology in both public and private sectors:

- Reports forecast worldwide spending on robotics will reach $188 billion in 2020.[3]
- South Korea is planning to invest $450 million in robotic technology over the next five years.[4]
- Reports estimate venture capital investments reached $587 million in 2015[5] and $1.95 billion in 2016.[6]
- SoftBank recently received $236 million from Alibaba and Foxconn for its robotics division.[7]
- UBTECH Robotics raised $120 million in the past two years.[8]
- Factories and businesses in the U.S. added 10% more robots in 2016 than in the previous year.[9]

Humanoid robots typically connect better emotionally with humans, since they imitate our behaviors, body parts, and skills, such as walking. The more robots reflect human nature, the greater empathy we feel when interacting with them. Other robots are designed to

[2] https://en.wikipedia.org/wiki/The_Terminator

[3] http://www.businesswire.com/news/home/20170110005131/en/Worldwide-Spending-Robotics-Reach-188-Billion-2020

[4] http://english.yonhapnews.co.kr/business/2016/10/10/83/0501000000AEN20161010009100320F.html

[5] https://www.ft.com/content/5a352264-0e26-11e6-ad80-67655613c2d6

[6] https://www.therobotreport.com/news/2016-was-best-year-ever-for-funding-robotics-startup-companies

[7] https://techcrunch.com/2015/06/18/alibaba-foxconn-softbank-and-pepper-walk-into-a-bar/

[8] https://www.crunchbase.com/organization/ubtech

[9] http://www.robotics.org/content-detail.cfm/Industrial-Robotics-News/2016-Breaks-Records-for-North-American-Robot-Orders-and-Shipments/content_id/6378

mimic predator animals and their movements[10] to convey a sense of authority or a particular skillset. Still others use wheels instead of legs, sharp objects or grippers instead of hands, fly using drone technology,[11] or swim autonomously.

Robot Adoption and Cybersecurity

Robots are already showing up in thousands of homes and businesses. All signs indicate that in the near future robots will be everywhere, as toys for children, companions for the elderly,[12] customer assistants at stores,[13][14] and healthcare attendants.[15] Robots will fill a dizzying array of service roles, as home and business assistants, intimate physical companions,[16] manufacturing workers,[17] security and law enforcement,[18] etc.

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[19] 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.

As human-robot interactions improve and evolve, new attack vectors emerge and threat scenarios expand. Mechanical extremities, peripheral devices, and human trust expand the area where cybersecurity issues could be exploited to cause harm, destroy property, or even kill.

There have already been serious incidents involving robots, including a woman being killed by an industrial robot in 2015 at the Ajin USA plant in Cusseta, Alabama, when an industrial robot restarted abruptly.[20] A couple of similar incidents occurred the same year

[10] https://www.wired.com/2011/02/darpas-cheetah-bot-designed-to-chase-human-prey/
[11] https://www.youtube.com/watch?v=T6kaU2sgPqo
[12] http://futurism.com/wp-content/uploads/2016/10/Robot-Companions_v2.jpg
[13] http://www.chinapost.com.tw/business/asia/2016/12/21/487286/Taiwan-Mobiles.htm
[14] http://www.businessinsider.com/chinese-restaurant-robot-waiters-2016-7
[15] http://www.digitaltrends.com/cool-tech/riken-robear/
[16] http://www.mirror.co.uk/news/world-news/sex-robots-could-biggest-trend-7127554
[17] http://www.forbes.com/sites/gregsatell/2016/08/14/how-rethink-robotics-sees-the-future-of-collaborative-robots/
[18] https://www.wired.com/2016/07/11-police-robots-patrolling-around-world/
[19] http://www.computerworld.com/article/3135434/security/ddos-attack-on-dyn-came-from-100000-infected-devices.html
[20] http://www.newser.com/story/235494/robot-kills-woman-2-days-before-wedding.html

at other plants as well.[2122] The US Department of Labor maintains a list of robot-related incidents, including several that have resulted in death.[23]

Notable robot-related incidents could fill an entire report. Here are just a few examples:

- A robot security guard at the Stanford Shopping Center in Silicon Valley knocked down a toddler; fortunately, the child was not seriously hurt.[24]
- A Chinese-made robot had an accident at a Shenzhen tech trade fair, smashing a glass window and injuring someone standing nearby.[25]
- In 2007 a robot cannon killed 9 soldiers and seriously injured 14 others during a shooting exercise due to a malfunction.[26]
- Robotic surgery has been linked to 144 deaths in the US by a recent study.[27]

While these incidents were accidents, they clearly demonstrate the serious potential consequences of robot malfunctions. Similar incidents could be caused by a robot controlled remotely by attackers.

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. We evaluated several robots of different models and vendors to provide a more general analysis.

Our results show how insecure and susceptible current robot technology is to cyberattacks, confirming our initial suspicions. Furthermore, many other vendors and robots could be vulnerable to the same issues we discovered, scaling the potential for havoc to much higher and broader levels.

[21] http://www.independent.co.uk/news/world/asia/worker-killed-by-robot-in-welding-accident-at-car-parts-factory-in-india-10453887.html

[22] https://www.ft.com/content/0c8034a6-200f-11e5-aa5a-398b2169cf79

[23] https://www.osha.gov/pls/imis/AccidentSearch.search?acc_keyword=%22Robot%22&keyword_list=on

[24] http://www.theverge.com/2016/7/13/12170640/mall-security-robot-k5-knocks-down-toddler

[25] http://mashable.com/2016/11/21/xiao-pang-chinese-robot-smashes-glass/#nrErRt0Pe5qX

[26] https://www.wired.com/2007/10/robot-cannon-ki/

[27] http://www.bbc.com/news/technology-33609495

Cybersecurity Problems in Today's Robots

In order to identify the cybersecurity problems to which modern robots could succumb, 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. Since robots are generally still expensive and acquisition is sometimes not possible due to availability and global shipping restrictions, 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."

We found several serious cybersecurity problems in technology from multiple vendors, including:

- **SoftBank Robotics**: NAO and Pepper robots
- **UBTECH Robotics**: Alpha 1S and Alpha 2 robots
- **ROBOTIS**: ROBOTIS OP2 and THORMANG3 robots
- **Universal Robots**: UR3, UR5, UR10 robots
- **Rethink Robotics**: Baxter and Sawyer robots
- **Asratec Corp**: Several robots using the affected V-Sido technology

Our research covered home, business, and industrial robots, as well as the control software used by several other robots. SoftBank Robotics, UBTECH Robotics, and ROBOTIS develop robots for business and the home. Universal Robots and Rethink Robotics develop industrial robots. Asratec Corp develops robot control software used in robots from multiple vendors, including some of those we tested.[28]

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

[28] https://www.asratec.co.jp/?lang=en#top_v-sido-robot

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.

We're not going to provide full technical details of the cybersecurity problems we discovered in this initial paper. We have responsibly reported our findings to the affected vendors so the issues can be addressed to prevent their robots from being hacked. In a few months following the disclosure process, we do intend to publish the technical details. In the meantime, we'll discuss the most common problems we discovered to provide a general sense of our findings and awareness of the current situation.

The following is a high-level (non-technical) list of some of the cybersecurity problems we found.

Insecure Communications

Communications are a vital part of a robot's ecosystem, as they allow users and ecosystem components to interact seamlessly. For example, users can program a robot with a computer, they can send commands in real-time with a mobile application, or the robot can connect to vendor Internet services/cloud for software updates and applications, etc. It's vital to keep a robot secure by using cryptographically strong communications. Otherwise, attackers can easily intercept communications and steal confidential information, compromise key components of the robot ecosystem, hack the robot, etc.

Unfortunately, most robots evaluated were using insecure communications. Mobile and software applications connected with the robots through the Internet, Bluetooth, Wi-Fi, etc., without properly securing the communication channel. They're sending critical information in cleartext or with weak encryption. Some robots also connect to the Internet by sending data to vendor services or the cloud in cleartext without any protection.

Authentication Issues

It's important to properly identify the users authorized to access any system, including robots. Only valid users should be able to program robots or send them commands. Failing to guard against unauthorized access means attackers can easily and remotely use certain features without a valid username and password, allowing them to essentially control the robot.

Most robots exposed one or more services that can be remotely accessed by computer software, mobile applications, Internet services, etc. These services included complex and critical functions, such as programming the robots and receiving external commands, as well as simpler functions like returning basic robot information.

We found key robot services that didn't require a username and password, allowing anyone to remotely access those services. In some cases, where services used authentication, it was possible to bypass it, allowing access without a correct password.

This is one of the most critical problems we found, allowing anyone to remotely and easily hack the robots.

Missing Authorization

All robot functions should be accessible only to authorized users or resources with the appropriate permissions. If authorization is not properly implemented, robot functions could be abused by an unauthorized attacker.

We found most robots did not require sufficient authorization to protect their functionality, including critical functions such as installation of applications in the robots themselves, updating their operating system software, etc. This enables an attacker to install software in these robots without permission and gain full control over them.

Weak Cryptography

Data protection is key for ensuring integrity and privacy. Robots can store sensitive information, including passwords, encryption keys, user social media and email accounts, and vendor service credentials, and send that information to and from mobile applications, Internet services, computer software, etc. This means communication channel encryption is mandatory for avoiding data compromises. Robots also receive remote software updates, and proper encryption is necessary to ensure that these updates are trusted and have not been modified to include malicious software.

We found most robots were either not using encryption or improperly using it, exposing sensitive data to potential attackers.

Privacy Issues

Robot ecosystems can include access to a wealth of information, depending on the robot and its intended use. Some of this information should be kept private and not shared with anyone other than the robots' owners. Private information could include personal or financial data, or data related to the robot ecosystem itself. Users should have full control over this information and what is shared with whom and when.

Some robots' mobile applications send private information to remote servers without user consent, including mobile network information, device information and current GPS location. This information could be used for surveillance and tracking purposes without the user's knowledge. Robots also remotely exposed private information without authentication, allowing access to anyone.

Weak Default Configuration

Most robots provide a set of features that are accessible and programmable through software services in the robot. These features should be securely configured by default so only authorized users can access them. They should also be password protected, allowing the authorized user to enable/disable them.

We found robots with insecure features that couldn't be easily disabled or protected, as well as features with default passwords that were either difficult to change or could not be changed at all. This means that anyone could abuse the robot's functionality because default passwords are usually publicly known or can be easily obtained since robot models share the same default passwords.

Vulnerable Open Source Robot Frameworks and Libraries

Many robots use open source frameworks and libraries. One of the most popular is the Robot Operating System (ROS)[29] used in several robots from multiple vendors.[30] ROS suffers from many known cybersecurity problems, such as cleartext communication, authentication issues, and weak authorization schemes.[31] All of these issues make robots insecure. In the robotics community, it seems common to share software frameworks, libraries, operating systems, etc., for robot development and programming. This isn't bad if the software is secure; unfortunately, this isn't the case here.

Not all of the robots we tested are vulnerable to every one of the cybersecurity issues listed. However, each robot we tested had many of the issues. While we didn't test every robot available on the market today, the research did lead us to believe that many robots not included in our assessment could have many of these same cybersecurity issues.

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.

[29] http://www.ros.org

[30] http://wiki.ros.org/Robots

[31] https://discourse.ros.org/t/announcing-sros-security-enhancements-for-ros/536

Cyberattacks on Robots

Each robot has different features; the more features, the more advanced and smarter the robot typically is. But these features can also make robots more vulnerable and attractive to abuse by attackers.

Certain features are trending in recent releases from robot manufacturers. These common features improve accessibility, usability, interconnection, and reusability, such as real-time remote control with mobile applications.

Unfortunately, many of these features make robots more fragile from a cybersecurity perspective. During our research, we found both critical- and high-risk cybersecurity problems in many of these features. Some of them could be directly abused, and others introduced severe threats.

The following list gives a brief overview of some possible threats and attacks for common robot features:

- **Microphones and cameras**: Once a robot has been hacked, microphones and cameras can be used for cyberespionage and surveillance, enabling an attacker to listen to conversations, identify people through face recognition, and even record videos.
- **Network connectivity**: Sensitive robot services are vulnerable to attack from home/corporate/industrial networks or the Internet. A hacked robot becomes an inside threat, providing all of its functionality to external attackers.
- **External services interaction**: The robot owner's social networks, application stores, and cloud systems could be exposed by a hacked robot. This means an attacker can gain access to private user information, usernames, passwords, etc.
- **Remote control applications:** Mobile applications or microcomputer boards can be used to send malicious commands to robots. Mobile phones could be an entry point for launching attacks against robots; if a user’s phone is hacked, then the robot can be hacked too. Likewise, an attacker could use a hacked robot to launch attacks against the owner's phone.
- **Modular extensibility:** When a robot allows installation of applications, it can also allow installation of custom malware. Malicious software could cause the robot to execute unwanted actions when interacting with people. Ransomware could take robots hostage, making them unusable and allowing hackers to extort money to make them usable again.
- **Safety features:** Human safety protections and collision avoidance/detection mechanisms can be disabled by hacking the robot's control services.

- **Main software (firmware):** When a robot's firmware integrity is not verified, it is possible to replace the robot's core software and change its behavior in a malicious way by installing malware, ransomware, etc.
- **Autonomous robots**: A hacked autonomous robot can move around as long as its battery continues to provide power. This allows hackers to control an "insider threat" and steal information or cause harm to nearby objects or people.
- **Known operating systems:** Since many robots use the same operating systems as computers**,** many of the same attacks and vulnerabilities in those operating systems apply to the robots as well.
- **Network advertisement**: It is common for robots to advertise their presence on a network using known discovery protocols. Attackers can leverage this to identify a robot in a corporate/industrial network with thousands of computers, and possibly interact with its network services.
- **Fast installation/deployment:** Since many vendors do not highlight the importance of changing the administrator's password in their documentation, a user may not change it during fast deployment. This means that any services protected by this password can be hacked easily.
- **Backups:** Configuration files and other information may be backed up on the robot vendor's cloud or the administrator's computer. An unencrypted backup could result in a compromised robot and a leak of sensitive data if obtained by an attacker.
- **Connection ports everywhere:** Physical connectivity ports lacking restriction or protection, could allow anyone to connect external devices to the robots.

Consequences of a Hacked Robot

A hacked robot could suffer the same familiar consequences as a hacked computer, but hacked robots can be even more dangerous. As mentioned, robots are basically computers, made more physically capable with the addition of arms, legs, or wheels, exponentially increasing the threats.

Robots in the Home

A hacked robot operating inside a home might spy on a family via the robot's microphones and cameras. An attacker could also use a robot's mobility to cause physical damage in the house. Compromised robots could even hurt family members and pets with sudden, unexpected movements, since hacked robots can bypass safety protections that limit movements.

As robots become smarter, threats will also increase. Hacked robots could start fires in a kitchen by tampering with electricity, or potentially poison family members and pets by mixing toxic substances in with food or drinks. Family members and pets could be in further peril if a hacked robot was able to grab and manipulate sharp objects.

Robots that are integrated with smart home automation could unlock and open doors and deactivate home alarms, making them a new best friend to burglars. Even if robots are not integrated, they could still interact with voice assistants, such as Alexa or Siri, which integrate with home automation and alarm systems. If the robot can talk or allow an attacker to talk through its speaker, it could tell voice-activated assistants to unlock doors and disable home security.

There is also a financial impact to security vulnerabilities in robots. While home robots are not prohibitively expensive, they are not yet cheap either. A hacked, inoperable robot could be a lost investment to its owner, as tools are not yet readily available to "clean" malware from a hacked robot. It could be difficult, even impossible, to reset the robot to factory defaults and recover it. If the core robot software (firmware) is hacked, it would be impossible to recover the robot. Once a home robot is hacked, it's no longer the family's robot, it's essentially the attacker's. Ransomware has been on the rise generally and it's on the horizon for robots as well, where people will have to pay attackers to regain the use of their robots.

Robots in Businesses

It's already common for business robots to be customer-facing, so a hacked robot could easily impact a business' most valuable assets. A hacked robot could be made to use inappropriate language, deliver incorrect orders, or go offline for instance. All of which would negatively impact the business, likely resulting in loss of customers (or at least customer confidence) and sales. An attacker could exploit a robot to physically hurt customers or company employees, causing even greater problems. If robots have access to customer information, such as personal and credit card data, that data could also be at

risk. Robots could cause destruction of property by starting fires or physically damaging business assets.

The financial impact for a business is similar to that of a home, just on a larger scale; business robots are generally much more expensive. A company with several hacked robots could suffer losses into the hundreds of thousands or even millions of dollars. Malware also has a larger impact in these robots, because it could be used to steal trade secrets or other sensitive company information.

Robots in Industry

This is one of the most dangerous scenarios, as industrial robots are usually larger, more powerful, and programmed to make precise movements and actions. A hacked industrial robot could easily become a lethal weapon. A number of people have already died in accidents caused by industrial robot malfunction, so we are not speaking theoretically when describing a hacked industrial robot as potentially lethal.

Financial impact could also be huge, since industrial robots are generally very expensive. If a company's industrial robots are hacked, they likely must stop production. Robots that remain inoperable will result in financial losses due to business disruption and replacement or remediation costs.

A hacked robot in a business or industrial setting could also be used to access other robots. Robots sharing the same network could have the same configuration (permissions, passwords, services, etc.) making them easier to hack once the first robot is compromised. This means that an attacker gaining control over one robot could foreseeably quickly hack all of the other robots on the network. Furthermore, compromised robots could be used to hack other computers or IoT devices on the same network. A hacked robot becomes an attack platform to exploit vulnerabilities in other network devices and propagate the attack.

Robots in Healthcare

While we didn't specifically test healthcare robots, it's important to mention that we believe they could suffer from the same cybersecurity problems we found in other robots. Robot adoption in healthcare is growing,[32] and if these robots are not secure, it doesn't require much imagination to foresee how they could put lives at serious risk. Vendors producing robots for this sector must take cybersecurity very seriously for obvious reasons. If not, they could face the same issues that have already been found in medical devices,[33] which could threaten human lives.

[32] http://medicalfuturist.com/robotics-healthcare/

[33] http://www.healthline.com/health-news/personal-medical-devices-vulnerable-to-hackers#1

Robots in Military and Law Enforcement

While we didn't specifically test military and police robots within the scope of this initial robot research, we believe robots used in these capacities could very well suffer from the same cybersecurity issues. Robot adoption in law enforcement and the military is not new, and they are actively being used in the field.[34] These robots are some of the most dangerous when hacked, since they are often used to manipulate dangerous devices and materials, such as guns and explosives.

[34] http://www.guns.com/2016/12/11/weaponized-robots-are-machines-the-future-of-american-policing/

Improving Robot Cybersecurity

Building secure robots is not a simple task, but following some basic recommendations, including provided examples below, can exponentially improve their cybersecurity.

- **Security from Day One:** Vendors must implement Secure Software Development Life Cycle (SSDLC) processes.
- **Encryption:** Vendors must properly encrypt robot communications and software updates.
- **Authentication and Authorization:** Vendors must make sure that only authorized users have access to robot services and functionality.
- **Factory Restore**: Vendors must provide methods for restoring a robot to its factory default state.
- **Secure by Default:** Vendors must ensure that a robot's default configuration is secure.
- **Secure the Supply Chain:** Vendors should make sure that all of their technology providers implement cybersecurity best practices.
- **Education:** Vendors must invest in cybersecurity education for everyone in their organization, with training not only for engineers and developers, but also for executives and all others involved in product decisions.
- **Vulnerability Disclosure:** Vendors should have a clear communication channel for reporting cybersecurity issues and clearly identify an individual or team to be responsible for handling reports appropriately.
- **Security Audits**: Vendors should ensure a complete security assessment is performed on all of the robot's ecosystem components prior to going into production.

Conclusion

The robotics industry is starting to disrupt other industries with its innovative technology, and has become an impressive development for humanity in general. However, this industry must quickly mature its security practices to avoid the potential for serious consequences as society becomes more dependent on robots.

Many of the cybersecurity issues our research revealed could have been prevented by implementing well-known cybersecurity practices. We found it possible to hack these robots in multiple ways, made a considerable effort to understand the threats, and took care in prioritizing the most critical of them for mitigation by the affected vendors. This knowledge enabled us to confirm our initial belief: it's time for all robot vendors to take immediate action in securing their technologies.

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.

Research from the University of Washington performed in 2009 found that household robots did not protect users' security and privacy.[35] This confirms that robot cybersecurity hasn't improved in almost eight years, in fact, it's worse.

Fortunately, since robot adoption is not yet mainstream, there is still time to improve the technology and make it more secure. Prominent scientists, such as Stephen Hawking, and billionaire technology entrepreneur Elon Musk are warning about the possible dangers of artificial intelligence (AI).[36] If we combine powerful burgeoning AI technology with insecure robots, the Skynet scenario of the famous *Terminator* films all of a sudden seems not nearly as far-fetched as it once did.

While we continue researching and hacking robot technology, we hope this paper will be a wake-up call for robot vendors to start taking cybersecurity seriously. If robot ecosystems continue to be vulnerable to hacking, robots could soon end up hurting instead of helping us, and potentially taking the "fiction" out of science fiction.

[35] http://www.washington.edu/news/2009/10/08/household-robots-do-not-protect-users-security-and-privacy-researchers-say/
[36] https://en.wikipedia.org/wiki/Open_Letter_on_Artificial_Intelligence

Acknowledgements

Special thanks to Marc Goodman for his great and inspiring book, *Future Crimes*[37] and to James Cameron, Gale Anne Hurd, and William Wisher Jr., for the *Terminator* films.

For more information on IOActive's robotic technology security research and services, please visit: http://ioac.tv/robotsecurityhack

About IOActive

IOActive is a comprehensive, high-end information security services firm with a long and established pedigree in delivering elite security services to its customers. Our world-renowned consulting and research teams deliver a portfolio of specialist security services ranging from penetration testing and application code assessment through to semiconductor reverse engineering. Global 500 companies across every industry continue to trust IOActive with their most critical and sensitive security issues. Founded in 1998, IOActive is headquartered in Seattle, USA, with global operations through the Americas, EMEA and Asia Pac regions. Visit www.ioactive.com for more information. Read the IOActive Labs Research Blog: http://blog.ioactive.com. Follow IOActive on Twitter: http://twitter.com/ioactive.

[37] http://www.futurecrimesbook.com

