Cybersecurity Issues in Robotics

George W. Clark Jr., Michael V. Doran, Todd R. Andel
Department of Computer Science
School of Computing
University of South Alabama
Mobile, Alabama 36688
Email: george.clark@jagmail.southalabama.edu, {mdoran, tandel}@southalabama.edu

***Abstract*—Cybersecurity is not highly prioritized during the design and manufacture of robots. As with other embedded systems a higher priority is placed on development costs and delivering functionality to consumers. In the future greater attention to cybersecurity will need to be given as the use of robots continues to grow in the manufacturing, military, medical, eldercare and the automated vehicle markets. This work identifies current and potential cyber threats to robotics at the hardware, firmware/OS, and application levels. Attack scenarios at each level are presented and discussed. Additionally, the economic and human safety impact of a cyber attack on robots is examined. Finally, possible countermeasures are suggested.**

I. Introduction

Robots have been used in manufacturing for well over 50 years. Ever since General Motors first used the Unimate robot in 1961 to assist in automobile production, the application of robotics in manufacturing has exploded [1]. In the last decade robots have and are increasingly being used for applications that affect our daily lives. We now depend on drones for our national security and defense. Our supply chain and goods distribution through companies like Amazon is also carried out by robots. More attention is also being given to using robots for medical and eldercare. Companies like Tesla and Google are researching and developing automated vehicles. An analysis of 280 companies by the Department of Commerce on Competitiveness showed an average growth rate of twenty percent for robotics use in the manufacturing, service, and medical markets along with a sixty-two percent average growth rate in the markets of healthcare and eldercare [2]. Based on this data, it is clear that robotics is a rapid growth industry and that the use of robots will continue to increasingly become a part of our everyday lives.

Given such a high growth rate, robotics manufacturers must not be tempted to undervalue cybersecurity during design. As with other embedded systems, robotics manufacturers place a high priority on safety, cost of development, speed to market, and providing customer features. Cybersecurity is a lower and sometimes forgotten priority in part because security is not a primary consideration for customers. Users place more value on cost, usability, features, and functionality [3]. However, due to their direct interaction with human beings, robotics applications must be required to be more secure than other embedded systems.

This paper focuses on identifying current and potential cybersecurity threats on robots, discussing both their economic impact and impact to human safety, and suggests possible countermeasures to these threats. Section 2 presents a target level categorization of cyber attacks on embedded systems and discusses how it applies to robot applications. Using this categorization, Section 3 discusses how cyber attacks might be applied to robots. In particular, scenarios for attacks on eldercare robots, drones, automated vehicles, and manufacturing robots are discussed. Section 4 describes the impact of cyber attacks both economically and to human safety. Finally, possible countermeasures are suggested to prevent robot cyber attacks.

II. Embedded System Cyber Attacks Categorization

"An embedded system is a computing system built into a larger system, designed for dedicated functions that consists of a combination of hardware, software, and optionally mechanical parts" [4]. "Robots can be defined as a combination of mechanical structures, sensors, actuators, and computer software that manages and controls these devices" [5]. Therefore robots are a type of embedded system and can be susceptible to the same types of cyber attacks that plague other embedded systems. In this paper, attacks on embedded systems will be classified based on the target layer of the embedded system architecture: hardware, firmware/OS and application [4].

A. Hardware Attacks

Embedded systems are vulnerable to hardware attacks both when manufactured and in the field of use. Some common forms of hardware attacks are hardware backdoors, hardware trojans, eavesdropping, fault injection, and hardware modification. Robots are also susceptible to hardware attacks both at production time and during their use. As with other embedded systems, robots are mass produced to reduce costs. This gives attackers opportunity to reverse engineer a robot's components and possibly add hardware trojans during the manufacturing process. Attackers could also add kill switches or hardware level backdoors for gaining access to the robot while in use [6]. Robots could also be attacked in the field either by an attacker with access during its use or during the maintenance process.

B. Firmware/OS Attacks

In most embedded systems, firmware code is stored in flash memory to allow OS upgrades remotely via an Internet

978-1-5090-6662-7/17/$31.00 ©2017 IEEE

connection [7]. This ability to upgrade its firmware, device drivers, and OS provides ample opportunities for attacks. Embedded systems with an OS are also susceptible to attacks on vulnerabilities in the OS. The Linux OS has been used in many consumer devices and has been shown to be vulnerable to atacks such as denial of service, execution of arbitrary code, and root-level access to the system. An example of this was reported in September of 2016 when hackers used 1.5 million devices that were mostly security cameras to form a Botnet to perform a DDoS attack on KrebsonSecurity.com. The attackers took advantage of a vulnerability in the root Linux OS that allowed full control of the device by typing a username with too many characters. The attackers then planted malware on the devices that turned them into bots [8]. Robots will inherently be vulnerable to both upgrade and OS vulnerability attacks.

C. Application Attacks

Embedded systems also contain software programs to perform the tasks they were designed for. Some common attack methods at the application level are viruses, worms, software trojans, and buffer overflow. An example of an application level attack is Stuxnet. Stuxnet is a malware threat that targets industrial control systems [9]. Its initial intrusion was through a thumb drive on a Windows system. It would then detect if it resided on a PC that was part of a Siemens programable logic controller (PLC) control system. If so, it would use the communications application between the PLC and the PC to gather information and deliver malicious code to the PLC to destroy the end device. A robot might have this same type of application vulnerability issue through the use of a common library or Internet communications application.

III. Application examples of Attacks on Robots

This paper presents four varieties of robots: eldercare, automated vehicles, military drones, and manufacturing. For each type of robot, motivations for attacks are discussed and cyber attack scenarios are given based on target level.

A. Eldercare Robots

In the future robots will reside in our homes as eldercare or home assistance robots. Eldercare robots such as the Care-O-Bot [10] will be responsible for performing household tasks, providing mobility assistance, and performing home maintenance. This type of robot would communicate health status with physicians, distribute scheduled medications and notify emergency personnel when assistance is needed. Due to their physical presence in the home, these robots will need the highest level of security with regard to cyber attacks.

Possible motivations for a cyber attack on an eldercare robot range from an attacker showing off their skills to other more notorious motives. For instance, an attacker that is a family member could gain control over an eldercare robot in order to murder its user for financial gain from inheritance. A more likely motivation would be for an attacker to gain control of the eldercare robot to monitor its user looking for data like credit card information for identity theft.

Attack Scenario: Consider the use of a robot in the home of an elderly person that lives alone. The function of the robot would be to allow the user's family to remotely monitor and locate them in case of a medical or health crisis. The robot is connected to the Internet via the home's wireless network and is equipped with a video camera, microphone, and speaker for the family to both view and communicate with the user. A financially motivated attacker could perform an application level attack by penetrating the home network and probing for the robot's IP address to reach the username/password login entry. Using a buffer overflow attack the attacker uses the entry of the login to overflow the stack with malicious code and inserts a return address that points to the malicious code. Once executed the attacker could have full control of the robot and is then free to monitor the elderly victim via camera or microphone seeking out information such as credit card data to be used for financial gain.

B. Automated Vehicles

On September 29, 2016, the state of California approved a bill that allows testing of self-driving vehicles where a human driver as a backup is not required. These vehicles will not be required to have a steering wheel, brake pedal, or accelerator [11]. Soon there will be robots operating autonomously on public streets. Foreign actors could be strongly motivated to commit critical infrastructure attacks on these robots. Once widely used, the consequences of an advanced persistent threat would be dire. Streets could become congested and vehicles could be used to attack members of the government directly or indirectly.

Attack Scenario: Consider that Tesla owners recently received a recall notice from the National Highway Traffic Safety Administration alerting them that a charger plug needed to be fixed because it had been discovered to be a cause of fires. Tesla was able to complete the fix for 29,222 vehicle owners via over the air software updates [12]. Tesla's ability to push out software updates to its vehicles creates the potential for a cyber attack at the firmware/OS level. A hypothetical attack might involve a two-phased approach where an attacker first gains access to an automated vehicle manufacturer's over the air update system and then pushes out a corrupted version of the vehicle firmware, perhaps one that would allow remote control over the vehicle. The attacker now has control over a legion of automated vehicles.

C. Military Drones

Military drones are unmanned aerial vehicles (UAVs) controlled remotely by a pilot and can be used to monitor and attack enemy targets. In January of 2014 it was reported that the U.S. military had 7,362 Ravens, 990 WASPs, 1,137 Pumas and 306 T-Hawks small UAS (unmanned aircraft systems) and 246 Predators and Gray Eagles, 126 Reapers, 491 Shadows and 33 Global Hawks that are large UAS [13]. This amounts to a small army of remote controlled robots and there would

be a strong desire by enemies of the U.S. to develop cyber attacks against them. The consequences of a cyber attack on robots carrying live missiles and ammunition could be deadly.

Attack Scenario: For purposes of discussion, assume that a military operation is being performed by China in the South China Sea and that the U.S. military is monitoring Chinese military actions via drones. Also assume that the drones were manufactured by an approved vendor for the military that in order to cut costs outsourced the microcontroller component to a Chinese company. This creates the potential of a hardware level attack where a Chinese attacker has an opportunity to introduce a hardware backdoor or trojan during production. Assume the attacker added a kill switch that is enabled when certain GPS coordinates are detected. Through GPS spoofing [14] the attacker can now disable the drones.

D. Manufacturing Robots

Robots are common in manufacturing and a recent online article in the Wall Street Journal reported that in the year 2014 there were close to 1.6 million industrial robots in operation worldwide. That number is projected to grow to nearly 2 million in 2017 [15] and amounts to a large portion of manufacturing labor activities being performed by robots. Cyber attacks on industrial robots might be economically or politically motivated by a foreign actor interested in disrupting supply chains and causing economic chaos. The economic consequences of a prolonged attack on an auto manufacturing facility or food processing facility could be severe.

Attack Scenario: Assume the situation of a system of manufacturing robots in a bread processing facility responsible for packaging all types of bread. The facility uses minimal human labor and PLCs to control the robots. The PLCs also report business data to a server via MODBUS where it is accessible by corporate headquarters. The attacker is a foreign government preparing for war against the U.S. Before conducting a military attack, the foreign actor wants to cause economic chaos and to interrupt the supply of food to troops that would be fighting in the war. A blended method of attack like Stuxnet has been planned for several years. It starts with an infected email sent to a receptionist at corporate headquarters which installs malware on the corporate network allowing the attacker access and the ability to search the network for the business data collection server. Malware is then installed allowing the attacker, when ready, to begin an application level attack that uses MODBUS communications between the server and the PLCs to write control data to the PLCs that causes the robots to flail about destroying their robotic arms. As a result the facility is brought to a standstill and if conducted simultaneously at multiple facilities, chaos will ensue and the supply of bread will be interrupted until the facilities are brought back online.

IV. Impact of Robot Cyber Attacks

In this section we present a description of the impact of a cyber attack on robots from both an economic and human safety point of view. In the economic description an attack on manufacturing, distribution, and transportation robots is examined. For the case of human safety, attacks on eldercare, military, and automated vehicle robots are examined.

A. Economic Impact: Manufacturing and Supply Chain

To date much of the economic research on robotics deals with the impact or threat of robots taking human jobs [16] [17] [18]. The authors are not aware of any research that analyzes the economic impact of a cyber attack on robots. However, it is possible to compare the economic impacts of a cyber attack on robots to that of a natural disaster. Some parallels can be drawn between the economic effects of a pandemic and an attack on robots. Webster's dictionary defines a pandemic as an epidemic over a large area. Consider that the spread of a virus in an epidemic for humans is similar to the infection and spread of malware in robots. In both cases there could be a loss of life (assuming the malware damaged the robot beyond repair) and downtime while the infection is cured for humans or removed in the case of robots.

The most recent major pandemic in the U.S. was the Spanish Flu in 1918. It killed millions and infected a significant number of working age people (15-54 year olds) [19]. Affecting a large number of working age people is one of the major challenges to the economy during a pandemic as it results in employee absenteeism due to illness or quarantines. In 1918 all manufacturing labor was performed by humans. In the manufacturing industry today, a significant portion of labor is performed either solely by robots or by robots assisting humans. Extrapolating further and considering robots as part of the workforce, a cyber attack on robotic systems in manufacturing could have a similar effect as a pandemic.

A recent report suggests that 10 percent of all manufacturing jobs are automated and will grow to 25 percent in a decade. In some industries more than 40 percent of manufacturing tasks will be performed by robots [20]. The automobile industry uses robots throughout the assembly process as either standalone robots or robots that assist humans. Envision the effect of a cyber attack via malware on an auto assembly plant. In the worst case, enough robots in the plant would be infected to cause bottlenecks in the assembly line. If the robots were damaged it could lead to a lengthy plant shutdown while they are repaired. It is beyond the scope of this paper to do an in depth study of the economic costs of such a scenario but some information can be gleaned from the effects of a different natural disaster. In 2011 Japan was hit by an earthquake and a tsunami that caused supply chain disruptions to the automobile manufacturers in the area. Toyota was forced to close its plants for nearly a month after the disasters and this caused Toyota's income for that quarter to drop 77 percent [21].

Supply chain disruption is an area of similar economic impact of a pandemic and a cyber attack on robots. The food industry is an example of how a pandemic or cyber attack on robots could create huge economic issues. The resiliency of the U.S. food system to pandemics was researched in 2015. The research pointed out that small profit margins and pressure to reduce costs in the food industry has led to consolidation,

where now only a few companies in the global food system control the majority of food products and that inventories are intentionally kept at low levels where food arrives just in time for consumption [19]. Indeed, supermarkets in large U.S. cities only stock a 7-day supply of food. This means that a major and persisting disruption in food supply will quickly lead to severe shortages [22]. Reconsider the bread packaging facility cyber attack in section 3. This attack could lead to consumer fear and over purchasing of bread resulting in empty store shelves and a short term rise in the price of bread.

A primary use for automated vehicles will be transportation of goods and similar to a pandemic's absenteeism effect on the trucking industry, a cyber attack on automated vehicles would disrupt the supply chain. As goods were not delivered, shortages would occur. The economic effects would be more severe as they would not be limited to one industry.

B. Human Safety: Military, Transportation, and Eldercare Robots

Much of the research with regards to human safety and robotics has focused on human robot interaction (HRI). Robots as they exist now are generally large heavy machines that are predominantly used in a manufacturing environment. In this environment robots are in close quarters and sometimes working hand in hand with people. This has led researchers to address topics like mechanics, control techniques, fault handling, and developing safety standards [23]. Additionally, automation of vehicles has led to research in topics like collision avoidance, lane warning/prevention, active cruise control and automated parking. As the use of robots becomes more mainstream, the impact of human safety with regards to cybersecurity will also have to be addressed.

The impact of a cyber attack on a military robot or drone is the most feared since they are intended to conduct surveillance or to deliver a deadly payload. The obvious attack would be delivering an armed payload to the wrong target resulting in injury and loss of innocent civilian or military lives. Even without a payload, an attacker could gain control and force a collision with a target such as a civilian airplane or with innocent people on the ground. Furthermore, a surveillance drone if hacked could report back incorrect coordinates or targeting information that might lead to airstrikes on civilians, allies, or friendly military.

Previous research has shown that automobiles have vulnerabilities that make them susceptible to attacks and that the automotive industry lags in their effort to address them [24]. Human safety has become an area of concern with regard to the use of automated vehicles as there have already been a few cases where errors have resulted in the deaths of their drivers. A recent example was the May 7, 2016 crash of a Tesla Model S while in autopilot mode where the vehicle's sensors failed to recognize an 18 wheel semi truck crossing the highway resulting in the vehicle hitting the truck at full speed and killing the driver [25]. In this case, if the driver had been aware, he could have overridden the vehicle, taken control, and avoided the accident. Future automated vehicles will be driverless and there may be no option to override the vehicle by the passenger. They may even be without passengers and only used for transporting goods. The lack of effort by the auto industry in developing cyber secure vehicles and the development of fully autonomous vehicles has the potential to be a tempting target for a malicious cyber attack. Checkoway et al. [24] discusses the ability for an attacker to identify a particular person using vehicle telematics. If combined with an attack on the vehicle itself, an attacker could locate and injure or kill a particular passenger.

Eldercare robots will be designed to cohabitate with the humans they assist or care for. Therefore it's easy to assume that an eldercare robot would only affect the safety of one or two individuals. However, once commonplace, they will likely be mass produced by a few manufacturers similar to other appliances in the home. These robots will receive software updates and could receive care and drug dosage instructions from physicians. By communicating with a central location, it's possible that groups of eldercare robots could be attacked simultaneously and instructed to physically attack the humans they care for. Drugs could be denied, dosage levels could be manipulated, care could be neglected, or physical force could be applied. These robots may also impact human safety in a psychological manner. An attacker could take advantage of the trust developed between the robot and the patient and stage an attack to confuse the patient by manipulating activity schedules to different days of the week or from the day to night. This may worsen symptoms for patients that have dementia or Alzheimer's disease or falsely make them believe they suffer from these conditions.

V. Countermeasures to Robot Cyber Attacks

This paper now briefly discusses possible countermeasures with respect to the target layer of the robot system: hardware, firmware/OS, and application.

A. Hardware attack level countermeasures

As discussed in section 2, robots are susceptible to hardware attacks both at production and in the field of use. At the production stage manufacturers at a minimum should employ personnel and business related security processes to limit access to sensitive material. Manufacturers will also need to validate suppliers to insure that supplied electronic components such as FPGAs or memory units have not been compromised. Third-party hardware will need to be checked for triggering mechanisms or nefarious payloads. As documented by [26] several solutions have been proposed including isolation mechanisms between IP cores [27], payload detecting solutions [28], and IC fingerprinting [29]. As of now there is no clear cost effective all encompassing solution to securing third-party hardware.

B. Firmware/OS attack level countermeasures

It is suggested that robot manufacturers move toward adopting a common standardized operating system. To help prevent firmware and OS attacks, manufacturers could standardize on

a common OS such as the open source NuttX OS. Through standardization, robot manufacturers could create a consortium to oversee the platform and be responsible for securing the OS, reporting security issues, and releasing security updates. The consortium would publish security and testing standards to be followed by robot application developers. The consortium should also formalize authentication methods to validate firmware updates insuring downloads come from a trusted source via digital signature with encryption.

C. Application attack level countermeasures

To prevent application level cyber attacks, robot manufacturers will need to place an emphasis on developing secure application code. Cybersecurity considerations should be prominent in design and development and developers should program and test their code with security in mind, paying special attention to vulnerabilities such as buffer overflows. Any communication protocols developed between the robot and third parties should be secure and encrypted. Other areas of research beneficial to the robotics industry would be the use of tools that prevent or detect cyber attacks during application execution. Pike et al. [30] incorporated control flow integrity (CFI) checks into the RTOS and Abera et al. [31] devised C-FLAT to remotely verify CFI on an embedded device.

VI. Conclusion

In this paper, we presented a target level categorization of common cyber attacks on embedded systems and applied them to robots. Using this categorization, the application of cyber attacks on robots was discussed and attack scenarios on eldercare robots, drones, automated vehicles, and manufacturing robots were presented. We also discussed the economic impact on manufacturing and supply chain of cyber attacks by comparing them to the worker absenteeism effects of a pandemic. This paper also described the impact on human safety of a cyber attack with regard to military, transportation and eldercare robots. Finally, this paper suggested possible countermeasures for robot manufacturers to implement to prevent such attacks.

References

[1] N. Hockstein, C. Gourin, R. Faust, and D. J. Terris, "A history of robots: from science fiction to surgical robotics," *Journal of robotic surgery*, vol. 1, no. 2, pp. 113–118, 2007.

[2] H. I. Christensen, T. Batzinger, K. Bekris, K. Bohringer, J. Bordogna, G. Bradski, O. Brock, J. Burnstein, T. Fuhlbrigge, R. Eastman *et al.*, "A roadmap for us robotics: from internet to robotics," *Computing Community Consortium*, 2009.

[3] S. H. Mirjalili and A. K. Lenstra, "Security observance throughout the life-cycle of embedded systems," in *Proceedings of the 2008 International Conference on Embedded Systems and Applications, ESA 2008*, no. EPFL-CONF-149724, 2008, pp. 186–192.

[4] D. Papp, Z. Ma, and L. Buttyan, "Embedded systems security: Threats, vulnerabilities, and attack taxonomy," in *Privacy, Security and Trust (PST), 2015 13th Annual Conference on*. IEEE, 2015, pp. 145–152.

[5] S. Morante, J. G. Victores, and C. Balaguer, "Cryptobotics: Why robots need cyber safety," *Frontiers in Robotics and AI*, vol. 2, p. 23, 2015.

[6] X. Wang, T. Mal-Sarkar, A. Krishna, S. Narasimhan, and S. Bhunia, "Software exploitable hardware trojans in embedded processor," in *Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT), 2012 IEEE International Symposium on*. IEEE, 2012, pp. 55–58.

[7] H. Elmiligi, F. Gebali, and M. W. El-Kharashi, "Multi-dimensional analysis of embedded systems security," *Microprocessors and Microsystems*, vol. 41, pp. 29–36, 2016.

[8] L. Franceschi-Bicchierai. (2016) How 1.5 million connected cameras were hijacked to make an unprecedented botnet. [Online]. Available: https://motherboard.vice.com/read/15-million-connected-cameras-ddos-botnet-brian-krebs

[9] N. Falliere, L. O. Murchu, and E. Chien, "W32. stuxnet dossier," *White paper, Symantec Corp., Security Response*, vol. 5, p. 6, 2011.

[10] M. Hans, B. Graf, and R. Schraft, "Robotic home assistant care-o-bot: Past-present-future," in *Robot and Human Interactive Communication, 2002. Proceedings. 11th IEEE International Workshop on*. IEEE, 2002, pp. 380–385.

[11] E. Baron. (2016) Fully autonomous cars get lift from gov. jerry brown. [Online]. Available: http://www.mercurynews.com/2016/09/29/fully-autonomous-self-driving-cars-get-lift-from-governor/

[12] A. Brisbourne, "Teslas over-the-air fix: Best example yet of the internet of things?" *Wired. http://www. wired. com/insights/2014/02/teslas-air-fix-best-example-yet-internet-things*, 2014.

[13] K. Osborn. (2014) Pentagon plans for cuts to drone budgets. [Online]. Available: http://www.dodbuzz.com/2014/01/02/pentagon-plans-for-cuts-to-drone-budgets

[14] S. Peterson and P. Faramarzi, "Exclusive: Iran hijacked us drone, says iranian engineer (video)," *Christian Science Monitor, Dec*, vol. 15, 2011.

[15] J. Hagerty, "Meet the new generation of robots for manufacturing," *Wall Street Journal*, pp. 3–4, 2015.

[16] P. Frase, "Class struggle in robot utopia," in *New Labor Forum*, vol. 25, no. 2. SAGE Publications, 2016, pp. 12–17.

[17] T. Frey, "Hi, i'm a robot and i'm here to take your job," *Journal of environmental health*, vol. 76, no. 2, p. 46, 2013.

[18] M. Ford, *Rise of the Robots: Technology and the Threat of a Jobless Future*. Basic Books, 2015.

[19] A. G. Huff, W. E. Beyeler, N. S. Kelley, and J. A. McNitt, "How resilient is the united states food system to pandemics?" *Journal of Environmental Studies and Sciences*, vol. 5, no. 3, pp. 337–347, 2015.

[20] H. L. Sirkin, M. Zinser, and J. Rose, "The robotics revolution: The next great leap in manufacturing," *BCG Perspectives*, 2015.

[21] B. Canis, *Motor Vehicle Supply Chain: Effects of the Japanese Earthquake and Tsunami*. Diane Publishing, 2011.

[22] D. Olson, "Agroterrorism: Threats to america's economy and food supply," *FBI Law Enforcement Bulletin*, vol. 1, 2012.

[23] A. De Santis, B. Siciliano, A. De Luca, and A. Bicchi, "An atlas of physical human–robot interaction," *Mechanism and Machine Theory*, vol. 43, no. 3, pp. 253–270, 2008.

[24] S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner, T. Kohno *et al.*, "Comprehensive experimental analyses of automotive attack surfaces." in *USENIX Security Symposium*. San Francisco, 2011.

[25] D. Yadron and D. Tynan. (2016) Tesla driver dies in first fatal crash while using autopilot mode. [Online]. Available: https://www.theguardian.com/technology/2016/jun/30/tesla-autopilot-death-self-driving-car-elon-musk

[26] S. Sethumadhavan, A. Waksman, M. Suozzo, Y. Huang, and J. Eum, "Trustworthy hardware from untrusted components," *Communications of the ACM*, vol. 58, no. 9, pp. 60–71, 2015.

[27] T. Huffmire, B. Brotherton, G. Wang, T. Sherwood, R. Kastner, T. Levin, T. Nguyen, and C. Irvine, "Moats and drawbridges: An isolation primitive for reconfigurable hardware based systems," in *2007 IEEE Symposium on Security and Privacy (SP'07)*. IEEE, 2007, pp. 281–295.

[28] A. Waksman and S. Sethumadhavan, "Tamper evident microprocessors," in *2010 IEEE Symposium on Security and Privacy*. IEEE, 2010, pp. 173–188.

[29] D. Agrawal, S. Baktir, D. Karakoyunlu, P. Rohatgi, and B. Sunar, "Trojan detection using ic fingerprinting," in *2007 IEEE Symposium on Security and Privacy (SP'07)*. IEEE, 2007, pp. 296–310.

[30] L. Pike, P. Hickey, T. Elliott, E. Mertens, and A. Tomb, "Trackos: A security-aware real-time operating system," in *International Conference on Runtime Verification*. Springer, 2016, pp. 302–317.

[31] T. Abera, N. Asokan, L. Davi, J.-E. Ekberg, T. Nyman, A. Paverd, A.-R. Sadeghi, and G. Tsudik, "C-flat: control-flow attestation for embedded systems software," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*. ACM, 2016, pp. 743–754.