Fall 2018

A Risk Assessment on Raspberry PI using NIST Standards

Michael Williams
Iowa State University

A Risk Assessment on Raspberry PI using NIST Standards

by

Michael Grant Williams

Creative Component submitted to the graduate faculty

in partial fulfillment of the requirements for the degree of

Master of Science

Major: Computer Engineering

Program of Study Committee:

Diane Rover, Major Professor

Iowa State University

Ames, Iowa

2018

Summary
This paper focused on the Raspberry PI computer to determine the security of this device via a security risk assessment utilizing the NIST standards. The paper reviewed and highlighted the results of this security assessment.
Key words:
Internet of Things security, Privacy, Raspberry PI Security, Risk Assessment, Threats and Vulnerabilities.

1. Introduction

The Raspberry PI device is used for various projects - anything from general computing to detailed ventures. These ventures include SmartHome projects, Home Entertainment solutions, and home and personal security, along with configurations for hacking both tools and applications. These small computers have been used for numerous and diverse applications and can be integrated within networks, which has lead to questions regarding security weaknesses. An assessment was completed to determine the security of the Raspberry PI device and if major security risks or vulnerabilities exist.

The National Institute of Standards and Technology (NIST) Special Publication (SP) series was utilized as the assessment tool for this process since NIST is accepted as an industry standard and is implemented by most influential agencies for assessment and authorization, including the United Stated Department of Defense (DoD).

This risk assessment (RA) incorporates the Risk Management Framework (RMF) and uses the *NIST SP Guide for Conducting Risk Assessments* (NIST SP 800-30), the *Guide for Applying the Risk Management Framework to Federal Information Systems* (NIST SP 800-37) and other NIST standards and federal publications. Using these guidelines to conduct this security assessment allows the Raspberry PI to be uniformly evaluated for overall security posture; this is a standard procedure that can be followed for future assessment and research.

2. Background

The Raspberry PI is a small, single board computer the size of a driver's license that uses the Linux operating system (OS). In February 2012, the Raspberry PI Foundation introduced its first Raspberry PI with the basic goal of promoting Science, Technology, Education, and Mathematics (STEM) in schools at a low cost. The Raspberry PI also teaches students the fundamentals of computer science.

Since then, Raspberry PI has evolved for use with a wide range of projects, from SmartHome projects, Home Entertainment solutions, and home and personal security, to a web server and other cloud based applications. This has made Raspberry PI a powerful and efficient device for the Internet of Things (IoT). In 1999, Ashton [2] first described *the Internet of Things* (IoT). The IoT allows distinctively identifiable computer systems, such as Raspberry PI, to connect to other devices via the Internet using several network methods, including wired, wireless, and Bluetooth. The IoT continues to gain popularity. In 2009, the number of peer-reviewed articles related to the IoT was less than 20 but by 2013, the number increased to over 110 articles [39]. With the increased incorporation of IoT into everyday life, more devices are developed and integrated into this new technology every day. Researchers continue to discover functions in the IoT [39].

Because Raspberry PI and IoT incorporate "all kinds of devices (e.g., cars, robots, machines and tools), living beings (persons, animals, and plants) and things (e.g., garments, food, drugs, etc.)"[8], security is vital to the successful integration of Raspberry PI within the IoT. Following is a review of applications used in Raspberry PI, as well as the security needs of the device.

Gebhardt, Massoth, Weber, Wiens, and Darmstadt [11] discussed operating SmartHome automation software in Raspberry PI to control a standardized SmartHome. Beyond the SmartHome application, Lu, Liang, Shen, and Chen introduced the concept of a Smart Community. This concept connected Smart Homes to a Wireless Local Area Network (WLAN) "to improve community safety, home security, healthcare quality, and emergency response abilities" [19]. The SmartCommunity was comprised of three different domains. The first domain was the Home Domain, which was the individual SmartHome automated monitoring and sensing system. The second domain was the Community Domain, which was the core of the Smart Community; this domain contained all the home gateways, as well as the community center, and stored and processed data.

The third domain was the Service Domain, which contained the main component known as the Call Center. This domain was located centrally, possibly at a 911 Call Center or Fire/Police headquarters. Use of this Smart Community increased the safety and security of residents and the community. Some SmartHomes have incorporated Raspberry PI.

Researchers from Mokpo National University conducted research with Raspberry PI in the container transportation industry to track and monitor container shipments. Raspberry PI sent either an email or Short Message Service (SMS) alert that allowed for up-to-the-moment shipment information. This application "increase[d] the security and productivity of the supply chain" [24]. This became a useful application for Raspberry PI within the IoT. Use of Raspberry Pi in the trucking industry allows the driver to update dispatch regarding location and load status via pre-programmed tweets within Raspberry PI [15]. If a security risk in Raspberry PI exists, a hacker could disrupt transportation of products or services.

Researchers from Delhi Technological University developed a Raspberry PI protocol for the medical industry [4]. The prototype was a body sensor to monitor elderly patients for falls that processed and transmitted data to a central monitoring station. The "body sensor module will be extremely beneficial to the patients and their caregivers who will be able to monitor their health on their own. It will enable doctors and physicians to remotely monitor" these patients as well [4].

Researchers from Australian National University designed a tool known as SmartLink; this device allowed users to remotely discover and configure sensors regardless of the sensor's communication protocol. As the number of sensors increased and became too taxing to configure manually, this system had the capability "to configure sensors autonomously as well as within very short periods of time" [21]. The SmartLink tool contained the eight-step process. Raspberry PI has been used to conduct some of these steps, with others conducted via a Cloud based system.

Risks are threats that exploit vulnerabilities that can allow damage and destruction, up to and including loss of product, services or assets [29]. Threats can be internal or external, as well as accidental or intentional. They include a wide range of exploits and attacks that take advantage of vulnerabilities [29]. Vulnerabilities are weaknesses or gaps in security used by a nefarious person or program to either gain or denied access to assets and/or resources [29].

Figure 1 provides an excellent representation of the different routes an attacker could use for malicious actions against resources and assets. "Attackers can potentially use many different paths through your application to do harm to your business or organization. Each of these paths represents a risk that may, or may not, be serious enough to warrant attention" [36].

Fig. *1 [36] Threat process*

A risk assessment on Raspberry PI will determine the risk level for threats. The RA will evaluate four major threat sources.

- Adversarial, including Individual, Group, Organization, and Nation-State. [29]
- Accidental, including User, Privileged User, and / or Administrator [29]
- Structural, including Information Technology (IT) Equipment, Environmental Controls, and Software [29]
- Environmental, including Natural or Man-made Disaster, Unusual Natural event, and Infrastructure failure / outage [29]

A risk assessment is conducted in a logical and detailed manner. The first step is evaluating the overall security risks associated with Raspberry PI. Use of standard industry tools ensures consistency and validity of the risk assessment. The NIST risk assessment standard is widely applied and accepted in various applications and hardware devices, making it a wise choice for this assessment. NIST standards are simple to implement and provide easily understood output.

The NIST standard includes four key steps, shown in figure 2; each provides information and functions that feed into the next step. Step one must

"establish a context for the risk assessment. This context is established and informed by the results from the risk-framing step of the risk management process. Risk framing identifies, for example, organizational information regarding policies and

requirements for conducting risk assessments, specific assessment methodologies to be employed, procedures for selecting risk factors to be considered, scope of the assessments, rigor of analyses, degree of formality, and requirements that facilitate consistent and repeatable risk determinations across the organization." [29]

Step two

"produce[s] a list of information security risks that can be prioritized by risk level and used to inform risk response decisions. To accomplish this objective, organizations analyze threats and vulnerabilities, impacts and likelihood, and the uncertainty associated with the risk assessment process" [29].

Step three ensures that

"decision makers across the organization have the appropriate risk-related information needed to inform and guide risk decisions" [29].

Finally, the goal of step four is to

"keep current the specific knowledge of the risk organizations incur. The results of risk assessments inform risk management decisions and guide risk responses" [29].

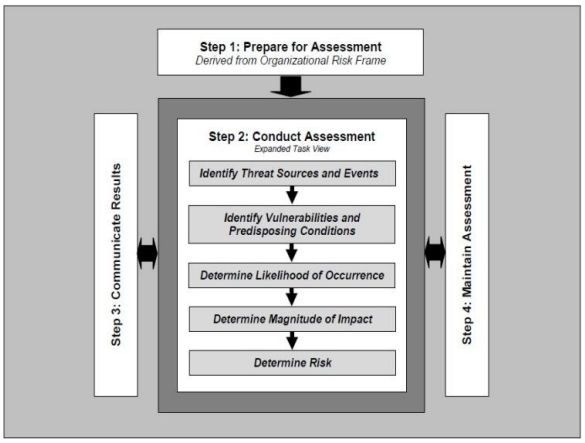

Fig. *2: NIST 800.30 Steps of the Risk Assessment [29]*

Because of the risks inherent with the implementation of Raspberry PI in the IoT and the serious consequences that can occur, a risk assessment of the device is necessary. It is vital to ensure that high risks and vulnerabilities have countermeasures in place. Using NIST to perform this assessment will produce the desired information to accomplish this goal.

3. Define the Specific Problem

Raspberry PI has a variety of risks and threats that can exploit its vulnerabilities. These can occur accidently or intentionally, either by internal or external forces. Cyber Attacks, include Denial of Service (DoS), Man in the Middle (MiM), or malware, to name a few. Acts of nature are important to consider and include blizzards, floods, and loss of power. Of additional concern are human factors, like theft or destruction of equipment, data, and facilities; this also includes the modification or alteration of information, hardware, or software. Some application and software issues that can affect Raspberry PI security include updates, patches, and passwords. These types of security issues, can affect the operation of Raspberry PI in a normal work environment, but could drastically disrupt service or functionally within a specific industries. A risk assessment on Raspberry PI offers specific details regarding the weaknesses and vulnerabilities that would allow the user to take proper security steps to harden the device.

The goal of this research is the determination of the various security issues related to Raspberry PI network connections, operating services, and systems vulnerability, with a hypothesis that many risks exist. A high security risk rating was hypothesized based on the assumption that Raspberry PI has numerous services running, several ports open, software and application that need to be patched / updated.

Raspberry PI can run applications that control virtual and physical safety, like the SmartHome, security / monitoring or cloud based applications, and connect to the IoT; users should be aware of any security risks and vulnerabilities associated with its use. While Raspberry PI provides great benefits, it also offers a means to disrupt or limit use within the IoT. When deploying Raspberry PI in a remote access network environment, one should harden the device to prevent cyber-attacks. Without proper security measures, this device could become a bot or be hacked, resulting in system compromise.Understanding these risks, threats, and weaknesses allows the user to prevent STRIDE (Spoofing identity, Tampering with data, Repudiation, Information disclosure, Denial of service, Elevation of privilege) attacks. Other security threats Raspberry PI could encounter include Jamming, Eavesdropping, and Man-in-the Middle (MiM) attacks. A risk assessment of Raspberry PI will increase awareness of the issues, and help determine the countermeasure to thwart these risks.

Using Raspberry PI and similar devices to connect to systems or software that houses sensitive applications and/or data without proper security measures in place opens the user to malicious attacks to gain access to these devices and applications. Aside from opening the garage door for easy criminal access, a hacker can cause other issues. For example, hackers would be able to modify the home temperature or electric use with a SmartHome device. It is then possible to lower the thermostat in the winter to allow pipes to freeze and burst, increase usage by leaving every light on, or potentially set fire to the home by turning on the coffee pot. Further disruptions in security involves SmartCommunity programming, including parking availability and pollution levels, as well as police fire and rescue responses. Disruption of any of these could cause problems ranging from slightly irritating to completely devastating.

In the medical industry, sensitive data is protected by strong systems. If the Raspberry PI is not properly hardened for use within this environment, hackers could gain access and release sensitive patient information or inject data to create a false condition leading to improper treatment, surgery, or death. Similarly, if Raspberry PI is used for the transportation industry and not configured properly, hackers could input or display false data on the location, contents, or route of a shipment., allowing for illegal movement of containers.

One of the main outcomes of a risk assessment is to determine the risk for an attack. It determines the level of threat and the vulnerabilities present that create weakness. Since applications and software implemented into the Raspberry PI have also been integrated within IoT, security measures must be addressed. Security needs to be taken seriously before, during, and after deploying Raspberry PI online. Since this type of technology allows users connect remotely and monitor their environments and assets, an improperly secured device could allow hackers and cyber-criminals to attack. Addressing security concerns in Raspberry PI and similar devices makes the product safer when deployed, which is vital in home security, transportation, and medical applications, among others.

4. Developing a Solution

Many risk assessment researchers used industrial standards like COBIT, ISO, ITIL, OCTAVE, SANS Institute and NIST. Each of these standards qualitatively measures and ranks vulnerabilities. Researchers then analyze and report the data [25 and 27]. NIST standards are well documented, freely available for use, and easy to implement. Because of this, as well as their use within the DoD and other federal agencies, NIST standards were chosen for this risk assessment.

This research is not meant to find an alternative risk assessment method. It yields qualitative data for analysis via the NIST risk assessment standards and methodology. These standards are valid and reliable for this type of risk assessment. The use of a well-known tool allows other researchers to access these same standards and utilize the methodology described for reproduction of results [35].

This risk assessment on the Raspberry PI analyzes and reviews the threats and vulnerabilities inherent with a stock non-hardened Raspberry PI. Active processes and services, their necessity, and whether disabling them is an option is determined. Results presented are in a qualitative form that allows for an unbiased evaluation and to ensure that the assessment could easily be replicated with similar findings should a different assessment team repeat this study. The results are qualitative and are analyzed and reviewed via the qualitative standards. For this RA, two port scans and one vulnerability scan were conducted. The equipment utilized during this phase included an Asus laptop running VM Player, supporting Kali-Linux 1.10. A Raspberry PI running Debian 7.0 (Wheezy) was directly connected to the Wi-Fi router, and was plugged into a DSL modem. Figure 3 shows the network configuration of this test environment.

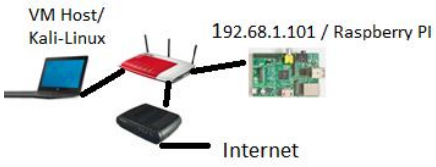

Fig. *3: Network Overview*

Zenmap software was used to perform the two port scans; this software was included with the Kali-Linux distribution. The first port scan revealed 2000 ports, including the 1024 well-known ports. Of these 2000 scanned ports, 1001 were open, 1017 were filtered, and 981 were closed. There were 5681 packets sent during this scan. Figure 4 shows the results.

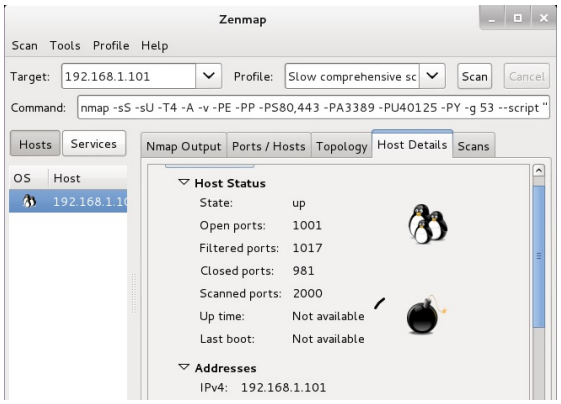

Fig. *4: Initial Port Scan*

One of the security procedures included disabling services and ports that are open or unnecessary. To ensure the ports are disabled, a second scan was performed. The second scan found 2000 ports. In this scan, only one port was open, one port was filtered, and 998 were closed. There were 5702 packets sent during the scan. Figure 5 shows the results.

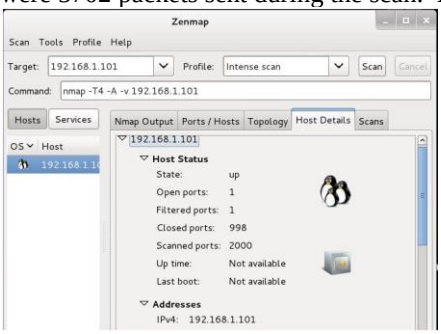

Fig. *5: Subsequent Port Scan*

Port 22 was open for Transmission Control Protocol (TCP) to create a Secure Shell (SSH). Raspberry PI uses this protocol to allow remote access for installation and configuration of the device. Aside from port 22, the second scan confirmed that known open ports had been disabled.

The next step was to perform a vulnerability scan on the Raspberry PI. The vulnerability software utilized for this scan was *Retina*, a software-based application developed and supported by *Beyond Trust*. *Retina* was the standard vulnerability scanner used by the DoD until 2015. The network architecture remained the same as in figure 3. *Retina* was installed directly onto a laptop running Windows 8.1.

The results of the vulnerability scan detected only two information audits. These two vulnerabilities were SSH Local Access Audit ID No. 2264 and ICMP Timestamp Request Audit ID No. 3688. Both are low-level events. Raspberry PI successfully passed this vulnerability test. Figures 6 and 7 show the results and summarize the Retina Scan.

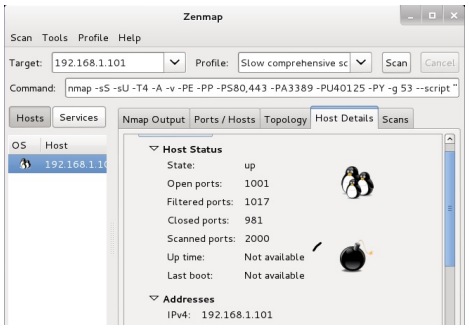

Fig. *6: Retina Scan Results*

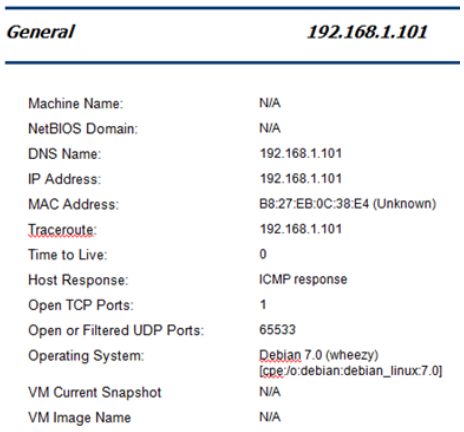

Fig. *7: Retina Scan Summary*

Figure 8 provides delineation of known issues into the three security controls categories - Management, Operational, and Technical - organized from high to low [29]. For the next step in this risk assessment, the risks were determined and listed in figure 8. The three categories utilized include:

- Management security controls –"The security controls (i.e., safeguards or countermeasures) for an information system that focus on the management of risk and the management of information system security" [29].
- Operational security controls– "The security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by people (as opposed to systems)" [29].
- Technical security controls–"Security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system." [29]

Ratings of low, moderate, and high were used for this assessment. Using these guidelines, each threat identified within [37] was given a rating, which in turn, was used to populate Figure 8.

Total Findings by Risk Rating				
Class	**High**	**Medium**	**Low**	**Total**
Management	0	1	5	6
Operational	4	3	12	19
Technical	5	9	14	28
Total	9	13	31	53

Fig. *8: Total Risk Ratings [37]*

Figure 8 represents just one part of the RA using the NIST guidelines [29]. Table 1 describes the high risks in each of the three categories discovered. Not all the items listed within [32] were used, since not all were applicable to the Raspberry PI.

Risks	Recommendations
Perform perimeter network reconnaissance / scanning.	Support team should determine whether replacement of the existing Firewall with an Intrusion Prevention System (IPS) is a cost-effective response.
Perform network sniffing of exposed networks.	Support team should determine whether replacing the existing Firewall with an Intrusion Prevention System (IPS) is a cost-effective response.
Perform reconnaissance and surveillance of the targeted device.	Support team should analyze whether replacing the existing Firewall with an Intrusion Prevention System (IPS) is a cost-effective response.
Insert untargeted malware into downloadable software and / or into commercial information technology products.	Support team should determine whether replacing the existing Host Base Firewall with a Host Base Security Software (HBSS) is a cost-effective response.
Exploit recently discovered vulnerabilities.	Support team should implement procedures for reviewing and updating vendor-recommended patches so that patches are applied in a timely manner.
Conduct wireless jamming attacks.	None - management must elect to accept this risk.
Conduct targeted Denial of Service (DoS) attacks.	Support team should analyze whether replacing the existing Firewall with an Intrusion Prevention System (IPS) is a cost-effective response.
Conduct non-targeted zero-day attacks.	None - management must elect to accept this risk.
Obtain sensitive information through network sniffing of external networks.	Support team should implement procedures for encrypting data and information at rest and in transit.

Table *1: Risk & Recommendations [37]*

Once discovered, one can create and design tests and controls to identify and thwart specific threats unique to the system assessed.

The Risk Model (figure 9) identifies, detects, and determines the impact on organization resources and assets; it then determines and then implements the appropriate controls to prevent or reduce the impact to the organization. The organization needs to determine the best method to mitigate each item identified.

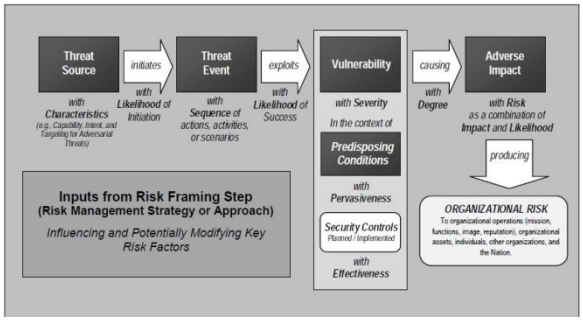

Fig. *9: GENERIC RISK MODEL WITH KEY RISK FACTORS [29]*

After the assessment was completed and analyzed, determination of a mitigation strategy could be addressed. There are four mitigation strategies that allow the organization to accept, avoid, limit, or transfer the risk. With risk acceptance, the company would be willing to accept the defined type of exposure as a part of doing business. Dissimilarly, with risk avoidance, the company would not conduct any type of business that exposed the organization to the defined risk. Risk limitation is the most common type of mitigation; the process consists of implementation of counter measures or safeguards to prevent or limit threats and risks. Risk transference places the risk with another firm; for example, buying insurance to protect against a specific threat or risk. The mitigation methods defined in this assessment were analyzed to determine which were financially feasible and best suited for the device.

After completion of the RA and analysis of the results, it was determined that the overall security of the Raspberry PI was better than previously hypothesized. The risk assessment revealed 53 vulnerabilities, of which 31 were low risk, 13 had a moderate risk, and 9 held a high risk rating. Because of the combined risks of threats, vulnerabilities, likelihood of attack, impact of damage, and possible mitigation needs, the overall risk associated with the operation of the Raspberry PI was determined to be Moderate. Among the 53 vulnerabilities identified, 17% were unacceptable because serious harm could result and effect the operation of Raspberry PI. Immediate, mandatory implementation of countermeasures is needed to mitigate
the risk of these threats to an acceptable level. Of the 53 vulnerabilities, 58% were acceptable for use within this environment because only minor problems would result. Recommended countermeasures were also suggested to reduce or eliminate these risks. While weaknesses were discovered in implementation of certain management, operational and technical security controls, the overall effect of these layered controls still provided adequate protection for the system.

Table 2 lists threat agents that could be used against Raspberry PI based on the findings of this study.

• Hacking
• Social engineering
• System intrusion, break-ins
• Unauthorized system access
• Computer crime (e.g., cyber stalking)
• Fraudulent act (e.g., replay, impersonation, interception)
• Information bribery
• Spoofing
• System intrusion
• Information warfare
• System attack (e.g., distributed denial of service)
• System penetration
• System tampering
• Information theft
• Computer abuse
• Malicious code (e.g., virus, logic bomb, Trojan horse)

Table *2: Types of Vulnerability [37]*

The immediate remediation of all High and Moderate finding is required to achieve a secure operating device. The identified risks [37] require countermeasures at the application and infrastructure level for secure system operation. Additionally, policies and procedures should be in place to convey system security measures.
The most significant security concern for Raspberry PI was the lack of technical controls. Recommendations to remedy this include:

1) Implement procedures for encrypting data and information at rest and in transit.
2) Develop user roles and associated privileges, as well as policies regarding removal of accounts.
3) Develop a Security Awareness and Training program.
4) Analyze whether replacing the existing firewall with an Intrusion Prevention System (IPS) is a cost-effective response to the risks.
5) Implement procedures for reviewing and updating vendor-recommended patches to ensure all are applied in a timely manner.

Users should implement best security practices with the Raspberry PI to help maintain user security while hardening the device. The first step in hardening this device would be to use one of the recommended Raspbian distributions. Next, the user should change the default password, followed by disabling unused services. The final task would be to install updates on the system frequently, including anti-virus software.

- Additionally, the following configuration changes should be made:
  - Configure IP tables.
  - Configure logging and setup.
  - Configure SELinux.

- These few tasks greatly increase the security of operating this device.

The Raspberry PI assessment identified many risks embedded in the operation area; these did not meet minimum requirements nor had adequate countermeasures been applied. The risk assessment determined the likelihood of a breech, cyber-attack, or

other weaknesses and suggested countermeasures to mitigate the identified risks with appropriate level-of-protection that met all minimum requirements.

5. Conclusions

- This paper reviewed various projects and applications related to the security of the Raspberry PI. Some of these projects process and transmit sensitive data and need proper steps to prevent unauthorized access and service interruptions. A risk assessment was performed on the Raspberry PI device to determine the security of the device.

- Data to support a risk assessment of this type was drawn from a thorough review the literature surrounding the Raspberry PI device, Raspberry PI documentation, interviews, and certification testing. This process evaluated the management, operational, and technical security controls of the Raspberry PI in accordance with NIST documents.

During this RA of the Raspberry PI it was discovered that this device is susceptible to 7 of the 10 worst vulnerability listed within the OWASP top-ten worst vulnerability list. Reviewing the OWASP risk rating results also helps determine the severity of these threats. Below in figure 10 is the OWASP top-ten worst vulnerability list.

1 Insecure Web Interface
2 Insufficient Authentication/Authorization
3 Insecure Network Services
4 Lack of Transport Encryption
5 Privacy Concerns
6 Insecure Cloud Interface
7 Insecure Mobile Interface
8 Insufficient Security Configurability
9 Insecure Software/Firmware
10 Poor Physical Security

Figure 11: OWASP 2013 Top 10 [36]

NIST and OWASP use a similar system that rates vulnerability to determine the severity of threats within applications and systems. These risk-rating tables are either 3 x 3 (Low to High) or 5 x 5 (Negligible to Extremely High). Figure 11 shows a 3 x 3 risk-rating table.

Threat Agents	Attack Vectors	Weakness Prevalence	Weakness Detectability	Technical Impacts	Business Impacts
App Specific	Easy	Widespread	Easy	Severe	App / Business Specific
	Average	Common	Average	Moderate	
	Difficult	Uncommon	Difficult	Minor	

Figure 11: OWASP Risk Rating [36]

This research determined the overall security risk of the Raspberry PI in accordance with NIST standards to be Moderate. This negates the working hypothesis of a high-risk rating for Raspberry PI, and the null hypothesis was accepted. Because the device achieved a Moderate rating, the Raspberry PI device still needs to be patched and hardened to lower the chance of compromise. Mitigation methods were provided for consideration.

- Some of the lessons learned during this project and offer the opportunity for growth are.
  - 1. A prior determination of risks and pitfalls may have allowed for a successful framework earlier in the process.
  - 2. During the project, it was discovered that NIST 800-181 or NIST 800-171 might have been well suited for this project. NIST 800-171is a light version of NIST 800-53, and NIST 800-181 was developed to apply in the public, private, and academic sectors. If either of these two frameworks were used as the foundation, the base control list would have been shorter.

6. Future Work

Future work will focus on creating a specific standard for IoT devices, this research will look to develop a new security framework entitled “Riskless Internet of Things Standard (RIOTSS) and incorporation a scoring feature within this new framework”. The intended purpose of RIOTSS is to create standards, policies, and procedures used in this proposal to prevent or limit security weaknesses introduced into products while mitigating procedures implemented in a secure manner without restricting device functionality or capability. This project will review and analyz several standards and frameworks to create a framework distinctively designed for the uniqueness of IoT devices.RIOTSS will addressed the extraordinary characteristics of IoT devices without exposing other functions to risks and threats or creating a device so secure it was unusable.

References

[1] S. H. Albakri, B. Shanmugam, G. N. Samy, N. B. Idris, and A. Ahmed, “Security risk assessment framework for cloud computing environments,” Security and Communication Networks, 2014

[2] K. Ashton. That ’internet of things’ thing- in the real world, things matter more than ideas. [Online]. Available: http://www.rfidjournal.com/articles/view?4986

[3] J. S. Atkinson, J. E. Mitchell, M. Rio, and G. Matich, “Your wifi is leaking: Building a low-cost device to infer user activities,” in Service Oriented System Engineering (SOSE), 2014 IEEE 8th International Symposium on. IEEE, 2014, pp. 396–397.

[4] S. Banerjee, D. Sethia, T. Mittal, U. Arora, and A. Chauhan, “Secure sensor node with raspberry pi,” in Multimedia, Signal Processing and Communication Technologies (IMPACT), 2013 International Conference on. IEEE, 2013, pp. 26–30.

[5] J. Breier, “Security evaluation model based on the score of security mechanisms,” Information Sciences and Technologies Bulletin of the ACM Slovakia, p. 19, 2014.

[6] J. Breier and L. Hudec, “On identifying proper security mechanisms,” in Information and Communication Technology. Springer, 2013, pp. 285–294.

[7] L. Coetzee and J. Eksteen, “The internet of things-promise for the future? an introduction,” in IST-Africa Conference Proceedings, 2011. IEEE, 2011, pp. 1–9.

[8] D. De Guglielmo, G. Anastasi, and A. Seghetti, “From ieee 802.15. 4 to ieee 802.15. 4e: A step towards the internet of things,” in Advances onto the Internet of Things. Springer, 2014, pp. 135–152.

[9] P. FIPS, “199, standards for security categorization of federal information and information systems,” Federal Information and Processing Standards, 2004

[10] ——, “200, minimum security requirements for federal information and information systems,” NCSD March, 2006.

[11] J. Gebhardt, M. Massoth, S. Weber, and T. Wiens, “Ubiquitous smart home control on a raspberry pi embedded system,” in UBICOMM 2014, The Eighth International Conference on Mobile Ubiquitous Computing, Systems, Services and Technologies, 2014, pp. 172–177.

[12] A. Greenberg, “Hackers reveal nasty new car attackswith me behind the wheel,” 2013.

[13] N. Hurst. Trucker uses raspberry pi to connect his big rig. [Online]. Available: http://makezine.com/2015/01/16/trucker-uses-raspberry-pi-toconnect his-big-rig/

[14] X. Hu, H. Xu, and K. Han, “Design and implementation of secure nodes in the based-internet-of-things intelligent household,” Journal of Computer and Communications, vol. 2, no. 07, p. 1, 2014.

[15] Intel. Curie module: Unleashing wearable device innovation. [Online]. Available: http://www.intel.com/

[16] S. Jain, A. Vaibhav, and L. Goyal, “Raspberry pi based interactive home automation system through e-mail,” in Optimization, Reliabilty and Information Technology (ICROIT), 2014 International Conference on. IEEE, 2014, pp. 277–280.

[17] B. Karabacak and I. Sogukpinar, “Isram: information security risk analysis method,” Computers & Security, vol. 24, no. 2, pp. 147–159, 2005.

[18] X. Li, R. Lu, X. Liang, X. Shen, J. Chen, and X. Lin, “Smart community: an internet of things application,” Communications Magazine, IEEE, vol. 49, no. 11, pp. 68–75, 2011.

[19] X. Liu, “Security risks in the internet of things,” in Proceedings of the 2012 International Conference on Cybernetics and Informatics. Springer, 2014, pp. 59–64.

[20] M. N. M. M. Noor, “Community based home security system using wireless mesh network,” Journal of Academic Research Part A, vol. 5 no. 5, pp. 73–79, 2013.

[21] C. Perera, P. P. Jayaraman, A. Zaslavsky, D. Georgakopoulos, and P. Christen, “Sensor discovery and configuration framework for the internet of things paradigm,” in Internet of Things (WF-IoT), 2014 IEEE World Forum on. IEEE, 2014, pp. 94–99.

[22] C. Perera, A. Zaslavsky, P. Christen, and D. Georgakopoulos, “Context aware computing for the internet of things: A survey,”Communications Surveys & Tutorials, IEEE, vol. 16, no. 1, pp. 414–454, 2014.

[23] R. L. Rutledge, A. K. Massey, A. I. Ant´on, and P. Swire, “Defining the internet of devices: Privacy and security implications,” 2014.

[24] P. Saripalli and B. Walters, “Quirc: A quantitative impact and risk assessment framework for cloud security,” in Cloud Computing (CLOUD), 2010 IEEE 3rd International Conference on. IEEE, 2010, pp. 280–288.

[25] R. Sharma, Y. Lee, B. M. Kim, Y. J. Kim, Y. G. Heo, H. J. Jeon, K. H Kim, and S. R. Lee, “Auto location and security alert embedded with container identification for real time applications,” in ICT Convergence (ICTC), 2013 International Conference on. IEEE, 2013, pp. 365–370.
[26]] M. Sherburne, R. Marchany, and J. Tront, “Implementing moving target ipv6 defense to secure 6lowpan in the internet of things and smart grid,” in Proceedings of the 9th Annual Cyber and Information Security Research Conference. ACM, 2014, pp. 37–40.
[27]] S. K. Sidhu, “A study of nist sp 800-144 standard on it risk management in cloud computing: Creating a novel framework for implementing it in small and medium sized enterprises (smes) by applying coso and isacas risk it frameworks,” 2013.
[28] E. Sitnikova and M. Asgarkhani, “A strategic framework for managing internet security,” in Fuzzy Systems and Knowledge Discovery (FSKD), 2014 11th International Conference on. IEEE, 2014, pp. 947–955.
[29] G. Stoneburner, A. Goguen, and A. Feringa, “Risk management guide for information technology systems,” NIST special publication, vol. 800, no. 30, pp. 800–30, 2002.
[30] ——, “Guide for applying the risk management framework to federal information systems,” NIST special publication, vol. 800, no. 37, pp. 800–37, 2014.
[31] ——, “Managing information security risk organization, mission, and information system view,” NIST special publication, vol. 800, no. 39, pp. 800–39, 2011.
[32] ——, “Security and privacy controls for federal information system and organizations,” NIST special publication, vol. 800, no. 53, pp. 800–53, 2013.
[33] ——, “Assessing security and privacy controls in federal information systems and organizations: Building effective assessment plans,” NIST special publication, vol. 800, no. 53A, pp. 800–53A, 2010.
[34] S. Vidalis, E. Morakis, and A. Blyth. Measuring threat using vulnerability trees.
[35] R. H. Weber, “Internet of things–new security and privacy challenges,” Computer Law & Security Review, vol. 26, no. 1, pp. 23–30, 2010.
[36] C.B. Westphall, "Challenges Towards Secure Internet of Things", *IARIA SECURWARE 2014 - PANEL*, Lisbon, Portugal, 2014, pp. 1-4 Jan 2015
https://www.owasp.org/index.php/OWASP_Internet_of_Things_Top_Ten_Project#tab=OWASP_Internet_of_Things_Top_10_for_2014
[37] M. G. Williams, “Raspberry-pi-rar.”
[38] [38] L. Willcocks and H. Margetts, “Risk assessment and information systems,”European Journal of Information Systems, vol. 3, pp. 127–127, 1994.
[39] L. Xu, W. He, and S. Li, “Internet of things in industries: A survey,” 2014. [
[40] X. Zhang, N. Wuwong, H. Li, and X. Zhang, “Information security risk management framework for the cloud computing environments,” in Computer and Information Technology (CIT), 2010 IEEE 10th International Conference on. IEEE, 2010, pp. 1328–1334.