Bob Jones University Robotics Team
Cyber Challenge Report

Date Submitted: May 17, 2019

Team Captain: RJ Ring | rring214@students.bju.edu

Fall 2018 Team Members:

Daniel Clauser | dclau415@students.bju.edu
Nathan Collins | ncoll943@students.bju.edu
Elizabeth Franklin | lfran167@students.bju.edu
Joshua Grimm | jgrim876@students.bju.edu
Lemuel Jacobson | ljaco134@students.bju.edu
Jacob Koechig | jkoec341@students.bju.edu
Ruth May | rmay657@students.bju.edu
Jared Mundy | jmund674@students.bju.edu
Bradley Pauley | bpaul675@students.bju.edu
Lydia Petersen | lpete480@students.bju.edu
Ezra Pio | epio175@students.bju.edu
Natalie Reed | nreed914@students.bju.edu
Sinjin Seiber | sseib267@students.bju.edu
Carter Shean | cshean@bju.edu
Jeremy Tan | jtan716@students.bju.edu
Steven Vanphavong | svanp649@students.bju.edu
Kyle Weberg | kwebe254@students.bju.edu
Nathanael Winslow | nwins689@students.bju.edu

Spring & Summer 2019 Team Members:

Lane Camfield | ccamf948@students.bju.edu
Alex Raddatz | aradd575@students.bju.edu
Marcela Martinez | mmart372@students.bju.edu
RJ Ring | rring214@students.bju.edu

Faculty Advisors:

Bill Lovegrove | blovegro@bju.edu
Will Woodham | wwoodham@bju.edu

Statement of Integrity:

I certify that the design and engineering of the vehicle by the current student team has been significant and equivalent to what might be awarded credit in a senior design course.

Faculty Advisor: William K. Woodham, M.S.P.D.
Assistant Professor
Department of Engineering
Bob Jones University

Faculty Advisor Signature: _____ Date: 5-14-2019

I. INTRODUCTION

As part of the engineering Mechatronics course, eighteen students from Bob Jones University implemented and integrated several subsystems to transform a Polaris GEM2 vehicle into an autonomous vehicle named Bruin 3. This vehicle is described in the separate Design Report; only Cyber-Challenge-Specific details are included in this report.

A team of four students took over the project after the completion of the school year and applied the NIST RMF process to the vehicle, adding several security controls to the design. The process was as follows:

1. Study the RMF process
2. Select a Threat concept
3. Apply the RMF to the threat concept
4. Apply the RMF to our competition vehicle
5. Choose controls to implement based on auditability
6. Implement and document controls
7. Write the demonstration strategy

Organization and design process

Marcela did steps 1-5 and wrote this report. The remaining members of the team will implement and document the controls. The whole team is responsible to understand and maintain the security controls.

II. THE NIST RMF PROCESS

Overview of the RMT process

Categorize
This is the first step in in the NIST RMF process. In this part we evaluate our system and identify potential threats to it. Then we categorize each of those threats into different risks levels, depending on how much damage each one can produce.
Select
In the second step of the NIST RMF process, we select adequate security controls based on the categorization in step one. After selecting the security controls, we then tailor them in order for them to suit the specific requirements of our system.
Implement
Moving to the next step of the NIST RMF process, the team now implements the security controls we selected to our system and configure it if necessary. This will include writing policies, configuring our system, implementing the use of different programs or apps, etc.
Assess
In the fourth step of the NIST RMF process, the team then determines if the security controls are effective, meets the security requirements, and works as predicted. This would be done through testing and tailoring if necessary.
Authorize
During this next step, the Authorization Official (AO) will use the information gather during our assessment process and will determine if the proposed controls are adequate to address the risk. In order to determine whether our risks are threatening, the AO might consider the help other security officers.
Monitor

The last step of the NIST RMF process, requires a monitor system or process to keep on check if the security controls are still in place and if any risks affecting their effectiveness have come up.

Identified threat concept

Bruin-3 is a hypothetical autonomous electric vehicle that provides fee-based transportation on the Bob Jones University campus. A website and app allow patrons to request and schedule taxi-like transportation service via the driverless vehicle. The service area is limited to the campus. An on-board touch screen provides passenger interaction. The vehicle parks in a dedicated parking location with charging capability in the centrally located parking garage. The transportation department maintains the vehicle and monitors the service through a web portal.

The information systems at risk include the on-board computers, and the back-end management system. Presented here is a list of possible threats:

- A student hacker might take over the vehicle for fun.
    - Information sought: access (vehicle passwords), operation (vehicle documentation)
- Someone might take over the vehicle and use as a weapon.
    - Information sought: access (vehicle passwords), operation (vehicle documentation)
- Someone might hack the vehicle and stop it from functioning.
    - Information sought: access (vehicle passwords), operation (vehicle documentation)
- Criminal wanting customer credit card or ID information.
    - Information sought: User data (credit card numbers)
- Student hacker wanting to take down the access website
    - Information sought: Server access, website access, database access
- Student hacker curious about RTK code or vehicle code in general
    - Information sought: RTK and team CODE

Security category and security impact level

Security Category	Confidentiality	Integrity	Availability
A student hacker might take over the vehicle for fun.	Low	Moderate	High
Someone might take over the vehicle and use as a weapon.	Moderate	High	High
Someone might hack the vehicle and stop it from functioning.	Low	High	High
Criminal seeking user data.	High	Low	Low
Student wanting to take down service.	Low	Moderate	High
Student hacker wanting to take down the access website.	Low	Moderate	High
Student hacker curious about RTK code or vehicle code in general.	High	Moderate	Low

Identification and Mapping of Cyber Controls to Counter Identified Threats

Technology based controls

SECURITY CATEGORY	AC-1	AC-3	AC-7	AC-11	AC-12	AC-19(1)	IA-2(1)	IA-3	SI-8(1)	SI-3(1)(2)	PE-8(1)	PS-1
A student hacker might take over the vehicle for fun.						X				X	X	
Someone might take over the vehicle and use as a weapon.			X		X	X	X		X	X	X	X
Someone might hack the vehicle and stop it from functioning.	X	X	X		X	X	X		X	X	X	
Criminal seeking user data.	X	X	X		X	X	X		X	X	X	
Student wanting to take down service.	X	X		X			X	X				
Student hacker wanting to take down the access website.	X	X		X			X	X				
Student hacker curious about RTK code or vehicle code in general.		X		X	X				X	X	X	

Security policies

Security Control	Tailoring
AC-1	Access Control Policy and Procedures: Only members of the Robot Team that have signed the non-disclosure agreement are allowed to have administrator logins.
AC-3	Access Enforcement: The password will be changed every 2 months and will be given again to the Robot Team members. Integrity questionnaires will be handed to check if anyone has shared the password.
AC-7	Unsuccessful Login Attempts: We will use a tool to detect how many continuous unsuccessful logging attempts have been made over a period of time. After 7 unsuccessful attempts the account will be locked.
AC-11	Session Lock: The session will be locked if suspicious activities are detected.
AC-12	Session Termination: The session will be terminated if a series of suspicious activities is detected by the same account over a period of time.
AC-19(1)	Access Control for Portable and Mobile Systems, User Identification and Authentication, and Device Identification and Authentication: The students that will request the vehicle will do so using their university email and password.
IA-2(1)	
IA-3	
PE-8(1)	
SI-8(1)	Spam and Spyware Protection: A tool will be used in case a of someone wanting to damage our vehicle or wanting to get access to our code.
SI-3(1)(2)	Malicious Code Protection: A tool will be used to detect code that is damaging our system and destroy it with the authorization of the team members.
PS-1	Personnel Security Policy and Procedures: In case of an emergency caused by someone using the vehicle as a weapon, the faculty, staff, and students will be required to follow the emergency evacuation policies set by the university.

III. THE NIST RMF PROCESS APPLIED TO COMPETITION ROBOT

Categorize

- A student hacker might take over the vehicle for fun.
    - Information sought: access (vehicle passwords), operation (vehicle documentation)
- Someone might hack the vehicle and stop it from functioning.
    - Information sought: access (vehicle passwords), operation (vehicle documentation)
- Competing teams might want to steal ideas.
    - Information sought: Team Code, team documentation
- Foreign governments might want to steal DOD code.
    - Information sought: RTK code, RTK documents, team documents

Threat Modelling

Security Category	Confidentiality	Integrity	Availability
A student hacker might take over the vehicle for fun.	Low	Moderate	High
Someone might hack the vehicle and stop it from functioning.	Low	High	High
Competing teams might want to steal ideas.	High	Low	Low
Foreign governments might want to steal DOD code.	High	Low	Low

1. Select

SECURITY CONTROLS	AC-1	AC-3	SA-5	SA-6	SI-8	SC-13	SC-30
A student hacker might take over the vehicle for fun.	X	X		X			X
Someone might hack the vehicle and stop it from functioning.	X	X		X	X	X	X
Competing teams might want to steal ideas. (e.g. Team Code, team documentation)	X	X	X	X	X	X	X
Foreign governments might want to steal DOD code. (e.g. RTK code, RTK documents, team documents)	X	X	X	X	X	X	X

2. Implement

Security Control	Tailoring
AC-1	Access Control Policy and Procedures: Only members of the Robot Team that have signed the non-disclosure agreement are allowed to have administrator logins.
AC-3	Access Enforcement: When students leave the project, the password must change.
SA-5	Information System Documentation: The DOD code is only installed on University computers, not student computers.
SA-6	
SI-8	Spam and Spyware Protection: A tool will be used in case a of someone wanting to damage our vehicle or wanting to get access to our code.
SC-13	Cryptographic Protection: The code is stored in an encrypted format.
SC-30	Concealment and Misdirection: We will make our Wi-Fi network name not viewable to outsiders and to access one must know the name. We can also change our network name to a something not related to our vehicle like the name of a coffee shop. A second misdirection Wifi network will attract and confuse attackers.
	Geo-fence the vehicle to the intended operating areas: the test track on the BJU campus and the competition track at IGVC

3. Assess

For the IGVC competition the demonstration strategies shown later in the report will serve as assessment.

4. Authorize

The Robot Team coach is responsible of authorizing the security controls. He will evaluate the security plan and approve its implementation or request further study of additional controls.

5. Monitor

At the start of the competition we will do a security audit to make sure the security controls are still in place.

Description of Implemented Cyber Controls

Relation of Chosen Controls to Mitigated Risk

1. AC-1
    - Helps us control that only authorized members have administrative rights.
2. AC-3
    - Helps us keep on check that the updated password stays within authorized members.
3. SA-5 and SA-6
    - Helps us keep on check were the information documentation is stored and who has access to them.
4. SI-8
    - This control will help us keep on track of any spyware threats and what actions should be taken if detected.
5. SC-13
    - This control makes sure that the DOD code is an encrypted that only authorized users can view.
6. SC-30
    - This control will make sure that the Wi-Fi network name is either concealed or has a misleading name.
7. Geo-fencing
    - This control will prevent the vehicle from operating outside of a designated area.

Design and Implementation Details of Controls

The team has designed policies to go along with the security controls to improve their effectiveness.

AC-1

1. The team members that want to gain administrative rights must sign a non-disclosure agreement.
2. If any of the team members share the administrative logins with an unauthorized person, the password must be changed. The team member who shared the password will be stripped from administrative rights.

AC-3

1. Whenever a team member leaves the project, the password must change.
2. The password will be change at the end of every school year by one of the Robot Team's coaches.

SA-5 and SA-6

1. The DOD code is installed only in the university computers.
2. Only team members with administrative rights can access the DOD code.

SI-8

1. During the competition one of the team members will be in charge of checking on an hourly basis that no spam or suspicious activity is occurring within our vehicle's software.
2. If any suspicious activities are found, the student must report to the team coach and asses what counter defensive actions must be taken.

SC-13

1. Every year there will be a check on the encrypted code to make sure it remains undamaged.
2. During a competition a check will be performed.

SC-30

1. The Wi-fi network name would be concealed. Only people who know the actual network name will be able to connect.
2. We will install another network that does not connect to anything in order to mislead other people trying to connect. Also, the real network will have a name that has nothing to do with our vehicle, like the name of a fast food restaurant or a café.

Geo-fencing

1. We will write a program to prevent the vehicle form leaving the competition grounds.
2. When arriving at the competition we will make sure that the coordinates are correct.
3. Every year the coordinate will have to checked and updated to match the university ground's coordinates.

Description of Appropriate but Unimplemented Controls
AC-7 Unsuccessful Logon Attempts

- This control would have notified how many unsuccessful logins attempts a user would have tried.

AC-11 Session Lock

- This control would have locked the user's session if any suspicious activities were detected.

AC-12 Session Termination

- This control would have terminated the user's session if he had tried to make the vehicle leave campus.

PE-8(1) Visitor Access Records

- This control would have allowed us to have records of any visitors without administrative right using our vehicle's software.

SI-3(1)(2) Malicious Code Protection

- This control would have allowed us to use a program able to detect if any malicious code had been damaging our vehicle's software.

Demonstration Strategies

1. These computers require a password for login.

The judges will be given access to these computers to verify that they require a password.

2. The code is stored in an encrypted format.

The judges will reboot Francisco and note the request for the encryption password.

3. When students leave the project, the password must change.

Two students left the team upon graduation on May 3, 2019. The passwords were changed on May 8, 2019 as demonstrated in the screenshot in Figure 1.

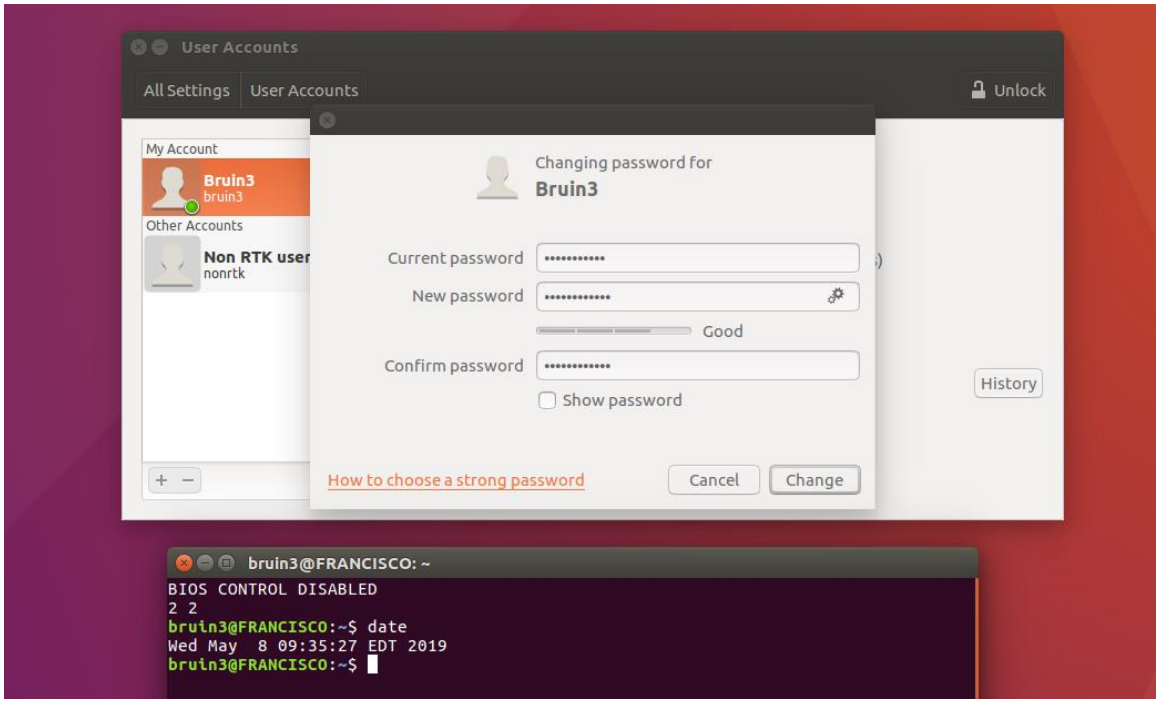


Figure 1

4. We require strong passwords as shown in Figure 2.

Judges can confirm this setting if desired on the project computers

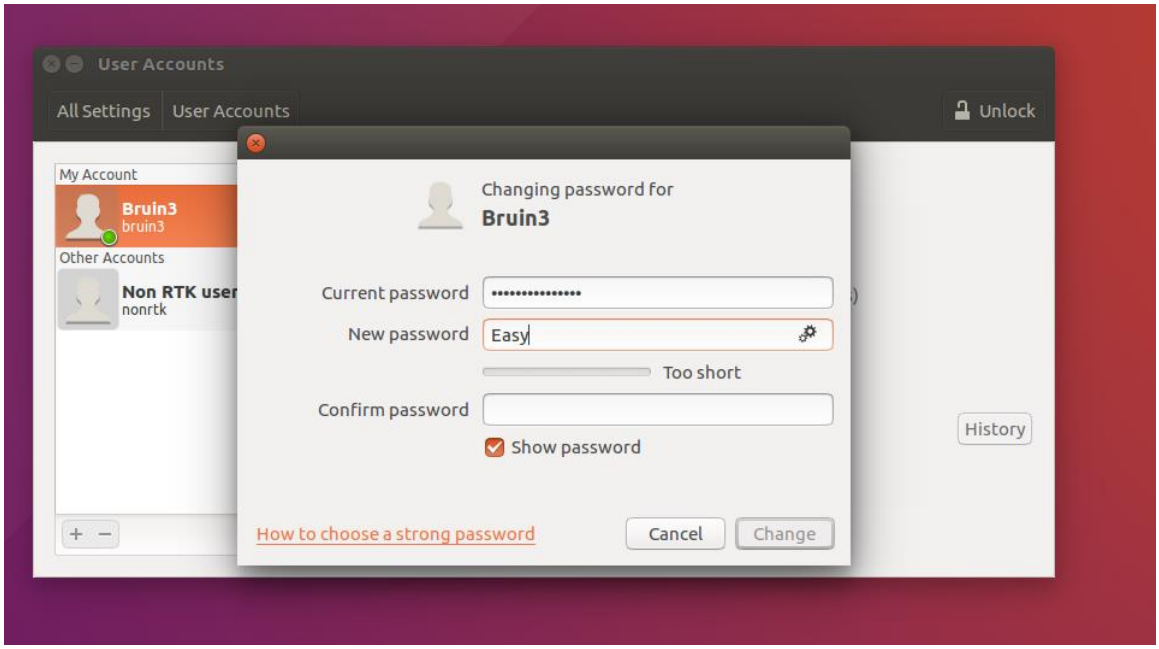
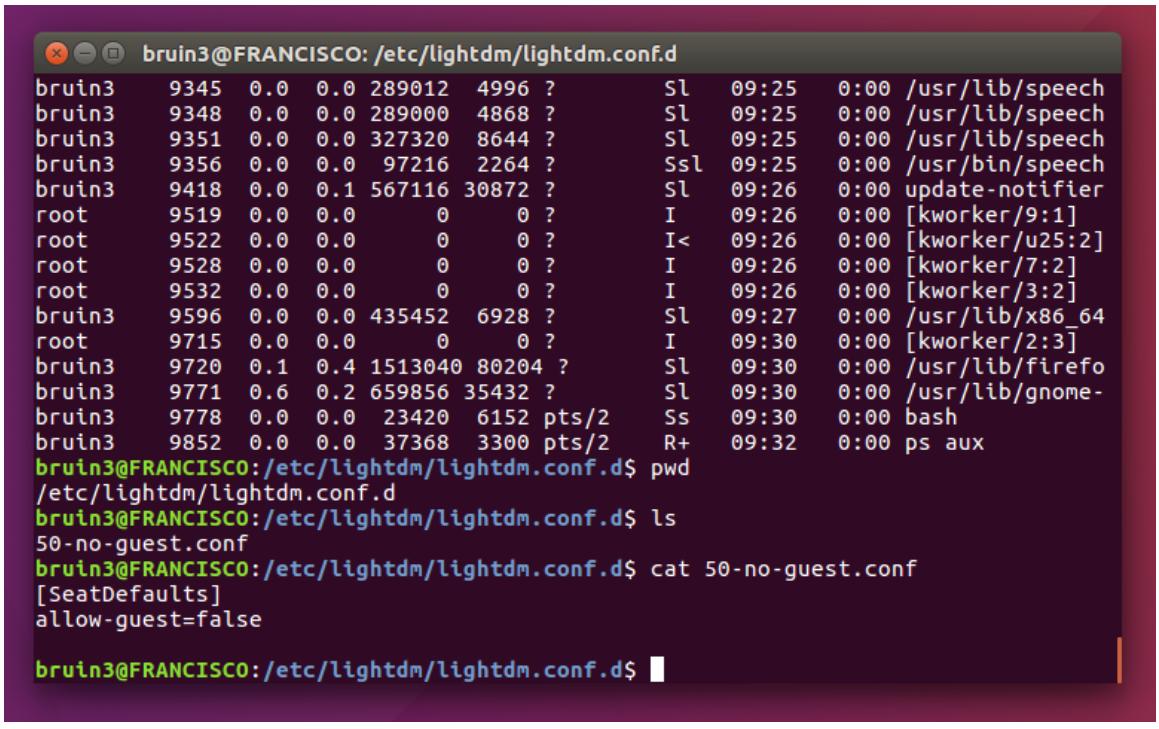


Figure 2

5. We have disabled the guest login

Judges can confirm from the login screen.



6. When students leave the team they also need to lose access to Gitlab.

Gitlab has expiration dates for this purpose as seen in Figure 3. Judges can confirm this setting with a visit to the Gitlab webbsite.

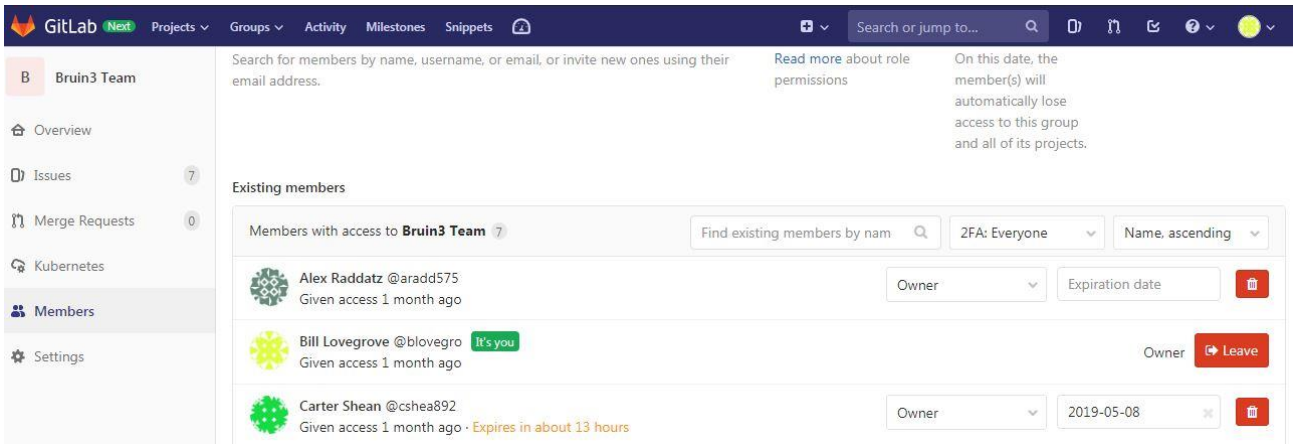


Figure 3

7. A misdirection Wi-Fi router discourages attacks.

Judges will note a public non-secure Wi-Fi network called Bruin-3. An inspection of the vehicle will show that this router does not connect to the actual vehicle but is for misdirection only.

8. The Wi-Fi router does not broadcast its name and has a misdirection name

Judges will be given the name of the actual Wifi network and note that it is not being broadcast.

Judges note that the name of the actual Wifi network is a misdirection in itself.

9. The Wi-Fi router uses both WPA security and a restricted mac address list.

Judges will note that WPA security is turned on for this device.

Judges will be given the password and note that access is not allowed from unauthorized mac addresses, even with the password.

10. Geofencing

Judges will cover the GPS antenna with foil to block signal and notice that the dashboard indicates loss of signal and unknown fence status. Observe that the controls are not operational.

The team will move the vehicle to a region outside the test track and not that the fence status indicates that the vehicle is outside the fence. Observe that the controls are not operational.

11. The DOD code is only installed on University computers, not student computers.

Judges can examine student computers at the competition for the presence of the RTK software. They can question team members about the know locations of the software.

12. Only students who are approved to work on the DOD code and who have signed the non-disclosure agreement are given the password.

Judges can query the non-RTK team members about their knowledge of passwords and their access to the RTK code.