MANIPAL INSTITUTE OF TECHNOLOGY
MANIPAL
A Constituent Institution of Manipal University

PROJECT MANAS
BRINGING BITS TO LIFE

27th INTELLIGENT GROUND VEHICLE COMPETITION

17th May, 2019

CYBER CHALLENGE REPORT

Team Leader: Siddarth Venkatraman (projectmanas.mit@gmail.com)
Tech Head: Shrijit Singh (tech_head@projectmanas.in)

I hereby certify that the development of vehicle, **Solo**, described in this report has been equivalent to the work involved in a senior design course. This report has been prepared by the students of Project MANAS under my guidance.

Professor & Head
Dept. of Computer Science & Engineering
Manipal Institute of Technology
Manipal - 576 104

Ashalatha Nayak Professor and Head of Department
Department of Computer Science & Engineering
E-mail: asha.nayak@manipal.edu

Contents

1 Introduction

Project MANAS, the AI robotics team from Manipal Institute of Technology, Manipal has designed its newest iteration of its autonomous bot Solo to compete in the 27^{th} Intelligent Ground Vehicle Competition. Solo is the next generation of our autonomous bot and represents the culmination of the hard work of our entire team. It continues to uphold MANAS's vision of pushing the boundaries of Artificial Intelligence and robotics, while ensuring its availability to the general population. Solo includes new cutting edge capabilities which have never been seen in other robots, including but not limited to it robustness, design, swiftness and software architecture.

2 Team Organization

The team is broadly divided into three separate divisions - Artificial Intelligence, Sensing & Automation and Mechanical. All subdivision and division heads are solely responsible for his/her division/subdivision. To assist with the managerial tasks of the team, we have a separate non-technical management division. The primary board comprises of the Team Leader, Tech Head and Team Manager who is responsible for the functioning of the entire team and take all majors decisions pertaining to the team under the guidance of our faculty advisers. The team is comprised exclusively of undergraduate students, numbering 63 in strength consisting of students from all branches of engineering and our interdisciplinary nature is the catalyst for our innovation and creativity.

The list of members who contributed towards Solo are: Avirat Varma, Shrijit Singh, Sahil Swaroop, Shivesh Khaitan, Arya Karani, Rishab Agarwal, Dheeraj Mohan, Sarathkrishnan Ramesh, Rakshit Jain, Raunaq Kalra, Dasarath Selvakumar, Shivanshu Agarwal, Chaitanya, Siddarth Venkatraman, Gaurav Singh Thakur, Manav Sachdeva, Tanaya Mandke, Ansel Dias, Omkar Jadhav, Vibhuti Ravi, Abhineet Choudhary, Adheesh H.M., Aneesh Chawla, Anish Biswas, Anurag Borkar, Apratim Mukherjee, Baidyanath Kundu, Dheeraj Rajaram Reddy, Dhruv Joshi, Garima Singh, Karan Khanna, Leander Melroy Maben, Sahil Khose, Sarthak Mittal, Shivam Agarwal, Aniket Bhawe, Asish Boggavarapu, Debayan Deb, Harsh Barde, H. Sai Manish, Parthesh Savla, Rohit Natu, Achintya Dutta, Akhil Bonagiri, Anirudh Ameya Kashyap, Arpit Chauhan, Kishore K., Gokul P., Nishan D' Almeida, Raj Tulluri, Ritwik Agarwal, Shoumik Dey, Shreesh Tripathi, Yagya Malik, Aditya Veerabahu, Akshat Rawat, Kaashvi Saxena, Manikya Sahai, Nikhil George Savio, Rishi Raj, Rithika Iyer, Ritu Chaturvedi, Siri Rajanahally

Total cost estimate of the entire bot with all components included is **$19,570**. The amount spent by the team this year is: **$3,060**. A huge cut down on the expenditure is the result of team's efforts to reuse the components already used last year.

3 Overview of NIST RMF Process

The Risk Management Framework provides a process that integrates security and risk management activities into the system development life cycle. The risk-based approach to security control selection and specification considers effectiveness, efficiency, and constraints due to applicable laws, directives, executive orders, policies, standards, or regulations.

Figure 1: RMF Process
Source: https://www.varonis.com/blog/risk-management-framework/

3.1 Categorize

Determine the criticality of the information and system according to potential worst-case, adverse impact to the organization, mission/business functions, and the system.

3.2 Select

Select security controls starting with appropriate baseline using categorization output. Apply tailoring guidance as needed based on risk assessment. Security controls are the hardware, software, and technical processes required to fulfill the minimum assurance requirements as stated in the risk assessment.

3.3 Implement

The agency should have documented and proven that they have achieved the minimum assurance requirements and demonstrated the correct use of information system and security engineering methodologies.

3.4 Assess

Determine security control effectiveness, are controls implemented correctly, operating as intended, and meeting the security requirements for the system and environment of operation. If necessary, the agency will need to address and remediate any weaknesses or deficiencies and then documents the security plan accordingly.

3.5 Authorize

Top management tests and approves the secured system based on the accepted risk it is willing to tolerate. It will identify how much risk is still present, and either authorize it or decide on changes needed.

3.6 Monitor

Set up an ongoing monitoring and assessment schedule for security controls to measure effectiveness. Document system or operation adjustments, and include impact analyses of changes made, Report findings to information security officials.

4 Identified threat concept

Our bot Solo is part of the 21st regiment of the forward marching US Army currently stationed in middle east. It is a hot and dry environment. This type of environment puts a lot of strain to soldiers carrying heavy equipment. Solo duals as a equipment carrier and a communication medium by creating a portable communication server which is accessible in the vicinity of the bot. With the solenoid lock keeping the contents of the box safe from unauthorized access, the bot will initiate a self destruct protocol when not in the designated range.

5 Thorough threat modelling

For the identified threat concept, the following are the possible threats and their impact level to security:

Threat	Confidentiality	Integrity	Availability
Access to the server hosted on the bot	High	Low	Low
Bot can be captured by enemy out of the geo-fence	Moderate	High	High
Illegal breaking into the storage carrier	High	Low	Moderate
Eavesdropping on communication	High	Low	Low
Changes in admin level management controls	Moderate	High	High
Changes in code base	Moderate	High	Moderate
Leaking sensitive information of other users	High	Low	Low
Leaking location information of the bot	High	Low	Low

The main threat is unauthorized access to the server hosted. This can lead to severe security breach. If the enemy gains access to the server a variety of information can be leaked

On a basic level the enemy can eavesdrop onto the communication on the server.Sensitive messages exchanged between battalions regarding location, plans and action can be leaked. The enemy can gain access to the live tracking feature of the bot giving away the location of the battalion as well as the current set radius of geo-fence, this could lead to an ambush on the battalion or capturing of the bot. Capturing of the bot means leaking of sensitive information as well as breach in the storage carrier. This is loss of confidentiality i.e. disclosure of information in the security objective. The enemy can gain access to basic features such as controlling the buzzer, lights and lock on board the bot.

On higher levels, the enemy can access to the admin level controls such as managing users and bot's code base. This could leave the bot vulnerable to modification of code base by enemy and thus a mole amongst the troops. This falls under loss of integrity i.e. modification or destruction of information in security objective. The enemy can block out current admins making the bot completely in control of the enemy. Loss of availability i.e. disruption of access in security objective. Sensitive information about user's logs on activity on the bot

like sessions or accessing storage carrier can reveal patterns of idle time which can be utilized by the enemy for their gain.

The information system, majorly, has two levels:

- Operational Management
- Tactical Management

The operational management is concerned with performing day to day activities, in this case users accessing the bot for tracking the bot and communication. The information is given to the user based on current information the system receives from the bot. These users can set radius for the geo-fence and track location of the bot while communicating with fellow battalions about progress, plan of action and threats.

The tactical management is concerned with overseeing the daily activities of users at the operational management level and possibly root out threats or block malicious users. These users monitor sessions of the user and logs to storage carrier as well as can modify roles/access of users of the information system.

The type of information system on the terms of mission-based information types is a homeland security - border and ground transportation information type. The bot's main purpose in the scenario chosen is to carry goods along with the battalion and implement border patrolling. The services delivery mechanism offered is of type direct services for citizens - Military operations.

The information system is divided into 5 subsystems:

1. Guest (access level 0)
2. General user (access level 1)
3. Developer (access level 2)
4. Admin (access level 3)
5. Database

The Database can only be accessed by the admin indirectly through management controls. There lies the innermost boundary in the information system between the admin and the database. The developer does not have access to admin level management controls and is dependent on admin to make management decisions such as assigning developer roles to users, this is the second boundary. A developer's task is to make modifications in the code base, these can only be viewed by a general user. The view of the information system and the ease of interactivity is dependent upon the developer and thus the third boundary. The 4^{th} boundary is of the general user who can only view information and hence the 4^{th} boundary beyond which no information can be accessed in any scenario. A subsystem independent of all the above is the guest subsystem. The guest subsystem has no access to any information. It is dependent on the admin to decide the user's access level. The outermost boundary encapsulating all the above which shields the information system with the outside world is log-in authentication boundary. Only after log-in can the user enter the information system.

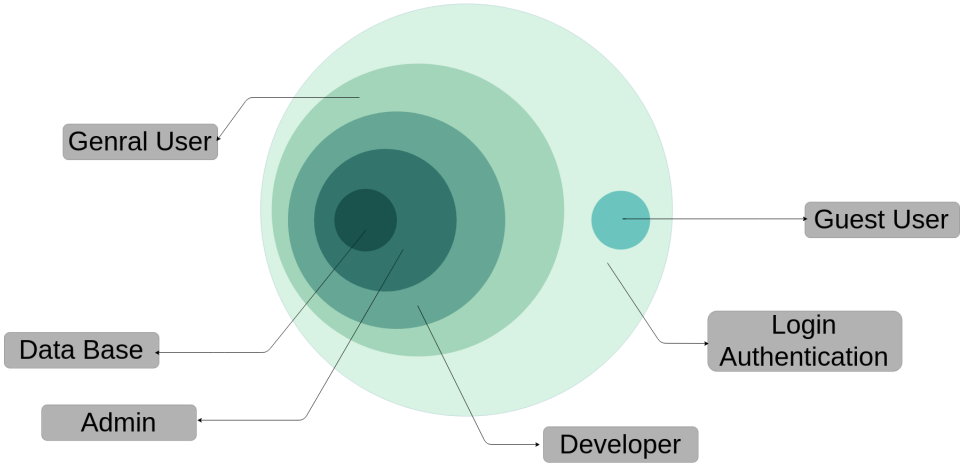

Figure 2: Information System Boundary

6 Identification and mapping of Cyber controls to counter identified threats

6.1 Defense in Depth

Defense in Depth (DiD) is an approach to cybersecurity in which a series of defensive mechanisms are layered in order to protect valuable data and information

Cyber Control	
Role based access control	AC-3(7)
	AC-3(8)
Role-based duties	AC-5
Privileged accounts	AC-6(5)
	AC-6(10)
Protected routes	AC-14
Identification and Authentication	IA-2(1)
	IA-2(2)
	IA-2(3)
	IA-2(4)
	IA-2(10)

6.2 Management and Operational controls

Cyber Control	
Account Management	AC-2
	AC-2(6)
	AC-2(7)(a)
	AC-2(8)

	AC-2(13)
Privileged Accounts	AC-6(5)
	AC-6(10)
Monitor Sessions	AU-2
Incident Report	IR6(1)
Position Risk Designation	PS2 (Security clearances)
Incident Response Plan	IR-8
Personnel termination	PS4 (Account termination by user)

6.3 Security Policies

User Account Policy
This policy defines what a user should do in order to have or maintain another user in a specific system.

Cyber Control	
Hashing Password	SC-13
Authenticator Feedback	IA-6
Cryptographic Module Authentication	IA-7
Unsuccessful login attempts	AC-7(1)
Authenticator Management	IA-5

Information Account Policy
This policy is to regulate access to information, hot to process information, how to store and how it should be transferred.

Cyber Control	
Unauthorized access on protected routes or lower access level user trying to access admin pages	SC-5(1)
Privileged accounts	AC-6(5)
	AC-6(10)

Remote Account Policy

Cyber Control	
Wireless access	AC-18(1)
Mobile access control	AC-19(1)
	AC-19(2)
	AC-19(3)

Network Policy
This policy is to restrict the access of anyone towards the network resource and make clear who all will access the network. It will also ensure whether that person should be authenticated or not.

Cyber Control	
Role-based access control	AC-3(7)

Role-based duties	AC-3(8) AC-6(5) AC-5

7 NIST RMF Process Applied to Competition Robot

7.1 Description of implemented Cyber controls

Wireless/Remote Log-in:
To gain access to the features of the information system, the user has to login with valid credentials. A database is maintained with every user's login credentials, email id and password, and other user information such as name, access level/role, username for that account and Validity of the account. Upon a login attempt, the credentials entered are matched with the ones in the database corresponding to that user, upon match the user is authenticated and redirected to the Home page. If the user does not exist (i.e. email id does not match) or a wrong password was entered, the user is denied access into the information system. This is in accordance with the clause AC-18(1) which states that information systems are protected by authentication.

Unsuccessful Log-in
With accordance to the clause AC-7(1), a user is given upto 3 tries in the case of an unsuccessful login attempt, after which the user's account is blocked until the admin interferes.

Sign-Up/Register
Signup/Register - Prior to a user logging into the information system, the user must first register into the system. The signup requires user information - name, username, email id, password. These are stored in the user database and fetched when user attempts logging in. Any of the above credentials must not be fully comprised of spaces. The clause AC-2(8) defines Dynamic Account Creation, which is implemented in this.

Session Lock
In case of inactivity for a particular information outlet for the specified time period, the information outlet is frozen until the information outlet is revoked through a secure re-connection scheme.

USB access
Access to USB ports are controlled and made available based on roles and priority levels of users to prevent sharing of sensitive information in accordance with AC-20

Password Authentication
The above mentioned login process uses password as the authenticator. Each user is given to enter a password, the password has to be of the format:

- Minimum length of the password should be 8 characters
- Must have at-least 1 uppercase letter
- Must have at-least 1 digit
- Must not contain any spaces

The security of the password is integral and hence in accordance to the clauses:

- IA-5(1), the password has the above mentioned constraints.

- IA-6, the password is obscured from the viewer on a computer/laptop and displays feedback for a limited time before obscuring it on mobile devices.
- IA-7 and SC-13, the password is stored as a hash into the database. Incoming password upon login attempt is also hashed and compared. Thus the password of the user is always obscured from the organization as well.

Access Levels
Each user in the database has a role assigned based on their access level. These access levels guide the information abstraction for each user i.e. Role Based Access Control (RBAC). The role based access levels defined are :

Access Level	Role	Permissions
0	Guest	Can only log in, full information abstraction.
1	General User	Has access to limited information like location/live tracking of the bot and communication over the network
2	Developer	Has access to all the above and can modify code.
3	Admin	Has access to all the above, in addition to that admin has access to management system - Delete users, change access level of users, block/unblock users and monitor user sessions.

A registered user has, initially, an access level of 0. The admin changes the access level for the user if need be. If a user tries to change their own access level or some other user's access level higher than theirs, the user's access is revoked and account is blocked. The system is in accordance with the clauses AC-3(7) for role based access control, AC-3(8) revocation of access based on security guidelines and AC-5 role based duties.

Protected Routes
The information system implements protected routing i.e. An unauthorized user trying to access the information system or an authorized user trying to access a sub-system in the information system beyond the scope of the user's access level, are all blocked. The user is rerouted to the login page (if not an authorized user) or blocked (if authorized user trying to access beyond their scope). The clause AC-14 is supported by the above implementation of a mandatory identification/authorization and SC-5(1) to restrict internal users.

Geo-Fencing
Given the scenario chosen for the bot, a live tracking option is available. The user can track the movement of the bot and can set radius of a hypothetical Geo-Fence. A map with the precision upto 1-2 meters shows the real time location of the bot and the Geo-Fence of the set radius. If the bot goes beyond the circle of set radius, the bot waits for 1 min (radius changes or corrects it's course) and then self destructs. A buzzer is activated to denote the bot is going to self destruct.

Communication
The bot doubles as a communication hub, in the likely event of primary communication breakdown. The server acts as a communication medium on which multiple users logged in can communicate through messages i.e. the bot provides an alternate telecommunication service in accordance to the CP-8 clause. The messages passed are encrypted and decrypted on sender and receiver side respectively, thus a secure alternate communication method is provided.

Code Base
The information system provides an option to view the files in the system, including the code files. It provides

a functioanlity to make changes/modify the files. A user of access level greater than 2 i.e. a developer or an admin has access to this functionality. This makes sure that unauthorized users cannot access the code base as well as allows dynamic modification of code base or files.

Admin Management
As admin, the user gets access to management systems. These management systems provide functionalities to maintain user base and change a user's role/function in the system. The management systems are as follows:

- Modify a user's access level/role
- Block/Unblock a user (for security concerns)
- Monitor user's sessions (log-in and log-out time)
- Monitor logs to the storage carrier
- Delete malicious users/accounts

The monitoring of sessions and logs to access of storage carrier are audit event, given in the clause AU-2.

Security Notification
In case of security breach, an email is sent, notifying the admin of the possible threat. This allows the admin to block or delete malicious users. The events regarded as security breach:

- Unsuccessful log-in attempts
- Unauthorized access to routes
- Access to routes out of the scope of a user's role

In accordance to the clause IR-8, the above security breaches and the solution is an incident response plan and the incident reporting is done via email, IR-6(1).

System Notifications
The system is designed to show on-screen notifications of recently completed tasks or errors in any recently given tasks. The alerts appear in the following scenarios:

Alert	**Scenario**
Successful login	
Unsuccessful login attempt	Wrong Password User not found Blocked account
Successful signup	
Unsuccessful signup	Empty Field Wrong e-mail format Wrong password format
Successful blocking/unblocking a user	
Unsuccessful blocking/unblocking a user	Wrong admin password User not found
Successful change of access level of a user	
Unsuccessful change of access level of a user	Wrong admin password

	User not found
Successful deletion of a user	
Unsuccessful deletion level of a user	Wrong admin password User not found
Unauthorized access of route higher than user's access level	
Successful logout	

These notifications give an indirect way of showing if the task is completed or not.

Mobile Access Control
All the above functionalities run smoothly on a mobile device as well, for on the go access to the information system. All kinds of mobile devices mentioned in the clauses AC-19(1), writable/portable devices, AC-19(2), personally owned portable devices and AC-19(3), portable storage devices with no identified owner.

Control Panel
The control panel on the homepage offers a variety of options:

- Lock/Unlock the storage carrier
- Switch On/Off buzzer
- Switch On/Off light

A user with access level greater than or equal to 2, has access to these controls. The lock is a safety measure, as only authorized users can unlock it thereby securing the storage carrier's contents. The lights are required for the bot to navigate in the dark, the lights are controlled by the user. The buzzer can act as a beacon call for rallying units if necessary or during self destructing of the bot as a warning.

MAC capture
MAC address of every connection is captured and logged to have accountability in case of failure. In accordance with IA-3

Magnetic Lock control
The system and sensors are physically locked using a magnetic lock which can be unlocked only by authorized personnel through their fingerprint using their mobile phones that are connected to the system that is on the bot. Accordance with PE-3

7.2 Description of Cyber Controls Demonstration Strategy

The officials will be handed a device of their choosing - a laptop or a mobile device. They may choose their own device too. They will be given the I.P. for the website. The control demonstration will happen in the following steps:

1. **Sign-up process**: The officials CAN sign up. They can try keeping field empty and wrong format for email or password. On screen notifications will display the error. If they sign up with correct credentials and can notice they are routed to the log-in page with on screen notification confirming the success.
2. **Log-in Process**: The officials can now log-in using their credentials entered in the previous step. They can try wrong email or wrong password and notice the on screen notification confirming error. Upon 3

unsuccessful attempts the account is blocked with on screen notification of the same. They can log-in with correct credentials, they will be routed to the homepage, with on screen notification confirming successful log-in. An email is sent to their email id confirming the same.

3. **Access Level**: A new account has initial access level of 0, the officials will initially have an access level of 0. They can notice no functionalities on the website and cannot directly access any routes either. The presenter their, as admin of the page will update the official's access level. Upon reloading of the page, officials may notice functionalities added onto the navigation bar. The officials on access level 1 can now access the track page and communication page.
4. **Bot tracking**: The track page, shows a map with the precise location of the bot up-to 1-2 meters. The officials are welcomed to change the radius for the geo-fence. The presenter will navigate the bot to show live tracking of the bot as well as take the bot outside of the geo-fence to show the on screen notification that shows the bot is set to self destruct.
5. **Communication**: The Officials can next check out the communication page. Here the officials will be shown the total users in the database and they can initiate communication with any one by sending a message. The officials can send and receive messages both of which will be displayed on screen along with a time-stamp. These messages are encrypted during exchange. When one user logs off the messages read by the user are deleted for security. The officials can initiate communication with the presenter who will demonstrate this feature by logging off or vice-versa
6. **File Browser**: The presenter as admin can update the access level of the officials to 2, giving them the role of a developer. As developer the officials have access to the file system that contains code for the information system. They can explore the file system and change/modify anything in the files.
7. **Control Panel**: The officials can now view the control panel on the homepage. The officials are welcomed to try any of the controls and view the result in real time on the bot. Controls such as locking/unlocking storage carrier, switching on/off light and buzzer.
8. **Management System**: The presenter as admin will update the access level of the officials to 3, giving them the role of an admin. As admin they have access to management pages such as updating access level, deleting accounts, blocking/unblocking accounts or monitoring user's sessions. The presenter while updating access level of the officials will demonstrate the update access level page.
9. **Account Deletion**: The official can now try deleting an account. They can try wrong password, non existential user and notice on screen notifications displaying the corresponding error. The officials are given a dummy account to delete. On success, notification is displayed on screen.
10. **Block/Unblock accounts**: The officials can checkout the change validity page. They can try wrong credentials for corresponding error to be displayed on screen. The officials will be given a dummy account they can block and unblock and notice the success notification.
11. **Monitor users**: The officials can visit the monitor page. Here the officials will notice all the sessions from the past and through the demonstration time. Every log contains user-name, log-in time and log-out time. The officials can notice their own entries as well.
12. **Log-out**: The officials can now logout of the website, they will be routed to the welcome page from where they started.