Towards a Critical Review of Cybersecurity Risks in Anti-Poaching Systems

Christelle Steyn and Dewald Blaauw
Centre for AI Research (CAIR), School of Data Science & Computational Thinking, and Department of Information Science, Stellenbosch University, Stellenbosch, South Africa

xtel911@gmail.com
dnblaauw@sun.ac.za

Abstract: Anti-poaching operations increasingly make use of a wide variety of technology for intelligence and communications. These technologies introduce cybersecurity risk, and they need to be secured to provide greater protection to the information and people involved in anti-poaching operations, ultimately protecting vulnerable animals better. A hypothetical network of anti-poaching technologies was simulated in Graphical Network Simulator 3 (GNS3), consisting of various field devices identified in the literature, and a main control room with relevant hardware devices. A virtual Kali Linux machine was connected to the network and played the role of a digital attacker or intruder. Several cyber-attacks were carried out, to show the risks inherent to such an interoperable and socio-technical network. These attacks included Man in the Middle (MitM) and Denial of Service (DoS) attacks. These attacks were then mitigated via system configurations. Further risks and threat considerations were identified in the literature. Using the STRIDE, DREAD and Attack Tree threat models, the risks to an anti-poaching network were classified and calculated. The most prevalent threats and the attacks performed in the simulation were all calculated to have a high risk level, posing a great threat to an unsecured network. The STRIDE classes of Denial of Service and Elevation of Privilege posed the most risk to the system, both having a calculated average risk score of 9 out of 10. Mitigations to general network threats and those identified in the simulation are mentioned. Additionally, authentication for such a system was investigated, as improper authentication practices were deemed a risk and provides a foothold for further risks in the network. Recommendations made, include the proper configuration of network devices, especially the router and switch, and the use of anti-virus, firewalls, and intrusion detection systems, as well as having an external audit performed annually. Multi-factor authentication, with a password/fingerprint combination, is recommended.

Keywords: cybersecurity, anti-poaching, GNS3, threat model

1. Introduction

1.1 Background Information

Poaching is the exploitation of wildlife that a state considers to be illegal (Duffy, 1999). Poaching is problematic for wildlife conservation (Cooney et al, 2016), and since 2008, poaching has reached a crisis point. Anti-poaching refers to the measures put in place to counter poaching. To combat poaching, conservationists make use of different technologies for intelligence and communication, and this has improved anti-poaching efforts (Thevar and Bhanot, 2021). Utilising technology introduces cybersecurity risks to a system and requires that a system is adequately protected and securely authenticated. Thevar and Bhanot (2021) state that poachers may have access to advanced technology that can infiltrate or attack anti-poaching systems.

Cybersecurity measures need to be implemented on socio-technical anti-poaching systems, which contain interoperable technologies and human actors. "Understanding, managing, controlling and mitigating risk" to relevant critical assets, is Sotnikov's (2022) definition of cybersecurity.

1.2 Problem Statement

Anti-poaching systems contain sensitive data, and a reliance on increasingly accessible technology, make them vulnerable to exploitation by progressively sophisticated attackers (Schoenfield, 2015). The formulation of risk mitigation strategies should have a high priority, as the poaching crisis is still a current problem, and the security of people and animals need to be guaranteed. While studies have been conducted on the use of various technologies in anti-poaching systems, very few address the specific cybersecurity concerns of such systems.

1.3 Limitations

It was anticipated that information regarding anti-poaching operations may be difficult to find, due to their confidential nature. The consultation of various sources can aid in forming a clear composite picture of a hypothetical, interoperable anti-poaching system.

1.4 Research Questions

The following research questions were asked:

RQ1: Can cybersecurity risks be adequately identified within a hypothetical anti-poaching system and mitigated using simulation tools?

RQ2: Can the risks identified in an anti-poaching system be calculated with threat models?

Together with a subsidiary question:

SQ1: What cybersecurity countermeasures are currently in place to protect the anti-poaching industry and what additional countermeasures can be added or modified to improve the safety of animals?

2. Literature Review

Literature on individual anti-poaching technologies is easy to source, but literature is scarce on current anti-poaching systems, and scarcer regarding the cybersecurity of these systems. By isolating the researched technologies and their relevant cybersecurity concerns, a picture of the risks faced by anti-poaching systems can be filled in. Academic sources, South African government guidelines and private initiatives' data were consulted.

Anti-poaching technologies identified to be pertinent to this study are:

- CCTV (DEA, 2020)
- Camera traps (CCF, 2022)
- Sensors (Yayha et al, 2019)
- Drones (Chapman & White, 2019)
- Mobile Apps (CCF, 2022)
- Tags (Bridge et al, 2019)

Common cyber-attacks on systems include Denial of Service (DoS) and Man in the Middle (MitM) attacks. These attacks can render systems unusable or infiltrate them to access information.

The then South African Department of Environmental Affairs (DEA) issued a guideline for anti-poaching systems, containing a threat management framework and suggested technologies (DEA, 2020). Another document contains a strategy regarding the creation of a national information system where rhino data can be centralised to advise security decisions, and calls for regular risk assessments (DEA, 2010).

The Connected Conservation Foundation (CCF), a technology backed anti-poaching initiative, was founded in 2015 by Dimension Data and Cisco (CCF, 2022). CCF makes use of numerous interoperable technologies to blanket a reserve and has succeeded in reducing poaching incidents (BusinessWire, 2018).

Borges (2021) lists malware (viruses, rogue software, trojans, spyware, worms), DoS attacks, phishing, rootkits, SQL injections and MitM attacks as the most prevalent threats to a system. Naagas and Palaoag (2018) compiled a comprehensive list of threats to an information system that can be applied here. Whitman (2004) also provides a list of threats and additionally names protection mechanisms that were employed – of which 100% of survey respondents used passwords. Authentication and identity management are important considerations for the security of systems.

Risk revolves around the probability of a threat affecting an asset, and the consequences of this. There are various types of risk, but here the focus is on cybersecurity risks. Threat modelling is a methodology where anticipated risks are modelled, to aid in determining countermeasures (Gonzales, 2022). This study will focus on several threat models, to aid in calculating risk.

Gonzalez (2022) states that pre-empting, isolating and countering threats can be achieved with threat modelling, which is vital to the organisation's security posture. There exist many threat models and threat models are not always used in isolation and combining models can provide a more holistic picture of the threat landscape. Attack Trees will be used to showcase overviews of existing threats. For the most prevalent system threats, STRIDE will be used to classify threats and the risk will be calculated using DREAD.

Authentication mechanisms make it more difficult for an attacker to breach a system and its failure poses a risk to a system. Passwords are a fundamental part of authentication but are easily disclosed by cyber-attacks (Almehmadi & Alsolami, 2019). The authors conclude that implementing multi-factor authentication (MFA) is necessary to deal with password vulnerabilities.

3. Method

3.1 Methodology

A hypothetical anti-poaching system was simulated in GNS3, running on a VMWare virtual machine, and can be seen in Figure 1. A virtual Kali Linux machine was connected to the system to simulate the role of an attacker.

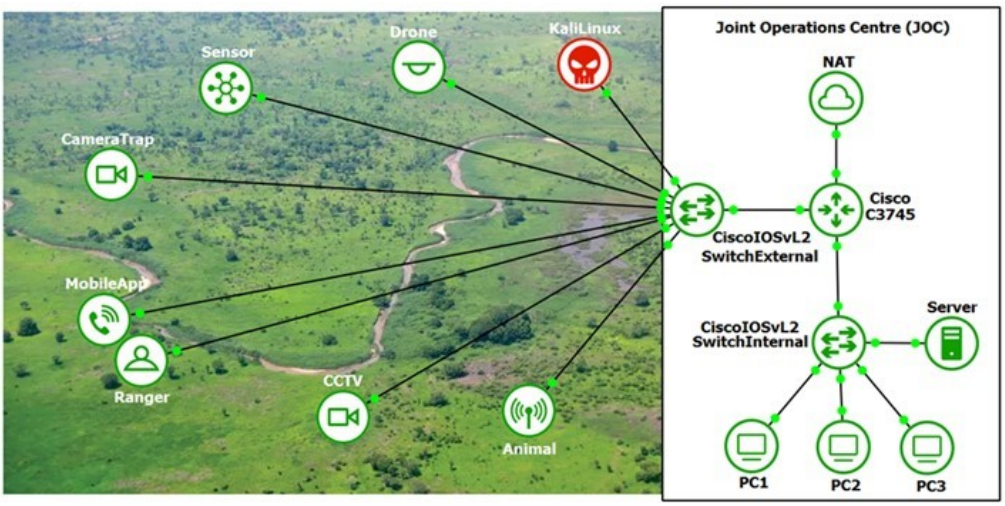

Figure 1: A hypothetical anti-poaching system simulated in GNS3

The Joint Operation Control Centre (JOC) is the headquarters of an antipoaching operation. All components are connected here via a switch and router to the Internet and to each other. PC1-3 represents the monitoring devices employed in the JOC.

The network was configured with a Dynamic Host Configuration Protocol (DHCP), and it was verified that all components received individual IP addresses and could communicate with the network and Internet.

3.2 Cyber Attacks

ARP poisoning, DHCP spoofing and starvation, STP attack, TCP/SYN flooding, CAM overflow and VLAN hopping were the attacks deployed on the network. These attacks were chosen because they are common attacks, cover different attack types (such as DoS and MitM attacks), and are considered among the common threats to a network by Borges (2021), and have been successfully simulated before (Bergs et al, 2022)

3.2.1 ARP Poisoning

IP forwarding was enabled on the attacking machine and Ettercap was used to launch the attack. The ARP of CameraTrap (IP 10.1.2.104) was poisoned. The attack was successful, as the component could not ping Google (8.8.8.8) and PC1 (10.1.1.101).

To mitigate this attack, DHCP snooping, and ARP inspection was applied to VLAN (Virtual Local Area Network) 1 on SwitchExternal (seen in Figure 2). Redeploying the attack, the console provided alerts that the mitigations were active, but the switch was unreachable from CameraTrap. The cause of this is uncertain and could be attributed to a software flaw.

```
Switch(config)#ip dhcp snooping vlan 1
Switch(config)#ip arp inspection vlan 1
```

Figure 2: Mitigations applied against ARP poisoning

3.2.1 DHCP Spoofing

MobileApp's (10.1.2.103) IP was cleared and verified to be 0.0.0.0. The attack was launched by providing Ettercap with a spoofed IP pool, Netmask and DNS server, as seen in Figure 3. MobileApp was instructed to reacquire its IP, however it acquired the IP from the legitimate DHCP server instead of the spoofed one.

DHCP Snooping can be applied to prevent DHCP spoofing, but its success could not be verified in this case.

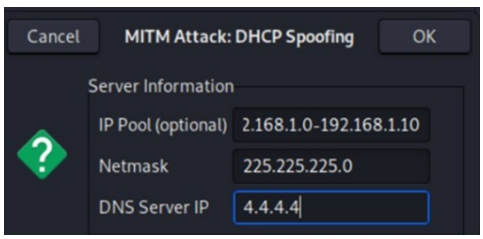

Figure 3: DHCP spoofing attack setup in Ettercap

3.2.1 DHCP Starvation

In the Kali machine, Yersinia was utilised to deploy this attack. This attack should slow the functioning of SwitchExternal, and Sensor (10.1.2.105) was used to verify this. Sensor was only able to intermittently ping Google and PC1, with every other ping experiencing a timeout, meaning the attack was successful.

DHCP snooping and rate limiting were used to counter the attack. The rate limit was set to 100 on SwitchExternal's interface with the Kali machine, as per Cisco (n.d.)'s recommendations (seen in Figure 4). When the attack was redeployed, Sensor was able to ping Google and PC1, making the mitigations effective.

```
Switch#
Switch#configure t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#ip dhcp snooping vlan 1
Switch(config)#interface g0/1
Switch(config-if)#ip dhcp snooping limit rate 100
```

Figure 4: Setting DHCP snooping and rate limits on switch

3.2.1 STP Attack

The Spanning Tree Protocol (STP) of VLAN 1 on SwitchExternal was viewed, with note being taken of the root address. Yersinia was instructed to claim the root role of the switch, which resulted in the root address being altered (Figure 5a and 5b) and the port now showing it to be the that of the Kali machine.

```
Switch>show spanning-tree vlan 1

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    32769
              Address     0cb7.b0c5.0000
              This bridge is the root
```

5a

```
Switch>show spanning-tree vlan 1

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    32769
              Address     0cb7.b0c4.0000
              Cost        4
              Port        2 (GigabitEthernet0/1)
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
```

5b

Figure 5: a) SwitchExternal's root address before the attack b) Altered root address and port after the attack

The main mitigations for the STP attack are to apply portfast, bpduguard and guard root. Once these have been implemented and Yersinia relaunched its attack, it could be seen that the mitigations proved successful, as the root role of the switch was not altered.

3.2.1 TCP/SYN Flood

Hping3 was commanded to flood SwitchExternal (Figure 7), with the intention of monitoring network traffic with Wireshark. Here the computer resources proved insufficient to make use of Wireshark while the attack was active and had to be abandoned. Ranger (10.1.2.102) was inspected to view the effects of the attack. Pinging Google resulted in timeouts or high latencies, but pinging PC1 or the switch was possible with normal latencies.

```
┌──(root💀kali)-[~]
└─# hping3 -V -c 100000 -d 10000 -S --flood 10.1.2.1
```

Figure 7: Command to launch TCP/SYN flood via hping3

A firewall was implemented by Bergs et al (2022) to combat this attack but could not be implemented here or be verified to be effective.

3.2.1 CAM Overflow

The MAC (Media Access Control) table of SwitchExternal was inspected and showed that it had ample space left for new connections (Figure 8). Using the macof tool on the Kali machine, it continuously generated and sent MAC addresses to the switch. The expectation was to see that the MAC table now had zero space left, but instead it was found that SwitchExternal went down and ceased to respond to commands. Animal (10.1.2.100) was used to ping Google and PC1. The former experienced high latency and timeouts, and the latter presented with intermittent high latency.

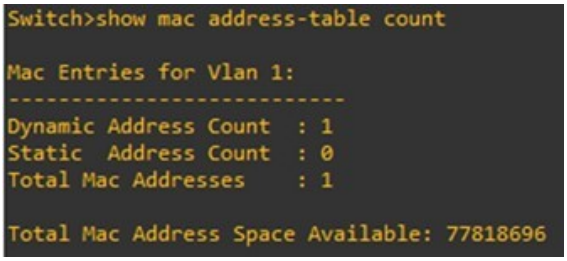

Figure 8: SwitchExternal's MAC address table, showing space available

Port security for the Kali machine's port was enabled on SwitchExternal to mitigate the attack. Heintzkill (2021) recommends only enabling five MAC addresses to be received from the Kali machine, after which the port will shut. SwitchExternal then withstood a relaunched attack and Animal could ping Google and PC1 with normal latency and no interruptions.

3.2.1 VLAN Hopping

After verifying that no trunks were present, Yersinia was used to launch an attack where it "enables trunking" on SwitchExternal. Upon reinspection it could be seen that the Kali Machine had created a trunk link on the switch, which could enable the attacker to access traffic on the link.

To mitigate this attack, trunking was disabled, and DTP (Dynamic Trunking Protocol) prevention was enabled on the switch, seen in Figure 9. After attacking again, the switch was prompted several times for a trunk link, but none were present, making the mitigation successful.

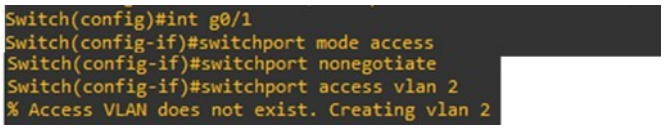

Figure 9: Mitigating VLAN hopping on SwitchExternal

3.3 Threat Modelling

Three threat models were considered for this study. Attack Trees are diagrams that include a root node as the attacking goal, with leaf nodes showing the ways in which an attacker can achieve this goal (Schneier, 1999). The STRIDE threat model can be used to classify threats into six categories – Spoofing, tampering, repudiation, information disclosure, denial of service or elevation of privilege (Abomhara, Gerdes & Køien, 2015). The DREAD threat model assigns numerical scores to identified threats and then translates theses scores to a qualitative risk level (Zhang et al, 2021). DREAD is short for:

- Damage Potential: How much damage can a threat cause?
- Reproducibility: Can the threat be easily duplicated by others?
- Exploitability: How easy is it to exploit the threat?
- Affected Users: Internally or externally, how many users will be impacted by the threat?
- Discoverability: Can one easily detect the threat?

3.4 Authentication

CERN (2018) provides a comprehensive list of good password practices and recommendations that can be considered, as it could be assumed that passwords will be present in an anti-poaching system. To satisfy MFA, additional authentication mechanism needs to be considered. Ali, Dida and Sam (2020) investigated the types of authentications most effective against certain threats, seen in Table 1.

Table 1: Authentication countermeasures against threats (Ali, Dida, and Sam, 2020))

Threat	Authentication Countermeasure
Spoofing	Biometric
Phishing	MFA
Trojan	Biometric
MitM attack	Biometric (fingerprint) and MFA
DoS attack	Biometric (fingerprint)

The use of password managers can also be considered, as CERN (2018) state they are effective in creating and storing strong passwords, as well as verifying previously accessed websites for legitimacy

4. Analysis and Findings

4.1 Cyber-attacks Summary

Table 2 provides a summary of the cyber-attacks performed, categorising them as MitM, DoS or Layer 2 (L2) attacks. It shows that several attacks can affect an anti-poaching network and that risk is evident. However, the table also indicates that these attacks can be mitigated with appropriate network configurations and component implementations.

Table 2: Cyber-attacks summary

Type	Attack	Effect on Network	Mitigation	Result
MitM	ARP Poisoning	Pings were unsuccessful and suffered timeouts	DHCP snooping and ARP inspection applied to switch	Switch not reachable, but alerts appear indicating mitigations
MitM	DHCP Spoofing	No effect, failed attack.	DHCP snooping (not applied here for this attack)	N/A
DoS	DHCP Starvation	Pings suffered higher latency or timeouts	DHCP snooping and rate-limiting applied to switch	Enabled the switch to limit and filter traffic coming from the Kali machine
MitM	STP Attack	The Kali machine assumed the root role of the switch	portfast, bpduguard and rootguard applied to switch	Ensured continued authority of the switch and disabled the Kali machine's ability to interfere
DoS	TCP/SYN Flood	Pings were intermittently successful, but suffered timeouts and high latency	Firewall (Not applied here)	N/A
DoS	CAM Overflow	Pings suffered occasional timeouts and higher latency	Activated port security on the Kali machine's port	Pings were successful with normal latency
L2	VLAN Hopping	Kali machine creates a trunk link and can access network traffic	Disabled DTP and trunking	No trunking was detected

4.2 Threat Model

An attack tree was created, in Figure 10, envisioning the paths a cyber-attacker might take to breach the JOC, based on the attack presented here. The tree shows the goal of the attacker, to poach an animal, and the leaf nodes show how they intend to achieve this. "Break In" was greyed out as, in the scenario, it is deemed to be impossible for the attacker to achieve this and they must therefore go via the virtual route.

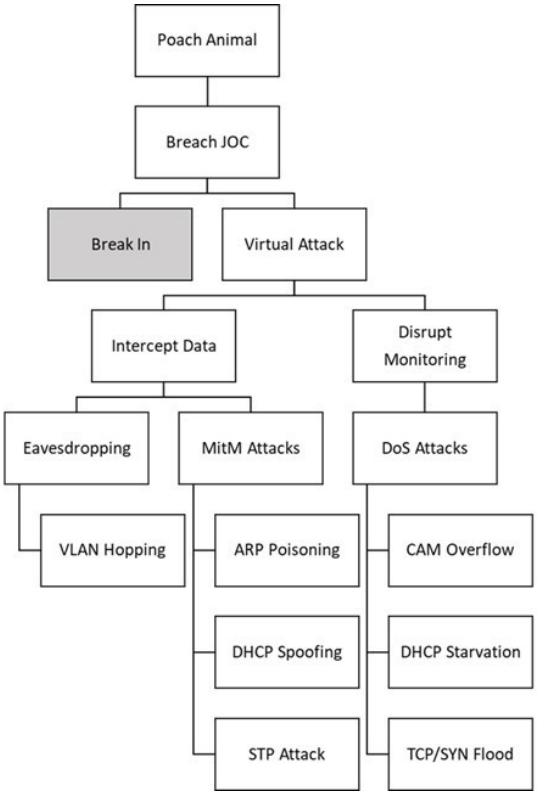

Figure 10: Poach Animal attack tree

Naagas and Palaoag (2018) provide the following equation to calculate DREAD risk scores: $rs_t=(D+R+E+A+D)/5$. A risk level of 7-10 is considered high, while 4-6 is medium and 1-3 is low.

First each DREAD class is individually scored and then all are added and averaged to get the final risk scores. Naagas and Palaoag (2018) investigated an information system and scored its risks, and their scores have been applied to the attacks and threats mentioned in this paper, in Table 3.

Table 3: STRIDE/DREAD threat and risk score table

Threat	STRIDE	D	R	E	A	D	Risk	Level
Malware								*High*
-Viruses	T	10	10	10	10	10	10	High
-Rogue Software	S	10	10	5	5	5	7	High
-Trojans	S	10	10	5	5	5	7	High
-Spyware	I	10	10	5	5	5	7	High
-Worms	T	10	10	5	5	5	7	High
DoS Attacks								*High*
-DHCP Starvation	D	10	10	5	10	10	9	High
-TCP/SYN Flood	D	10	10	5	10	10	9	High
-CAM Overflow	D	10	10	5	10	10	9	High
MitM Attacks								*High*
-ARP Poisoning	S	10	10	5	5	5	7	High
-DHCP Spoofing	S	10	10	5	5	5	7	High
-STP Attack	E	10	10	5	10	5	8	High
Phishing	I	10	10	5	10	5	8	High
Rootkits	E	10	10	10	10	10	10	High
SQL Injections	T	10	10	5	10	5	8	High
VLAN Hopping	I	10	10	5	10	5	8	High

From the above table, viruses and rootkits seem to pose the most individual risk to a system. The individual STRIDE classes can be viewed to find the specific class with the highest risk. Table 4 helps to determine that the class of Denial of Service and Elevation of Privilege are tied at 9/10 for highest risk. With regards to these classes, Naagas and Palaoag (2018) recommend Intrusion Detection Systems (IDS) to combat DoS attacks, and Maayan (2021) recommends a reliable antivirus, regular monitoring, the avoidance of phishing and up to date software as mitigations for rootkits, the main attack vector here for Elevation of Privilege. Due to the nature of the simulation, attacks falling under the Repudiation class could not be performed here.

Table 4: STRIDE risk scores and levels

STRIDE	Total Risk Score	Number of Threats	Average Risk Score	Average Risk Level
S	28	4	7	High
T	25	3	8.33	High
R	-	-	-	-
I	23	3	7.67	High
D	27	3	9	High
E	18	2	9	High

4.3 Multi-Factor Authentication and Authorisation

A password will be employed for secure access to an anti-poaching system. For additional security, a biometric mechanism can be added, with a fingerprint appearing to be the best option. A geographical location can be added to the MFA, in the case of secure data retrieval and storage inside the JOC. The access of peripheral agents, that often change location, to sensitive data can be verified by an OTP (One Time PIN) mechanism. While OTPs themselves can be vulnerable to attack, Peeters et al (2022) state that OTPs can be very effective in practice and that many users prefer it over other authentication mechanisms.

5. Conclusion

A hypothetical anti-poaching system can be simulated and attacked, mostly via MitM and DoS attacks. Mitigations can also be successfully applied.

With the gathered data, threat modelling took place. Attack trees captured visual depictions of threat sources and scenarios, while the STRIDE and DREAD models were used to classify and calculate risk. Individually, viruses and rootkits appear to pose significant risk to a network, but as a STRIDE class, Denial of Service (D) and Elevation of Privilege (E) maintained the highest average risk levels.

If authentication is securely implemented, with password managers and MFA, it lessens the risk for cyber-attacks to gain access to the network, as certain authentication mechanisms have been proven to remain resilient against attacks such as MitM and DoS.

5.1 Research Answers

RQ1: Yes. Risks were adequately identified with literature, simulation, and threat modelling.

A vast quantity of academic resources is available on information system risks, as well as cybersecurity countermeasures. The literature provided informed on risks, and these were incorporated into a simulation and threat model.

Cyber-attacks were successfully performed in the simulation, proving that risk is inherent in an unconfigured anti-poaching system. Only seven cyber-attacks were performed in the simulation, mostly DoS and MitM attacks, as other types of attacks were not always possible, such as password cracking or virus deployment. The simulation software here provided most of the capabilities with which one could mitigate these attacks.

The literature on threat models aided in identifying the risks associated with information systems. The threat models classified and calculated risks.

RQ2: Yes. The STRIDE and DREAD threat models were employed. The DREAD model proved useful in quantitatively scoring and calculating risk, and then translating it into qualitative terms based on the risk score. Classifying a risk with the STRIDE model and scoring it with the DREAD model ensures that risks can be prioritised and that the most problematic threats are highlighted.

SQ1: This question cannot be answered with the available data. While sources exist on anti-poaching technologies, no sources were found on what cybersecurity countermeasures are currently in place on such systems. No person working with these systems was found to be available for comment, even though contact was made with several organisations actively involved in this. Thus, additions and modifications cannot be made in confidence. Recommendations can be made, but will assume an unprotected system, and these recommendations will be general in nature or specific to the risks identified here.

5.2 Recommendations

The key recommendations that stand out as necessities when setting up an anti-poaching system, are:

- Install a comprehensive and reputable antivirus
- Keep software up to date
- Use Intrusion Detection Systems (IDS)
- Implement a firewall with appropriate configurations
- Educate personnel and create security awareness
- Have an expertly and securely configured network, router, and switch configuration.

This is not an exhaustive list and does not guarantee total security. It is recommended that at least one well-rounded cybersecurity expert is employed in anti-poaching operations, that can manage system risks and adapt the system when necessary. It can be investigated whether it may be feasible and beneficial for an independent cybersecurity audit to be performed annually.

While not performed here, regular risk assessments can complement threat modelling and be compiled into a risk framework, to guide anti-poaching cybersecurity strategies.

Regarding authentication, MFA is considered essential, where the combination of passwords and fingerprint biometrics are recommended. For certain use cases, geographical location factors or OTPs can be incorporated. Passwords should be strong and unique, and organisations can customise their password guidelines according to best security practices. Using an enterprise password manager should be considered, as this can generate and store highly secure passwords, avoiding the risk of insecure password behaviour.

5.3 Future Work

To accurately test the robustness of an anti-poaching system, an existing physical system would need to be assessed. New information can be gathered via surveys, interviews, and observations. More sophisticated cybersecurity tools can be introduced to protect the system and the effects of honeypots, DMZs, firewalls, and sniffers could be observed.

It can be investigated whether there is a more suitable threat model to apply to anti-poaching systems.

System authentication was reviewed, and research can be done into creating a more robust authentication system, via access control, MFA, and cryptography, that is practical for anti-poaching systems.

References

Abomhara, M., Gerdes, M. & Køien, G. M., 2015. A STRIDE-Based Threat Model for Telehealth Systems. *Norsk informasjonssikkerhetskonferanse* (NISK2015), pp. 1-15.

Almehmadi, T. & Alsolami, F., 2019. Password Security in Organizations: User Attitudes and Behaviors Regarding Password Strength. *16th International Conference on Information Technology - New Generations* (ITNG), Volume 800, pp. 9-13.

Bergs, C.-J., Bruiners, J., Fakier, F. & Stofile, L., 2021. Cyber Security and Wind Energy: A Fault-Tolerance Analysis of DDoS Attacks. International Conference on Cyber Warfare and Security, pp. 1-13.

Borges, E., 2021. Top 10 Common Network Security Threats Explained. [Online] https://securitytrails.com/blog/top-10-common-network-security-threats-explained [Accessed 30 June 2022].

Connected Conservation, 2022. Technology Solutions. https://connectedconservation.foundation/technology/ [30 January 2022].

Bridge, A. S. et al., 2019. An Arduino-Based RFID Platform for Animal Research. Frontiers in Ecology and Evolution, 7(257), pp. 1-10.

BusinessWire, 2018. Dimension Data and Cisco Take Anti-Poaching Technology into Africa. https://www.businesswire.com/news/home/20180508006383/en/Dimension-Data-and-Cisco-Take-Anti-Poaching-Technology-into-Africa [30 January 2022].

CERN, 2018. Password Recommendations.https://security.web.cern.ch/recommendations/en/passwords.shtml [28 July 2022].

Chapman, L. A. & White, P. C. L., 2019. Anti-poaching strategies employed by private rhino owners in South Africa. Pachyderm, Volume 61, pp. 179-183.

Cisco, n.d. Configuring DHCP Snooping. https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SXF/native/configuration/guide/swcg/snoodhcp.pdf [17 May 2022].

Department of Environmental Affairs, 2010. National Strategy For The Safety And Security Of Rhinoceros Populations In South Africa. http://www.stoprhinopoaching.com/wp-content/uploads/2021/08/DEA-National-Rhino-Strategy.pdf [3 February 2022].

Department of Environmental Affairs, 2020. Guidelines to Inform the Establishment of Anti-Poaching Related Systems and Services. https://www.environment.gov.za/sites/default/files/legislations/guidelinesforantipoaching_systemsestablishment.pdf [16 October 2021].

Gonzalez, C., 2022. Top 8 Threat Modeling Methodologies and Techniques. https://www.exabeam.com/information-security/threat-modeling/#:~:text=There%20are%20six%20main%20methodologies,threats%20facing%20your%20IT%20assets. [10 June 2022].

Heintzkill, R., 2021. CAM Table Overflow Attack Explained. https://www.cbtnuggets.com/blog/technology/networking/cam-table-overflow-attack-explained [18 May 2022].

Maayan, G., 2021. How to prevent a rootkit attack. https://blog.malwarebytes.com/how-tos-2/2020/01/how-to-prevent-a-rootkit-attack/#:~:text=To%20fully%20protect%20yourself%20against,then%20reinstall%20the%20entire%20system.&text=Phishing%20is%20a%20type%20of,or%20downloading%20an%20infected%20attachment.[6 July 2022].

Naagas, M. A. & Palaoag, T. D., 2018. A Threat-Driven Approach to Modeling a Campus Network Security. *ICCBN 2018: Proceedings of the 6th International Conference on Communications and Broadband Networking*, pp. 6-12.

Peeters, C., Patton, C., Munyaka, I., Olszewski, D., Shrimpton, T. & Traynor, P., 2022. SMS OTP Security (SOS): Hardening SMS-Based Two Factor Authentication. *ASIA CCS '22: Proceedings of the 2022 ACM on Asia Conference on Computer and Communications Security,* pp. 2-16.

Schneier, B., 1999. Attack Trees. https://www.schneier.com/academic/archives/1999/12/attack_trees.html [6 June 2022].

Schoenfield, B. S. E., 2015. Securing Systems: Applied Security Architecture and Threat Models. Boca Raton: CRC Press.

Sotnikov, I., 2022. How to Perform IT Risk Assessment. https://blog.netwrix.com/2018/01/16/how-to-perform-it-risk-assessment/ [25 May 2022].

Thevar, S. & Bhanot, N., 2021. How Technology has improved Anti-poaching Efforts. https://sanctuarynaturefoundation.org/article/how-technology-has-improved-anti-poaching-efforts [8 April 2022].

Whitman, M. E., 2004. In defense of the realm: understanding the threats to information security. *International Journal of Information Management*, Volume 24, pp. 43-57.

Yahya, A., Bogaisang, K., Gamoshe, O. G. & Maina, M. D., 2019. Anti-poaching System using Wireless Sensors Network. BIUST Research and Innovation Symposium, pp. 1-3.

Zhang, L. et al., 2021. A risk-level assessment system based on the STRIDE/DREAD model for digital data marketplaces. *International Journal of Information Security*, Volume 21, pp. 509-525.