Group 3 Final Project: Protecting Pandas

Jacob Napierskie, Kayvon Karimi, Michael Yap, RC Wright III

Shirley-Macros School of Engineering (SMSE), University of San Diego

CYBR-504: Applied Cryptography

Professor Templeton

April 14, 2025

Table of Contents

Introduction

The World Panda Protection League (WPPL) faces a critical challenge as poachers continue to successfully track and kill endangered pandas within the Jìnlìe Xióngmāo Bǎohùqū Forest Preserve. Despite deploying RFID-tagged collars, environmental sensors, and real-time monitoring systems, poaching persists even in areas presumed secure. The preserve covers extensive, rugged terrain, necessitating reliance on technology to monitor panda activity and alert ranger teams to potential threats.

Investigations revealed no direct evidence of hacking, physical sensor tampering, or data theft. Instead, our analysis uncovered that poachers might be exploiting indirect vulnerabilities through passive surveillance. Poacher camps contained equipment such as radios, cryptography literature, and encrypted USB devices. These findings indicate tactics similar to those documented in South Africa, where poachers utilized software-defined radios (SDRs) to intercept unencrypted RFID and GPS collar transmissions to track endangered rhinos (Juels, 2006).

Similar vulnerabilities exist within the preserve's current system. RFID tags use static identifiers that transmit openly, sensor data is sent without encryption over a 433 MHz RF mesh network, and uploaded images inadvertently expose geolocation metadata. Furthermore, the preserve's network of approximately 4,000 solar-powered sensors transmits predictable metadata, including timestamps, sensor IDs, and panda IDs, enabling poachers to infer movement patterns without decrypting the actual content.

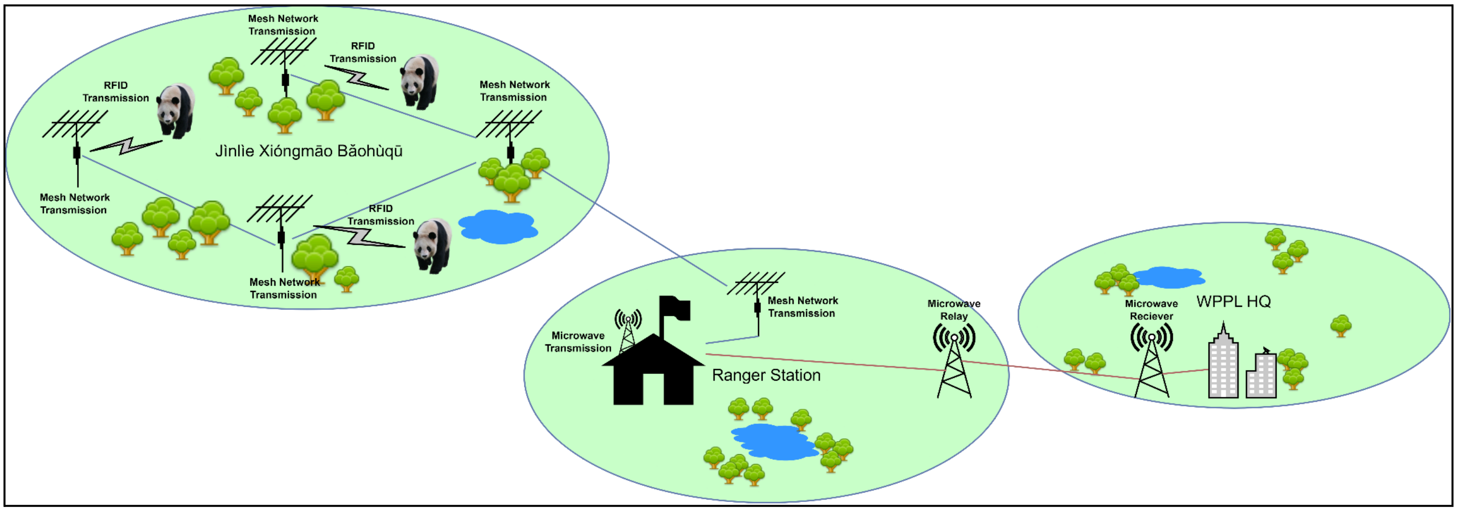
Additionally, critical vulnerabilities were identified at the ranger station, where tracking data is stored unencrypted on a local server, lacks multi-factor authentication, and operates on the same network as an unsecured Wi-Fi system. Previous attempts by consultants to secure the system through partial encryption failed to adequately address metadata exposure and traffic patterns, leaving the system vulnerable to analysis by adversaries and potential insider threats.

Compounding these technological vulnerabilities, the ranger team experiences high turnover with many part-time staff who possess limited cybersecurity training. This increases the risk of accidental data leaks or compromised security practices.

Our team was engaged to thoroughly investigate these issues and develop practical, affordable, and compatible solutions that can be integrated into the existing infrastructure without major hardware alterations. We propose a comprehensive, layered defense strategy incorporating technical upgrades, transmission obfuscation, operational enhancements, and improved physical security, all achievable within the preserve’s target budget of $100,000.

Figure 1.

Current Network Diagram



Note. Figure created by Jacob Napierskie via Draw.io.

Proposed Solutions

To effectively mitigate vulnerabilities identified within the preserve's tracking infrastructure, our team recommends implementing a comprehensive, multi-layered defense approach. Rather than depending solely on one solution, our strategy integrates technical enhancements, advanced monitoring capabilities, and strategic operational adjustments. Collectively, these measures significantly decrease the likelihood of exploitation by poachers. Importantly, these proposed solutions are tailored specifically to the preserve's existing technology, ensuring compatibility, cost-efficiency, and ease of use by non-technical personnel.

Encryption of Sensor Transmission to the Base Station

Problem

The preserve’s field sensors currently transmit data over a 433 MHz RF mesh network without any encryption. This leaves sensitive information, including panda detections, sensor activity, and environmental data, exposed to interception by adversaries using software-defined radios (SDRs). Even when message content is encrypted, past efforts in other preserves (such as Q and F) have failed due to incomplete implementations that left metadata such as timestamps and transmission patterns unprotected. These gaps enabled poachers to conduct traffic analysis and infer panda locations without decrypting the actual data. To mitigate this vulnerability, we recommend encrypting all communications between field sensors and the ranger station. Since modifying the core firmware of the sensors is not an option, we propose adding an inline encryption module between each sensor and its RF transmitter. This approach ensures that message content and metadata are fully protected before leaving the sensor, preventing interception and behavioral inference. The selected microcontroller must be low-power, cost-effective, and support modern authenticated encryption algorithms. Based on these needs, we propose the STM32 series, which offers hardware-accelerated AES encryption and is compatible with the preserve’s power and environmental constraints. Each module is estimated to cost $2.60, with a total deployment scope of 4,000 sensors (STMicroelectronics, n.d.).

Solution: Inline Encryption Using STM32 Microcontrollers

The proposed solution involves installing STM32 microcontrollers as inline encryption modules on each of the preserve’s 4,000 sensors. These modules will encrypt the entire message payload, including the timestamp, sensor ID, panda ID, and any environmental data, before it is transmitted over the RF mesh network. Unlike previous efforts in other preserves, this approach emphasizes full-payload encryption and metadata protection using authenticated encryption algorithms such as AES-CCM or ChaCha20-Poly1305. This ensures message confidentiality, integrity, and authenticity, even in the face of passive interception. The STM32 platform is a strong fit due to its low power profile, embedded cryptographic support, and affordability, making it suitable for scalable field deployment in remote and power-constrained environments.

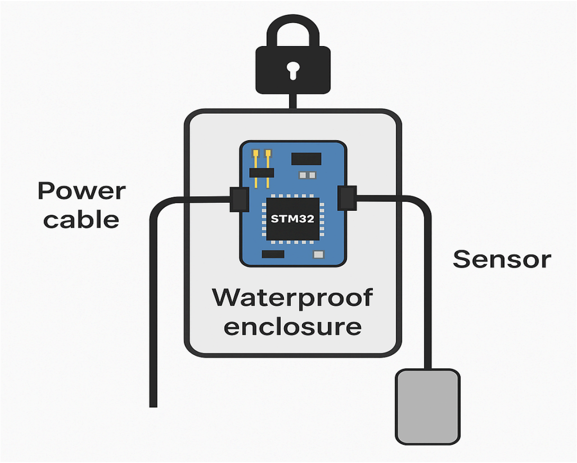
Implementation and Mitigation

After consultation with the preserve's ranger team, it was confirmed that they are willing to support full deployment of encryption modules across the preserve's 4,000 sensors, provided the process is simple and can be staged over time. To meet that need, the STM32-based encryption module will be designed as a plug-and-play device with weatherproofing and quick-connect interfaces to enable efficient installation in the field.

Each module will be preassembled and preprogrammed with firmware and symmetric encryption keys to eliminate the need for on-site configuration. The selected microcontroller series is the STM32 line, a low-power chip with hardware-accelerated AES encryption and ultra-efficient sleep cycles, ideal for the preserve's solar-powered sensor network. The module will be housed in an IP65-rated polycarbonate enclosure (e.g., Hammond 1551V2GY), providing protection against dust, moisture, and environmental wear (see Figure 2). Each module assembly (including the STM32 chip, waterproof case, input/output cabling, and mounting hardware) is estimated to cost between $8.80 and $13.20 per unit, making the full deployment cost range between $35,000 and $52,800, well within the project's preferred $100,000 budget.

Figure 2.

Example of the Plug-and-Play Device



Note. Image generated by ChatGPT (April 2025).

To enable field installation without technical expertise, each module will include waterproof connectors (e.g., M8 circular connectors or GX12-style aviation plugs) clearly labeled for input (sensor) and output (transmitter). Installation requires only disconnecting the existing sensor-transmitter cable, inserting the module in-line using the labeled connectors, and securing the device with mounting hardware such as Velcro straps, stainless steel zip ties, or industrial adhesive tape. Cable glands will be used where necessary to maintain waterproofing and reduce strain on wiring. Each installation is expected to take under 15 minutes per sensor.

To manage the scale of deployment, installation will be phased by geographic zone. The preserve will be divided into sectors based on sensor clusters and ranger patrol routes. With 25 rangers working in organized teams, and each team capable of completing 25–30 installs per day, full rollout is projected to take several weeks. Installation progress will be tracked using GPS-enabled mobile logs, and each module will be quality-checked and tagged upon installation.

This plug-and-play strategy ensures compatibility with existing infrastructure while minimizing the need for technical intervention in the field. By encrypting all outgoing transmissions at the sensor level, including metadata and environmental readings, the preserve eliminates a major vector for poacher surveillance. Even if transmissions are intercepted, they will contain no usable information. The simplicity, scalability, and cost-effectiveness of this design make it ideal for wildlife operations in rugged and remote environments like the Jìnlìe Xióngmāo Bǎohùqū Forest Preserve.

However, while encrypting network transmissions is a critical step in securing the preserve's data, it is not sufficient on its own. Consulting with the rangers confirms that sensors are only activated when a panda walks by or when battery levels are low. This means that the timing of each transmission itself can reveal activity even if the message content remains encrypted. Poachers do not need to decrypt a message to infer that a panda has passed nearby; they simply need to observe that a transmission occurred. Therefore, encryption must be paired with techniques to obscure transmission timing and patterns to fully defend against traffic analysis and behavioral inference.

Sensor Upload Frequency

Problem

While encrypting sensor transmissions protects message content and metadata from being read by adversaries, it does not prevent poachers from exploiting when transmissions occur. Ranger consultations confirmed that sensors only activate when a panda walks by or when a low-battery condition is triggered. This means that even an encrypted message becomes a signal that something happened. Poachers monitoring the 433 MHz mesh network with software-defined radios (SDRs) can spy and perform traffic analysis to identify patterns in transmission timing to infer panda presence or movement without decrypting anything.

Currently, messages are transmitted in near real-time if the network is up, or stored locally on SD cards and sent later. However, the rangers confirmed that real-time data is not necessary. They are fully comfortable receiving movement reports once per day, which opens the door to reducing transmission frequency and disguising behavioral patterns. To mitigate the risk of poachers using RF signal patterns to infer panda locations, we recommend reducing the frequency and predictability of sensor data transmissions. Since rangers do not require real-time updates, the current near-constant message relays present an unnecessary exposure point. The preserve can disrupt the poachers' ability to conduct effective passive surveillance by shifting to daily uploads and introducing transmission obfuscation techniques. We propose two alternative solutions to address this issue. Each option stands alone and can be selected based on the preserve's operational needs and implementation capacity.

Solution 1: Random Upload Timing with Padded and Dummy Messages

This solution calls for uploading buffered sensor data at a randomized time once daily. To further obscure communication patterns, the system would generate dummy messages at irregular intervals throughout the day. All messages, both real and decoy, would be encrypted and padded to a uniform size, preventing packet-level analysis. The combination of randomized timing and decoy traffic creates an unpredictable pattern, making it extremely difficult for poachers to determine when a panda has been detected. While this option adds moderate complexity due to timing variability and dummy message generation, it offers strong protection against traffic analysis. The impact on battery life is expected to be minor, depending on decoy frequency. Since messages are encrypted and processed at the server, rangers will not be exposed to or confused by dummy transmissions.

Solution 2: Fixed Upload Schedule with Padding and Guaranteed Transmission

This is the simpler of the two approaches, designed for more straightforward implementation and field management. It involves transmitting all buffered sensor data at a fixed time once daily, whether or not panda activity has occurred. This consistent behavior ensures the system never reveals inactivity through silence. As in the first solution, all messages are encrypted and padded to a uniform size to eliminate metadata cues. While this method simplifies scheduling and aligns well with ranger operations, the fixed upload time may become predictable over the long term unless augmented with decoy transmissions to obscure traffic patterns.

Implementation and Mitigation

Both proposed solutions significantly reduce the risk of poachers exploiting RF signal patterns to locate pandas. By eliminating near-real-time transmissions and introducing either randomized or consistent-but-covered upload behavior, the system becomes far more resilient to passive surveillance. These changes align with ranger input, real-time updates are unnecessary, and daily reporting is acceptable, providing operational flexibility without sacrificing effectiveness.

The transition from event-driven messaging to scheduled, obfuscated uploads leverages the rangers' ability to manage and install in-line modules across the preserve. Each module can handle timing logic, dummy traffic generation, and encryption without requiring changes to the sensors themselves. This modularity ensures compatibility with the existing infrastructure and minimizes disruption during deployment.

Pilot testing is recommended on a small group of sensors to assess the impact on network reliability, data integrity, and battery life. Results from this staged rollout will inform the broader deployment strategy. By starting small, the preserve can validate both technical performance and ranger workflows, ensuring a scalable, low-maintenance solution that strengthens protection without overwhelming staff resources.

Insider Risk

Problem

One of the preserve's critical security threats originates from insider vulnerabilities. The ranger team is relatively small, with 25 members, many of whom are part-time and experience high turnover. This environment results in reduced institutional knowledge, diminished accountability, and an elevated risk of intentional or accidental information leaks. Currently, the ranger station lacks essential security measures such as access monitoring, surveillance cameras, and building alarms. Sensitive panda movement data is stored on an unencrypted local server, secured only by basic username/password authentication without multi-factor authentication (2FA). Rangers regularly transfer sensitive data off-site via unsecured USB drives without proper auditing or oversight. Furthermore, sensors primarily activate based on panda movement, meaning even brief unauthorized access to the system could expose critical wildlife location data to poachers.

Solution: Role-Based Access, Monitoring, and Audit Integration

To mitigate these insider threats, we propose a comprehensive approach involving robust access controls, continuous monitoring, and mandatory cybersecurity training. First, we will implement two-factor authentication (2FA) on the server using SMS or authenticator apps like Google Authenticator, PAM, FreeOTP, or privacyIDEA. Ranger feedback has confirmed reliable cell reception at the station, making immediate implementation feasible without additional infrastructure.

Simultaneously, we will deploy logging tools such as auditd, Wazuh, or OSSEC to track and monitor file access, login attempts, and removable media usage. These tools will generate alerts upon detection of large data transfers or unauthorized access attempts, enabling timely detection of internal threats.

To enhance physical security affordably, we recommend deploying low-cost trail cameras at key entry points, particularly near the server cabinet and building entrances. A suitable option is the KJK Trail Camera 36MP 2.7K, available at approximately $28.07 per unit (KJK, n.d.). This camera offers 36 MP image resolution, 2.7K video capability, a quick 0.1-second trigger speed, a wide 130° detection angle, and IP66 waterproof rating, ensuring effective outdoor performance and discrete monitoring.

Implementation and Mitigation

Implementation will start with enhancing server security by enforcing unique Ranger logins, activating 2FA, and mandating regular password rotation every 30–60 days. Concurrently, we will introduce a USB access policy, using open-source solutions like USBGuard or Auditd to log and restrict removable media usage effectively. Next, we will install the KJK Trail Cameras at strategic locations, operating them on existing solar or backup power systems. If additional budget becomes available, RFID keypad locks or keypad entry systems can replace traditional locks to log and control physical access more precisely.

Finally, a mandatory one-day cybersecurity training session will be held for all rangers. This training will cover data sensitivity awareness, identifying and avoiding accidental data disclosures, recognizing signs of social engineering, and procedures for reporting suspicious activities. New ranger onboarding will incorporate this training to ensure continuous awareness. By systematically enhancing access control, physical monitoring, and cybersecurity training, the preserve can substantially mitigate insider risk, significantly strengthening the preserve's comprehensive security posture against poaching threats.

Panda Picture Uploads to WPPL

Problem

While speaking to the Rangers, the investigative team became aware that the Rangers will send pictures of the Pandas to the WPPL via a microwave relay system. The WPPL then uploads these photos to the main website once a week, to once every two weeks. It was determined that these photos are highly likely contributing to the death of the Pandas as there are multiple cases where a photo was sent to the WPPL, and within three to four days a Panda was killed. The photographic data is likely being exposed via the unsecure microwave relay system between the Ranger station and the WPPL HQ, and/or the images likely contain EXIF metadata that is not removed before uploading. This data typically includes elements of information that will aid in a poacher's objectives, such as geolocation information of where the picture was taken, and date and time the image was taken. This is a relevant finding as the Rangers **confirmed** that at least the last three poaching incidents took place within less than a week of an image being taken and uploaded to the WPPL.

In combination with radio frequency tracking, poachers are likely using image geolocation data, date and time the image taken, and terrain analysis techniques to determine an approximate area where the panda was last located. According to the Rangers, pandas can remain in a single area for a week or longer if there is available food and they are not disturbed.

Solution

To mitigate this vulnerability, we recommend taking measures to disable all geotagging within any cameras used to take photographs of the pandas and ensure all EXIF metadata from these images are removed using a variety of solutions. Additionally, it is our recommendation that the background within the images themselves should be cropped or blurred, and awareness training and policy updates should be conducted.

Implementation and Mitigation

We recommend the following implementation strategies:

1. Train the photographers, rangers, and field staff how to disable geotagging features on their cameras or smartphones. This will prevent sensitive location data from being embedded in the images at the time of capture.
2. Implement an automated workflow on the website which strips all metadata from images as soon as they are uploaded. This reduces human error by ensuring every image is sanitized consistently before it becomes public. If this cannot be accomplished, use a free

and open-source solution such as ExifCleaner application (Exifcleaner.com) to strip all the image metadata before uploading it to the website.

3. In addition to stripping metadata, explore techniques such as cropping or blurring background details that might reveal location-specific landmarks. This approach helps reduce context clues that could be exploited by poachers.
4. Lastly, update internal security policies and conduct regular training sessions for all staff involved in capturing, handling, and posting images. This training should focus on the risks associated with metadata and the best practices to mitigate those risks.

Operational Network Vulnerabilities

Problem

The current operational network at the ranger station presents multiple security vulnerabilities that could compromise the integrity and confidentiality of critical data. The network architecture consists of a mesh network of sensors that relay data to a central server located within the ranger station. This central server, running on Kylin OS with 32 GB of RAM, 4 TB of storage, and an Intel Xeon E5649 processor, is connected to five workstations with an unknown operating system. The data collected is transmitted once per day to a relay point via a microwave link, and from there, forwarded to the WPPL Headquarters. Several factors contribute to the overall vulnerability of the system:

The five desktops likely run on outdated versions of Linux or the Kylin OS, increasing their susceptibility to known vulnerabilities. This leads to a compromise of data at rest within the workstations themselves. These workstations employ only standard login passwords without the additional protection provided by multi-factor authentication (MFA). Basic antivirus solutions, if present at all, may not provide adequate defense against sophisticated threats.

The server, although protected by physical security measures (housed in a locked cabinet within a locked building), runs on a potentially outdated OS (Kylin), may not have up-to-date security patches, and the data itself is unencrypted. This combination makes it a soft target for exploits and data exfiltration.

The use of an unencrypted microwave link poses significant security risks. Since the transmission is not encrypted, any data sent from the ranger station to the relay point is susceptible to eavesdropping, interception, and unauthorized access. This means that sensitive data, potentially including exact sensor readings, timestamps, and location details, can be captured by adversaries with relatively simple and inexpensive equipment.

Without encryption, intercepted data can be read in plain text. This vulnerability not only jeopardizes the confidentiality of the sensitive information but also enables potential attackers to perform detailed traffic analysis. Adversaries can correlate intercepted data with other leaked information (such as geolocation from image metadata), enhancing their ability to deduce patterns, schedules, or even the precise locations of both the sensors and the wildlife being monitored.

The unencrypted nature of the microwave link makes it a prime target for man-in-the-middle attacks. Attackers could potentially alter or inject malicious data during transmission without detection. Such an attack might allow them to manipulate the data, cause false readings, or even disrupt the reliability of the environmental monitoring critical for anti-poaching activities.

In addition to data interception, unencrypted microwave communications are often vulnerable to jamming attacks. An adversary could disrupt the microwave signal, leading to delays or complete losses in data transmission. This could negatively impact real-time monitoring or delay detection of poaching events, thereby compromising the Rangers' ability to respond promptly.

Solution

We recommend updating the endpoints, the server, and the data transmission link as this is crucial for strengthening the overall security posture of the network. For endpoints, modernizing the devices is a priority. This involves upgrading outdated operating systems to current, supported versions that receive regular security patches. In addition, it is important to implement stronger authentication measures such as multifactor authentication and deploy advanced endpoint detection and response solutions to help protect against evolving threats. Regular vulnerability scanning and timely software updates will help ensure that the endpoints remain resilient against known and emerging exploits.

The server also requires a comprehensive update and hardening process. Running on an older version of Kylin OS introduces risks, so migrating to a more current and supported operating system or ensuring that the existing operating system is thoroughly patched and hardened is essential. Beyond simply updating the server software, establishing stringent access controls, enforcing the principle of least privilege, and maintaining detailed system logging will help strengthen its defenses against unauthorized access and potential compromises.

For data transmission, securing the microwave link is paramount. Given that the current transmission is unencrypted and vulnerable to interception and tampering, it is necessary to implement robust encryption protocols. Using solutions such as a virtual private network or

IPSec to create a secure tunnel for the data, or applying TLS at the application level, will help protect sensitive information in transit. Complementary measures such as rigorous key management practices, for example, regular key rotation and secure storage, will further reinforce the security of the transmission channel.

Implementation and Mitigation

To help secure the network, we need to focus on three main areas: improving the security computers used by the team (endpoints), strengthening the central server, and protecting the information sent over the network.

To address the vulnerabilities in the network, we propose a multi-layered mitigation strategy that focuses on updating endpoints, hardening the central server, and securing data transmission. For endpoints such as desktops and laptops, we recommend updating to the latest supported operating systems that receive regular security patches. This update will not only fix known vulnerabilities but also improve overall performance. In addition, implementing multi-factor authentication (MFA) will add an extra level of security by requiring a second form of verification when logging in. Advanced antivirus software and endpoint detection systems will be installed to monitor and respond to threats. Regular vulnerability assessments and patch management ensure that any newly discovered issues are quickly addressed.

For the central server, which is currently running an older version of the operating system, the strategy includes either upgrading to a more modern and actively supported platform or ensuring that the current system is fully patched and hardened. Restricting access to the server by enforcing strict user permissions and using strong authentication methods will minimize the chance of unauthorized access. Detailed logging and continuous monitoring will help detect any abnormal activity, allowing for swift action if a security breach occurs.

On the data transmission side, the unencrypted microwave link represents a significant risk since the transmitted information could be intercepted. To protect this data, we recommend encrypting the transmission using a VPN (Virtual Private Network) or an IPSec tunnel, which creates a secure, private connection between the ranger station and the relay point. This encryption method acts as a digital "lock" on the data, ensuring that even if someone intercepts it, the information remains secure and unreadable. Additionally, employing Transport Layer Security (TLS) at the application level further safeguards the data as it moves through the network. Effective key management practices, such as regular key rotation and secure storage, are also vital to ensure that the encryption remains robust over time.

Conclusion

Despite previous attempts to secure the Jìnlìe Xióngmāo Bǎohùqū Forest Preserve, poachers have continued to exploit subtle but critical gaps in the preserve's tracking infrastructure. Through passive surveillance methods, similar to those seen in other conservation contexts like South Africa's rhino reserves, adversaries have leveraged unencrypted transmissions, predictable sensor behavior, metadata leakage, and unsecured image uploads to accurately locate pandas without needing to breach the system directly.

Our analysis revealed that technical vulnerabilities, such as unencrypted RF signals, static RFID identifiers, and a lack of 2FA, intersect with operational weaknesses like unsecured servers, insider threats, and a lack of Ranger cybersecurity training. These combined issues create a system that unintentionally reveals sensitive behavioral data, even when the messages themselves appear secure.

To address this, we proposed a layered defense strategy grounded in real-world feasibility. From inline encryption modules on all 4,000 sensors to transmission obfuscation, image metadata scrubbing, access control enhancements, and endpoint hardening, each recommendation was designed to be compatible with the preserve's existing hardware, budget constraints, and ranger capabilities. Importantly, every solution supports phased implementation and low-maintenance upkeep in remote, rugged terrain.

The WPPL's mission to protect endangered species cannot rely on partial fixes. It demands an approach that defends not only the data itself, but also how that data behaves, moves, and is accessed. Our proposed solutions transform the preserve from a system vulnerable to traffic analysis into a resilient, context-aware defense platform, one that finally lives up to its purpose: protecting pandas.

References

About smart cards : Frequently asked questions. Secure Technology Alliance. (2018, May 4). https://www.securetechalliance.org/smart-cards-faq/

Juels, A. (2006). *RFID security and privacy: A research survey*. IEEE Journal on Selected Areas in Communications, 24(2), 381–394. https://doi.org/10.1109/JSAC.2005.861395. (n.d.).

KJK Trail Camera, Motion Activated 120° Wide-Angle Waterproof [Trail camera product listing]. Amazon. https://www.amazon.com/dp/B0CB3Y1C5J

OpenAI. (2025, April). *ChatGPT-generated illustration of a plug-and-play encryption module for field sensors*. Created using ChatGPT image generation tools.

Poacher Problem Assistance. (2025, April). *ChatGPT-based conversation with simulated ranger responses*. Personal communication.

STM32L031K6T6. *STM32L0 series ultra-low-power MCUs.* STMicroelectronics. https://www.st.com/en/microcontrollers-microprocessors/stm32l0-series.html