Protecting Pandas Project

CYBR-504 Final Group Presentation

Group 3

PRESENTATION

Jacob Napierskie - Kayvon Karimi - RC Wright - Michael Yap

01. INTRODUCTION

The World Panda Protection League (WPPL) is facing growing threats from poachers

Pandas are being tracked and harmed in the Jìnlìe Xióngmāo Bǎohùqū Forest Preserve.

WPPL uses RFID collars and environmental sensors to monitor pandas.

Despite efforts, poachers are still getting through. WPPL suspects:

- Intercept tracking signals
- Manipulate sensor data
- Exploit insider leakes to bypass security measures

Details of the Current Situation

Tracking System Overview

- WPPL uses RFID tags + 4,000 Zigbee-style sensors to track pandas.
- Sensors detect tags within short range, sending 32-byte messages to a central server.
- Rangers use a mesh network and limited on-site tools to monitor movement.

Ongoing Issues

- Pandas still go missing or are found harmed, despite safeguards.
- Two past consulting teams failed to stop the breaches.
- Critical vulnerabilities remain unresolved.

Evidence from the Field

- Poachers found with radios, computers, cryptography books, and encrypted drives.
- No signs of physical sensor tampering or station hacking.

TIF Works

Details of the Current Situation

Ranger Station Weaknesses

- 25 staff members, high part-time turnover
- Data stored on a local server (Kylin OS) with basic username/password
- No encryption on sensor data; no multi factor authentication

Sensor + Tag Limitations

- Passive RFID tags, detected only at short range.
- Messages unencrypted: timestamp, IDs, conditions.
- Sensors can’t be remotely reprogrammed.

Constraints

- Sensor hardware can’t be modified — only add-on modules allowed.
- Must ensure backward compatibility.

Budget: $100K preferred, $267K max.

Identifying the Problem

RFID Signal Vulnerabilities

- Tags operate on 433 MHz and emit detectable signals
- RF scanners can triangulate tag location
- No tampering needed - poachers can passively track pandas

Insider and Staff Related Risk

- Rangers are minimally trained, mostly part-time, with high turnover
- High potential for accidental leaks or insider collaboration with poachers
- Lack of operational security awareness or formal protocol

Passive System Exposure

- System appears uncompromised but leaks valuable info
- Even encrypted systems may reveal patterns through metadata
- Lack of signal discipline enables adversary inference

Additional System Weaknesses

Infrastructure and Encryption Gaps

- No two-factor authentication at ranger stations; weak internet security
- Data stored unencrypted at the ranger station
- Preserve Q: only encrypted IDs — timestamps exposed movement
- Preserve F: strong encryption, but still breached — shows encryption alone is not enough

Sensor Design Limitation

- Devices can’t be updated remotely
- Transmissions always include static fields (timestamp, panda ID, sensor ID)
- Consistent metadata creates a pattern that enables tracking over time

TIF Works

Proposed Solution

Encrypting Sensor Transmissions with STM32 Modules

Problem:

- Field sensors broadcast unencrypted over 433 MHz RF mesh
- Exposes panda location & sensor data to SDR-based eavesdropping

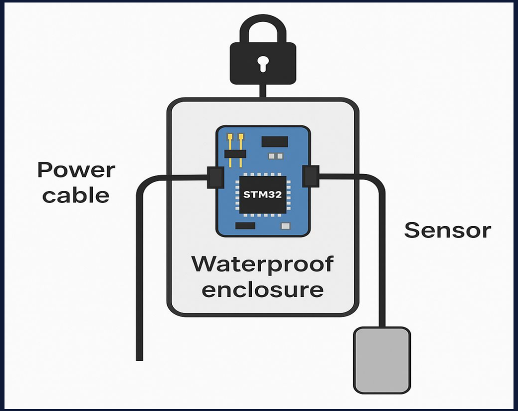
Recommendation:

- Inline encryption module between each sensor and RF transmitter
- Encrypts full payload: panda ID, sensor ID, timestamp, environmental data
- Prevents both content and behavioral inferences

Solution - Inline Encryption Using STM32 Microcontrollers:

- Deploy STM32 microcontrollers on all 4,000 sensors
- Supports AES-CCM / ChaCha20-Poly1305 for confidentiality and integrity
- Hardware-accelerated, low-power, field-ready
- Cost: ~$2.60/module (total: ~$10.4k)

Proposed Solution



Encrypting Sensor Transmissions with STM32 Modules

Implementation and Mitigation:

- Preassembled STM32L031K6T6 modules with built-in AES encryption
- Housed in IP65 waterproof enclosures with labeled quick-connect plugs
- Installs in <15 mins—no config or tech skills required
- Mounted with Velcro, zip ties, or adhesive; strain relief via cable glands
- Phased rollout by patrol zones; 25 teams = full deployment in weeks
- GPS-logged installs with verification tags
- Encrypts all outbound data, blocking surveillance
- Future updates to obscure timing for traffic analysis resistance

TIF Works

Proposed Solution

Sensor Upload Frequency

Problem:

- Encrypted messages still leak when events happen (panda sighting or low battery).
- Poachers with SDRs can analyze timing patterns to infer animal movement.
- Rangers confirmed that real-time data isn’t necessary—daily updates are sufficient.

Recommendation:

- Eliminate real-time transmissions and reduce predictability.
- Shift to scheduled, encrypted uploads once per day.
- Obscure timing using padding, decoys, and randomized behavior.

Solution 1 - Random Upload Timing with Padded and Dummy Messages:

- Upload real sensor data at a random time each day.
- Inject dummy encrypted messages throughout the day.
- Uniform message size hides real vs fake data.
- Strong protection, minimal battery impact, adds scheduling complexity.

TIF Works

Proposed Solution

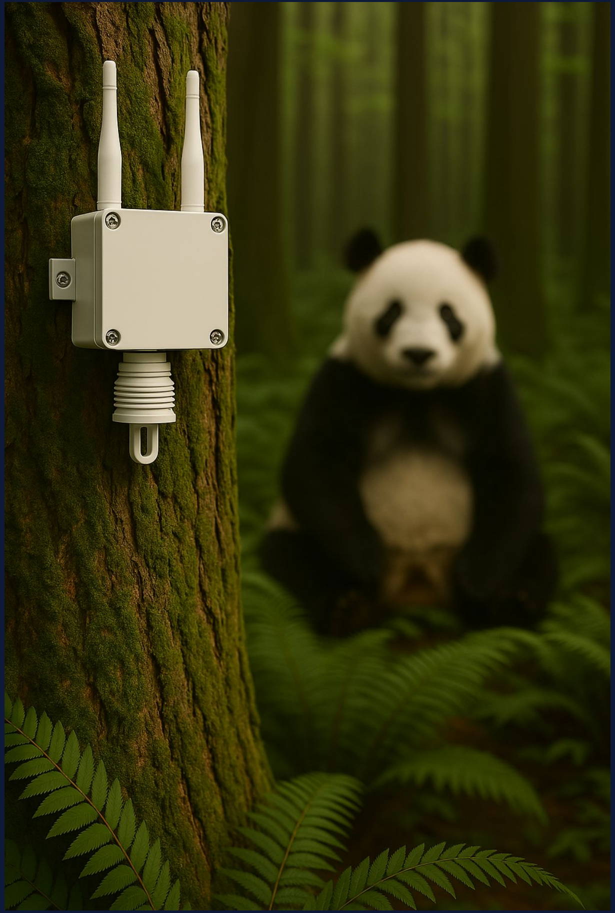
Sensor Upload Frequency

Solution 2 - Fix Upload Schedule with Padding and Guaranteed Transmission

- Transmit once daily at a set time, no matter if data exists.
- All messages encrypted, padded to identical size.
- Simpler for rangers, predictable over time unless paired with decoys.

Implementation and Mitigation:

- Both approaches block poacher traffic analysis via timing obfuscation.
- Inline modules handle logic + encryption; no changes to sensors required.
- Aligns with ranger workflows and deployment capacity.
- Pilot small-scale test to validate battery life, reliability, and usability.
- Modular strategy enables scalable deployment without overwhelming staff.



TIF Works

Proposed Solution

Insider Risk

Problem:

- High ranger turnover limits accountability and raises leak risk
- No 2FA or encryption on local systems
- USB ports allow untracked data transfers
- No cameras, access logs, or file monitoring

Recommendations:

- Enforce 2FA on Kylin OS using FreeOTP or privacyIDEA
- Apply role-based access controls and rotate credentials monthly
- Add trail cameras and keypad/RFID cabinet locks
- Use auditd, Wazuh, or OSSEC for system activity monitoring

Implementation and Mitigation:

- Configure 2FA, credential rotation, and USB restrictions
- Deploy audit tools for logins, files, and removable media
- Install surveillance at server cabinets and entry points
- Train rangers on data risks and insider threat prevention

Panda Picture Uploads to WPPL

Problem:

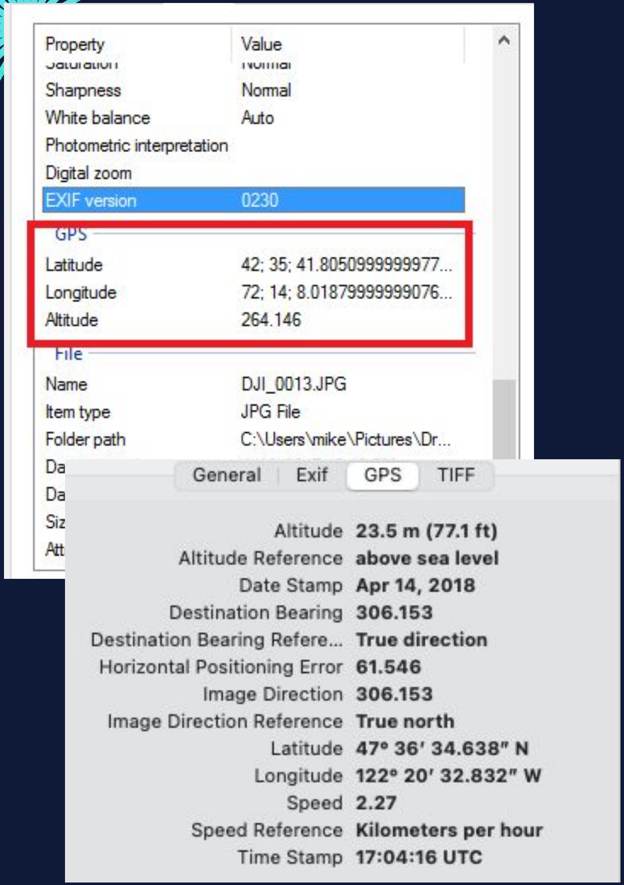
- Photos of pandas sent to the WPPL likely include EXIF data, such as geolocation, date, altitude, image direction - which can inadvertently reveal the animals’ whereabouts.
- Poachers are likely intercepting this data via the unsecure microwave relay system or by the EXIF data from the photos uploaded to the WPPL public website

Recommendations:

- Disable geotagging on all cameras and devices used for capturing panda images
- Ensure that all images have their EXIF metadata removed before uploading to the website

Implementation and Mitigation:

- Implement a workflow to strip metadata from images immediately upon upload, blur or obfuscate background of images.



Property	Value
Saturation	Normal
Sharpness	Normal
White balance	Auto
Photometric interpretation	
Digital zoom	
EXIF version	0230
GPS	
Latitude	42; 35; 41.8050999999977...
Longitude	72; 14; 8.01879999999076...
Altitude	264.146
File	
Name	DJI_0013.JPG
Item type	JPG File
Folder path	C:\Users\mike\Pictures\Dr...
Da	
Da	
Siz	
Att	

Altitude	23.5 m (77.1 ft)
Altitude Reference	above sea level
Date Stamp	Apr 14, 2018
Destination Bearing	306.153
Destination Bearing Refere...	True direction
Horizontal Positioning Error	61.546
Image Direction	306.153
Image Direction Reference	True north
Latitude	47° 36′ 34.638″ N
Longitude	122° 20′ 32.832″ W
Speed	2.27
Speed Reference	Kilometers per hour
Time Stamp	17:04:16 UTC

TIF Works

Operational Network Vulnerabilities

Problem:

- Workstations and server are running outdated operating systems with weak authentication and security measures, leaving them vulnerable to exploits and unauthorized access.
- Data transmitted via an unencrypted microwave link is susceptible to interception, potentially exposing sensitive information.

Recommendations:

- Modernize endpoints and harden server by upgrading to supported operating systems, implementing multi-factor authentication, and deploying advanced endpoint detection and response solutions.
- Secure data transmission by encrypting microwave link.

Implementation and Mitigation:

- Implement encryption protocols to create a secure tunnel for data transmission
- Establish process for updating endpoints and server, enforce strict access controls, and maintain comprehensive logging.

TIF Works

14. CONCLUSION

- Security Issues addressed:
  - Encryption of Sensor Transmission to the Base Station
  - Sensor Upload Frequency
  - Insider Risk
  - Panda Picture Uploads to WPPL
- Our approach emphasizes the system’s sensitive data - how it behaves, moves, and is accessed.
- Integration of these solutions is vital for the system to protect data in the hands of poachers.