In this project, my team specified and designed cryptographic services to protect a sensor network.

My individual tasks were: proposing the solution including any diagrams needed to clearly convey the solution, explaining what cryptographic methods/algorithms we used, explaining why they were chosen, and describing these sufficiently so that the customer can understand why they were selected.

The Situation: Design a sensor network that relays panda locations in a very large forest preserve in China. There are several hundred sensors deployed that can detect the location of nearby pandas. When a panda is detected, the sensor relays the location information across the sensor network to a collection server at the edge of the forest. The panda information is stored here for real-time tracking and behavioral analysis. Additionally, design the network to defend from cryptographically-savvy hunters who are exploiting the network by intercepting and reading panda location messages. Hunters may also physically access the internal storage of the sensors but cannot modify them.

Sensor design needs: solar powered, limited battery, resource constrained, low power with limited transmission capability and can only transmit to nearby sensors. The transmission uses much more power than reception. If too few sensors are active, messages can not be relayed through to the collection server. The sensor network must run unattended for long periods of time. If possible, add an ARM-based software module to the sensor between the sensor output and its radio transceiver.

CYBR-504 Applied Cryptography

Final Project 7.1 Designing Cryptographic Services

Shiley-Marcos School of Engineering (SMSE), University of San Diego

17th April 2023

The protection of endangered species worldwide is a critical concern. Hunters illegally tracking and killing pandas is a growing threat, and it is becoming necessary to monitor and safeguard the pandas. One such way to accomplish this is a network of sensors that can track RFID tags attached to the pandas. However, as protections evolve so do threats. The hunters are becoming more savvy as they study cryptography and learn how to hack the sensor network. In this paper, we define a new solution for the sensor network and RFID tags that would thwart attempts from the hunters to break into the network. We discuss the vulnerabilities and propose a comprehensive security solution, including a new lightweight cryptography algorithm and a new type of RFID tag.

Hunters present a wide variety of threats to the pandas. The hunters can intercept messages sent between sensors and the collection server, allowing them to determine the location of pandas. This can be addressed by encrypting the messages, so that even if they are intercepted, they cannot be read by the hunters. The hunters can record and replay messages sent between sensors, which can allow them to cause confusion and potentially misdirect efforts to find pandas. This can be addressed by including a time stamp or other mechanism in the messages to prevent replay attacks. The hunters may be able to modify messages in transit, potentially changing the location of pandas or introducing false information. This can be addressed by using message authentication codes (MACs), digital signatures, or authenticated encryption such as the one employed by ASCON-128 to verify the authenticity and integrity of messages. The hunters may be able to gain physical access to sensors and potentially access their internal storage. This can be addressed by encrypting data stored on the sensors and using secure boot mechanisms to prevent unauthorized modifications to the sensor software. Additionally, using hardware security modules (HSMs) or secure enclaves can help protect cryptographic keys and other sensitive data.

We analyzed how the hunters were able to exploit the encrypted network to find the pandas. While specific details pertaining to the hunter's successful exploitation of the other forests sensor network are limited, we believe that the items found by the rangers at the hunter camp assist in providing ideas as to how the hunters were able to obtain GPS coordinates for the pandas even though the sensor network communications were encrypted. Although we can't be entirely certain, it is safe to assume that the network of panda hunters across the various forests are communicating with one another, therefore, we believe that the hunter groups were sharing information on the most effective ways to track and capture the pandas.

At the hunter camp the rangers found radio equipment, a notebook computer, and books on cryptography. We believe that the hunters used an RFID tracking device, from a previously captured panda, in conjunction with a known RFID sensor. By doing so, the hunters created a makeshift controlled testing environment where they could control when the RFID tracking device activated the sensor. They then utilized the notebook computer to intercept network traffic and capture the encrypted RFID traffic. The hunters educated themselves on the various encryption algorithms and the most effective methods to decrypt them and pull the GPS coordinates from the traffic. Once they were able to successfully capture and decrypt traffic from the RFID tracker they were in possession of they began putting their "training" to work. We believe they used the radio equipment to monitor the sensor network for traffic from the various panda RFID trackers. This allowed them to capture traffic from various RFID trackers in real-time and decrypt GPS coordinates in real-time.

By using the ASCON family of encryption and hashing algorithms we can ensure that there are secure data communication sessions between the RFID tags and the sensors because secret keys that are only known to the tags and the sensors are being utilized. The technology that separates our solution apart from the failed attempt to protect the pandas in the other forest is that the ASCON family of ciphers incorporates a randomly generated nonce with the secret key and then creates the encryption key for each data exchange between the tag and the sensor. By doing so, even if the GPS coordinates of the panda being broadcasted across the sensor network are exactly the same, the nonce ensures that each encrypted message is different. This directly protects against any form of replay attacks.

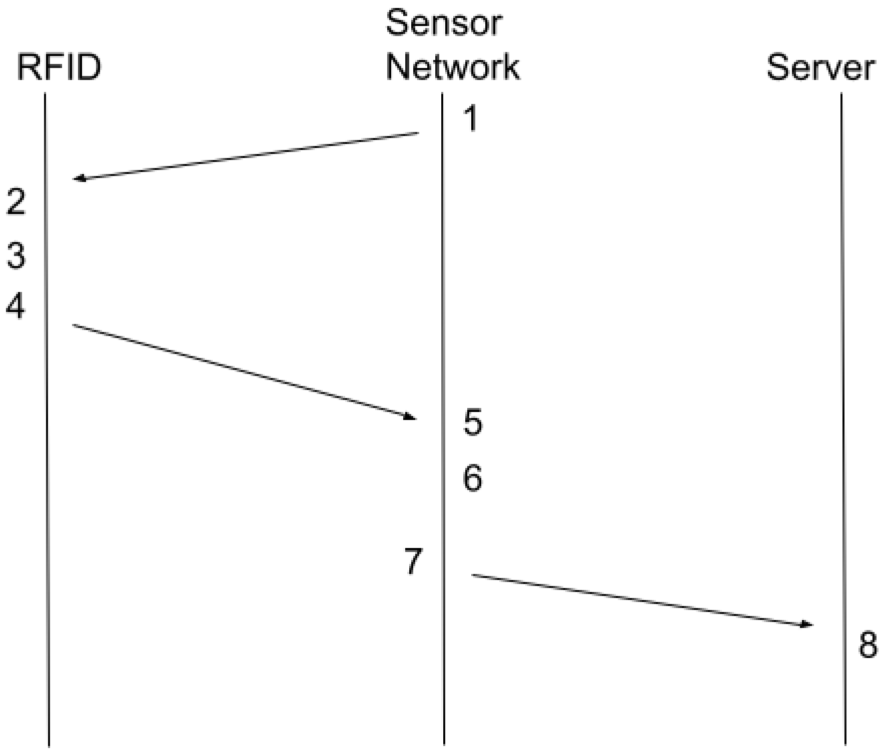
Our solution consists of a photovoltaics (PV) powered, ultra high frequency (UHF) radio frequency identification (RFID) tag that communicates with a distributed mesh PV sensor network. It employs an ASCON-128 lightweight cryptography (LWC) cryptographic engine to secure communications. The read range of our PV-RFID tag is eight times greater than that of passive RFID tags (Kantateddy 2019) allowing us to maximize our ability to detect pandas while preserving the tag's shelf life of 10-15 years.

ASCON-128 is a family of authenticated encryption and hashing algorithms that has comparable performance measures to AES with a smaller memory footprint, while still being robust and secure. The smaller footprint makes it ideal for Internet of Things (IoT) devices like RFID tags. NIST named ASCON as its new standard for lightweight cryptography in February 2023. The ASCON family provides 128-bit security as a nonce-based authenticated encryption algorithm that protects the confidentiality of the plaintext and the integrity of the ciphertext.

ASCON was designed with robust security which protects from a variety of attacks, including key recovery attacks and trivial forgeries.

ASCON uses a single lightweight permutation for each 64-bit block, which is divided in 5 words (x0 - x4). The permutation iteratively applies to blocks: 1) XORs a 1-byte constant to x2, 2) nonlinear substitution layer with a 5-bit S-box applied 64 times vertically across words, and 3) a linear diffusion layer that XORs different rotated horizontal copies of each word. The state is initialized with a key and nonce and is run through 12 rounds of a stronger permutation. Each plaintext block is run through six rounds of the core permutation. Finalization injects the key again, runs through 12 rounds of the same stronger permutation used in initialization, and produces the tag for authentication. The strengthened keyed initialization and finalization protects against misuse attacks, such as nonce-reuse attacks.

Power consumption is a major consideration in the development of passive RFID tags. ASCON requires anywhere from 2500 to 10000 gates to run. We designed these tags so that they only require a minimal area of around 2500 gates (2.5kGE). ASCON-x-low-area design mode is utilized for RFID tags requiring 2.57kGE. ASCON64 is the design mode that will be utilized on the sensors capitalizing on the installed 64 bit ARM modules requiring 5.86kGE. Processing power is 14 and 72 Mbps respectively.



1. Sensor broadcasts query signal.
2. RFID receives query and uses energy to power up circuits.
3. RFID encrypts panda ID number and its associated data.
4. RFID returns encrypted panda ID number and data to the sensor.
5. Sensor receives panda ID number and data*.
6. Sensor authenticates panda ID tag and encrypts information.
7. Sensor transmits the data over the sensor network to the server.
8. Server authenticates tag and decrypts data.

*Within the mesh network of sensors, each sensor can communicate with other sensors and with the central server. This allows for data to travel among multiple paths and offers redundancy and reliability.

Our solution aims to address current challenges and mitigate future ones to the best of our ability. We are tasked with protecting data in transit, RFID tag and sensor transmissions, as well as data at rest residing on the sensors. The main challenges reside in selection of the correct hardware and algorithm that will work together which is why we are confident with our choice of Ascon-128 and the 64 bit ARM modules. There is a limitation on processing power due to the small size of the RFID tags and sensors which is mitigated by installing a 64 bit ARM module in the sensor which assists in processing power and utilizes the Ascon 64 bit mode while the RFID tags are utilizing the Ascon-x-low-area mode.

Ascon-128 provides strong authentication and encryption in both Ascon 64 bit and Ascon-x-low-area modes. Attackers have the ability to sniff transmissions and decipher encrypted communications so robust encryption is necessary with an added element of randomness. Implementing Ascon-128 will mean that the private key is stored on the RFID tags and sensors which could lead to compromise by the attackers. However, with Ascon-128, even if the private key is uncovered, communications cannot be deciphered without the randomly generated nonce value.

Our ARM module is the ARM Cortex-A7 processor with an embedded Hardware Security Module (HSM). This module will work well with Ascon-128 providing adequate processing power at low energy consumption with the added benefit of the HSM to protect the hardware serving as an additional layer of security since the sensors could possibly be tampered with. The internal storage on the sensors is additionally secured with AES encryption, which will provide protection to the internal storage and will require authentication.

Future challenges will be seen in key management, RFID tag management, and sensor maintenance. Key management will be very important and the private key should be rotated every 15 days which will further mitigate any usefulness found in recovering the private key. Fortunately it is an easy process for key rotation with Ascon-128 providing the ability to generate a secure random key. If an RFID tag stops working it will be difficult to find the tag for servicing. A protocol should be put into place to handle such situations. The sensors and RFID tags have a fairly long service life; however, a plan should be put into place to begin rotating sensors and RFID tags out with new ones to avoid a scenario where all 250+ sensors need to be replaced at the same time. It is also recommended that the sensors be periodically checked for tampering and a response plan be drafted to handle possible compromise if evidence of tampering is suspected.

In conclusion, protection of pandas requires robust security measures to ensure the integrity and confidentiality of the network, especially data in transit and at rest. Our proposed solution combines ASCON-128 lightweight cryptographic engine, photo-voltaic RFID tags, and secure data storage mechanisms to ensure a comprehensive approach to safeguarding the pandas. By addressing vulnerabilities, such as replay attacks, message tampering, and unauthorized access to sensors, we significantly strengthen the network and the protection it offers the pandas.

References

ARM Processor With Independent Hardware Security Module Protects CAN Bus Networks From Cyber Threats. (n.d.). Copperhill. Retrieved April 15, 2023, from https://copperhilltech.com/blog/arm-processor-with-independent-hardware-security-module-protects-can-bus-networks-from-cyber-threats/

Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, U.S. Department of Commerce. (n.d.). *Lightweight Cryptography | CSRC | CSRC*. Retrieved April 3, 2023, from https://csrc.nist.gov/projects/lightweight-cryptography

Distribution, A. C. &. (2017b, March 27). *Understanding RFID and RFID Operating Ranges*. Retrieved April 10, 2023, from https://blog.acdist.com/understanding-rfid-and-rfid-operating-ranges#:~:text=Far%2Drange%20UHF%20RFID%20tags,of%20100%20meters%20or%20more.

Dobraunig, C., Eichlseder, M., Mendel, F., & Schläffer, M. (n.d.). *Ascon – Authenticated Encryption and Hashing*. Retrieved April 3, 2023, from https://ascon.iaik.tugraz.at/

Dobraunig, C., Eichlseder, M., Mendel, F., & Schläffer, M. (2021). Ascon v1.2 Submission to NIST. In *https://csrc.nist.gov/*. Retrieved April 5, 2023, from https://csrc.nist.gov/CSRC/media/Projects/lightweight-cryptography/documents/finalist-round/updated-spec-doc/ascon-spec-final.pdf

Groß, H., Wenger, E., Dobraunig, C. and Ehrenhöfer, C. (2015) Suit up! -- Made-to-Measure Hardware Implementations of ASCON. *2015 Euromicro Conference on Digital System Design*, Madeira, Portugal, pp. 645-652. Retrieved April 10, 2023, from https://ieeexplore.ieee.org/document/7302339

Lara-Niño, C.A., Morales-Sandoval, M., & Díaz-Pérez, A. (2016) An evaluation of AES and present ciphers for lightweight cryptography on smartphones. *2016 International Conference on Electronics, Communications and Computers (CONIELECOMP)*, Cholula, Mexico, 2016, pp. 87-93. Retrieved April 5, 2023, from https://ieeexplore.ieee.org/document/7438557

McKay, K., Bassham, L., Turan, M., & Mouha, N. (2017). Report on Lightweight Cryptography. In *https://nvlpubs.nist.gov/* (NISTIR 8114). National Institute of Standards and Technology. Retrieved April 3, 2023, from https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8114.pdf

NIST Selects 'Lightweight Cryptography' Algorithms to Protect Small Devices | NIST. (2023). *NIST*. Retrieved April 5, 2023, from https://www.nist.gov/news-events/news/2023/02/nist-selects-lightweight-cryptography-algorithms-protect-small-devices

Szondy, D. (2019, September 30). MIT developing light-powered RFID tags for the internet of things. *New Atlas*. Retrieved April 10, 2023, from https://newatlas.com/technology/mit-light-powered-rfid-tags-internet-of-things/

Thakor, V.A., Razzaque, M.A., and Khandaker, M. R. A. (2021). Lightweight Cryptography Algorithms for Resource-Constrained IoT Devices: A Review, Comparison and Research Opportunities. In IEEE Access, vol. 9, pp. 28177-28193. Retrieved April 5, 2023, from https://ieeexplore-ieee-org.sandiego.idm.oclc.org/document/9328432

Appendix 1 - Questions

How long do we have to complete the project?

Your solution, if approved, would be expected to be able to be implemented within 12 months of approval.

What stakeholders/departments need to be involved?

You will be working only with the WPPL rangers associated with a single preserve in southwest China.

What amount of sensors do we have to install?

Your solution is not required to install new sensors, but if your solution involved the sensors, there are about 250 in service.

Will it be a phased approach where we will evaluate or install all in this one project?

If your proposal was approved, you would implement it in a restricted location and provide a proof-of-concept evaluation, and if successful, deploy it throughout the forest in stages.

Are there certain sensors that need to be installed before other sensors?

No.

Is this a capital investment? Will there be operational funds available after deployment?

The intent is to not replace the sensors but to improve the code running on them. Hopefully, after deployment, there will be very little admin/maintenance cost above what they already provide.

In either case, what is the project budget?

If your solution would be approved, the target budget for implementation is $275,000, but they would prefer to stay under that if possible.

What is the lifespan of these sensors, if they weren't subjected to forces of nature?

Even with nature, the sensors in the field are designed to last at least 10-15 years.

What do we absolutely need in our security solution?

You need to provide a detailed and well-argued proposal as to how your solution would protect the pandas by securing the sensor network from hunters seeking to exploit it. Include specific algorithms, protocols, and other implementation details you feel would convince the WPPL rangers of your solution. State any specific problems you feel need to be addressed, your method to do so, and why. You should include and justify changes to the software on the server or sensors, and if needed, the add-on modules. If the rangers believe that your solution will work, they would then fund actual implementation and testing.

Has there ever been a security breach at the facility to date?

No. The rangers have never had a cyber or physical breach of the ranger station.

Are there any cyber standards we need to adhere to?

No, 'standards'; per se. You would not need to comply with NIST, ISO 27001 for GDPR, etc., but there may be other regulations you may need to consider.

Who will admin the sensors once implementation is complete? Will training need to be provided?

The rangers will provide any maintenance and administration of the sensor network and associated servers. They will need whatever training is appropriate.

Is there a Disaster recovery plan? Is there a business continuity plan?

The rangers' server is automatically backed up to 2 servers, one on-site, and the other off-site. Their recovery plans are simple but focus on continuing to collect panda data and not losing what has been collected.

Is there currently any two-factor authorization at the site that we can leverage?

The rangers do currently use two-factor authentication to access the server that collects the panda data.

Do we know what algorithm was already used?

The system you are working on is currently not using encryption. You don't know the other group's specific encryption method, but you do know that it used cryptographically strong/secure algorithms to encrypt communications.

Do the Pandas have chips/tagged in them so the sensors know it's a panda and not a hunter?

The pandas have tracking devices on them that the sensors can detect. The sensors do not detect the hunters.

Are the solutions only supposed to come from course material or do we do further research for other solutions?

There is sufficient material in the course material to come up with reasonable solutions. The only thing 'external' would be some reasoning
skills, but you are free to use outside material if you wish; just be sure to reference anything you directly reference.