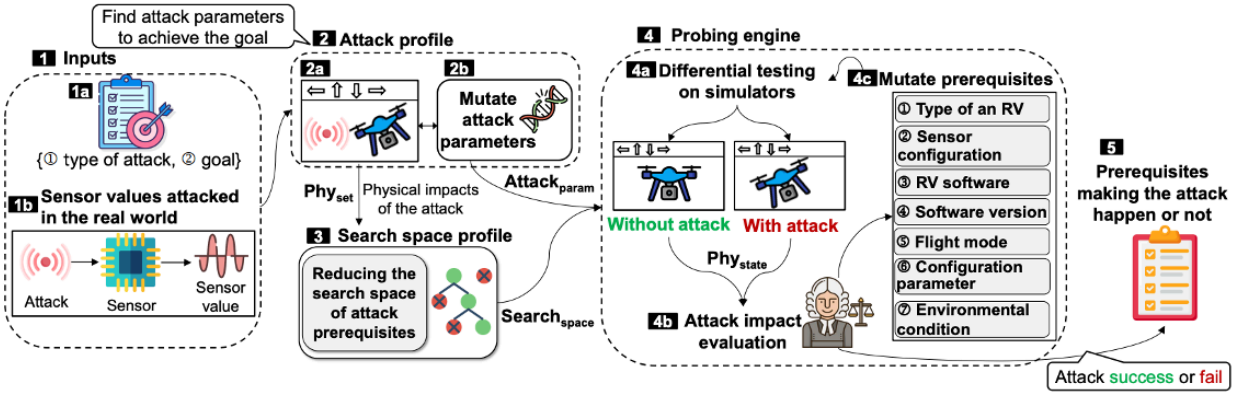
Theme: Evaluating Sensor Security in Robotic Vehicles
Names: Kevin Prabhu, Aayush Pandey

The increasing trend of autonomous systems has shifted the focus onto sensor security in robotic vehicles. Critical operations such as navigation and collision avoidance rely on accurate sensor data. However, there is a challenge to this reliability due to physical sensor attacks: hence, operational safety and mission success come into question. This research addresses "attack hardness", a systematic measure of how hard it is to exploit RV sensors under varied configurations.

The RVPROBER framework was designed to identify the pre-conditions for an attack, pointing out vulnerabilities in 57.08% of real-world RV configurations analyzed. Despite such unprecedented advances, misconceptions abound among developers. The idea of sensor redundancy may be thought by many to prove very effective against sensor attacks, and again, this research proves the opposite. It shows how the interference could be effective if a few prerequisite conditions were satisfied and the signals reached even the redundant systems. Spoofed GPS beats the legitimate ones in forcing disrupting navigation. The address required proactive defensive strategy coupled with enhancement over failsafe logic improvement on sensor data validation by using intrusion mechanisms that would be advanced, especially for RVs only.



While RVPROBER advanced the state of the art, increasing the number of detected vulnerabilities from 6 to 11, limitations remain: most of the research focused only on some kinds of RVs, simulations cannot emulate the complexity of the real world, and not all categories of sensors were studied. This work can be significantly improved in terms of enhancing the applicability of the findings by considering diverse configurations of RVs, real-world testing, and sensor types such as thermal or radar sensors.

Future work should also take up scalability through the development of lightweight and cheap security measures that can easily embed in the existing RVs. Further work on enhancing RVPROBER's capability for finding vulnerabilities in emerging technologies will further strengthen sensor security, hence safer autonomous operations.

References:
[1] Hyungsub Kim et al., "A Systematic Study of Physical Sensor Attack Hardness," 2024.J. Zhang et al., "Protect Sensitive Information against Channel State Information Based Attacks," 2017.
[2] X. Chen and S. Sankaranarayanan, “Reachability Analysis for CyberPhysical Systems: Are We There Yet?” in Proceedings of the NASA Formal Methods Symposium, 2022.

Theme: Solutions to Security and Privacy Issues in Mobile Social Networking CSE 707
Names: Jackey Wang, Nawar Khouri

During our presentation we talked about the solutions to security and privacy issues in mobile social networking. The paper was written in 2009, but the privacy issues discussed in that paper are even more relevant today. Social media has become more and more popular and with that user's privacy and security only become more and more important. The paper focused on location-area mobile social network systems (LAMSN). These apps rely on people's personal data such as location, relationships, and preferences to function. The paper focuses on WhozThat and Serendipity, which relies on users to be physically close to each other. The primary concerns with these two are direct anonymity issues, indirect/k-anonymity issues, eavesdropping, spoofing, reply, and wormhole.

While the discussed social networks don't exist today, modern social media have elements of LAMSN such as Snapchat's Snap Map, showing the user's location and what Snaps they've sent while in that location. The privacy and security concerns such as Direct anonymity, indirect anonymity, etc are still relevant in the field of cybersecurity today. The main weakness of the paper is the age. As mentioned before, WhozThat and Serendipity aren't relevant today. Since social media has exploded in popularity, more issues than what was mentioned have appeared. In a 2023 paper, additional problems such as data leakage, unauthorized access, cyberstalking, phishing attacks, malware, information overload, user profiling, inadequate privacy policies, third-party apps, photo and video privacy, end-to-end encryption, insecure wi-fi connections, and data retention have been identified and are being researched Social media has become much more complex and in turn the problems that come with it have become more complex as well.

Security and privacy should be continued to be researched, however the research should be focused on the popular social media of today such as Twitter/X, Facebook, and Instagram. Attacks on social media are constantly changing. Leveraging AI could introduce adaptive security that can detect and react to threats much faster than traditional means. The paper "An Overview of Artificial Intelligence in Enhancing Security and Privacy in Mobile Social Networks goes over all the previous discussed security concerns and addresses how to use AI to detect these emerging threats and how to counter them

References:

A. Beach, M. Gartrell, and R. Han, "Solutions to security and privacy issues in mobile social networking," 2009 International Conference on Computational Science and Engineering, vol. 4, pp. 1036-1042, Aug. 2009.

Fakhouri HN, Alawadi S, Awaysheh FM, Hamad F, Alzubi S, AlAdwan MN. An Overview of using of Artificial Intelligence in Enhancing Security and Privacy in Mobile Social Networks. In2023 Eighth International Conference on Fog and Mobile Edge Computing (FMEC) 2023 Sep 18 (pp. 42-51). IEEE.

Theme: Security Vulnerabilities in Bluetooth Technology for IoT
Names: Dharshini Adimoolam, Suraj Jaganathan

In our presentations, we talked about assessing vulnerability to shoulder surfing and discussed the security vulnerabilities present in Bluetooth technology as used in IoT. We decided to discuss a bit more about Bluetooth vulnerabilities because it has problems and there are research issues that currently exist with it. We also thought about including some thoughts about making it better that can address some of the drawbacks in our work focused on the paper. Bluetooth, since it came out, has been an integral part in wireless communications, especially with IOT. Bluetooth connections primarily share sensitive information about all the parties; therefore, it is considered a significant threat to privacy and security. Bluetooth's original protocol design was made in such a way that it couldn't address some of the diverse and complex problems that are now found in most of the latest wireless applications. We think that this work could have focused on that so that it could be considered for fixing vulnerabilities stemming from the Bluetooth' initial structural design

Though all the devices now use latest versions, some of them still are operated by older versions, when older versioned devices are paired with new and secure ones, the connection is automatically degraded to lowest version in the communication. This is a concern because older devices use static PIN codes, when passcodes like PINs are static like, there are numerous password-based attacks that are compromised using brute force attacks. Versions before 2.1 continues to exist which has weak encryption which is susceptible to Man in The Middle attacks and it uses PINs for pairing. One of the main issues affecting Bluetooth security is the reliance on older pairing and encryption protocols, such as the use of static PIN codes, which are highly susceptible to brute-force attacks. Moreover, the devices before 2.1 don't have proper storage of link keys, cracking them would compromise the whole communication. There is a lack of mutual authentication before version 2.1. This could be improved by imposing a restriction on using those devices that are still in use, this could leave a lot of devices unusable, but it could improve security.

Simple Secure Pairing (SSP) resolves most of these issues but use of the older version will still lower the security of the overall connection. The other big concern is the discoverability issue, while some devices even now support turning off discoverability modes many don't, so the device is automatically visible when Bluetooth is turned on. This results in a broad spectrum of attack vectors including Bluejacking, Blue Bugging, and even automotive hacking, highlighting the critical nature of these vulnerabilities in everyday devices, including vehicles and personal gadgets. Furthermore, even now all devices just have device authentication and not user authentication while initiating connections, this could result in unauthorized access when the device is stolen or lost.

To improve all of this, it is important to make compatibility a stricter measure to maintain security standards. Firmware patches can be deployed universally. Additionally, AI based detection systems can be made use of that will be capable of identifying and mitigating attacks to provide real-time insights of Bluetooth communications security especially in IOT environments.

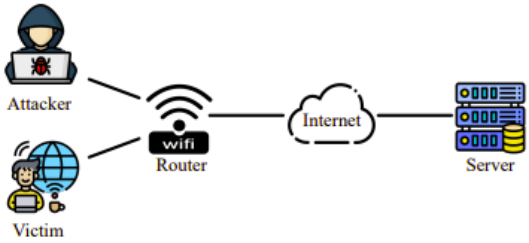
References:

Angela M. Lonzetta, Peter Cope, Joseph Campbell, Bassam J. Mohd and Thaier Hayajneh, Security Vulnerabilities in Bluetooth Technology as Used in IoT, Journal of Sensor and Actuator Networks, 2018.

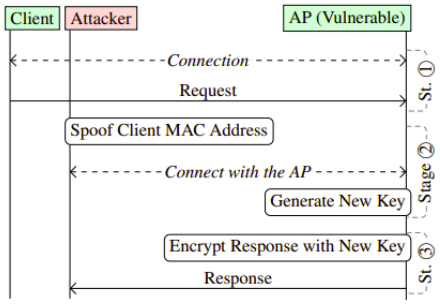
National Institute of Standards and Technology. Guide to Bluetooth Security; NIST 800-121-Rev 1; NIST: Gaithersburg, MD, USA, 2016.

Theme: Wi-Fi Network Security in NAT enabled Networks. CSE707
Names: Jack Dunfey, Joshua Wajnryb

In our presentation, we talked about a new side-channel vulnerability in NAT (Network Address Translation) enabled networks using TCP (Transmission Layer Protocol) hijacking. In this paper, the author focused on testing different types of routers from various manufactures to show attack success. In the procedure leading up to the attack, the source port number, SEQ and ACK numbers are what we look for to send malicious data back to the attacker from the victim client device. The results ranged from Wi-Fi generations 4 through 6 with WPA (Wi-Fi Protected Access) 2 and 3 enterprise/personal. Once hijacked, the attacker can perform TCP Denial-of Service, TCP hijacking and TCP Injection attacks.



This attack highlights three key security failures presented in a single router. NAT port preservation is the practice of many routers to keep the sources port of packets rather than constantly switching them. Reverse-path validation, which enables a router to detect IP-spoofing based attacks and drop forged packets from being sent. TCP window tracking is another security feature that checks the amount of data sent from a TCP connection. With one of these three features disabled, it is possible to obscure Wi-Fi signals. A more in-depth paper from 2023 shows how encrypted Wi-Fi data is manipulated over TCP between the client, attacker and the vulnerable AP (Access Point) in question.



This off-path vulnerability has the impact of compromised confidentiality, data manipulation and potential for large-scale attack vectors. Although this vulnerability is dangerous, there are immediate solutions and countermeasures for these attacks as the result primarily from router misconfiguration. A potential criticism of this research is that they only performed security tests on mostly networks that are already widely considered insecure like coffee shops and hotels. It would be interesting to see how their success metrics would change if they included security-critical networks. Furthermore, this paper assumes that networks employ no further defensive measures beyond router configurations. Some examples include Network-based Intrusion Detection Systems (NIDS) to detect anomalous traffic or static ARP tables (unrealistic for public networks). Another critique is questioning the ethics of testing network-based attacks on real-world networks. This paper did not discuss what steps they took to ensure another device wasn't unintentionally affected. Going forward, vendors must supply documentation that guides users and organizations to enable TCP detection methods for APs (such as Linksys) and improvements can be made to router antivirus software to this new TCP attack based on the data given to the affected manufactures.

References:
Yuxiang Yang, Xuewei Feng, Qi Li, Kun Sun, Ziqiang Wang, Ke Xu, "Exploiting Sequence Number Leakage: TCP Hijacking in NAT-Enabled Wi-Fi Networks", Network and Distributed System Security (NDSS) Symposium, 2024, doi: https://dx.doi.org/10.14722/ndss.2024.23419
"Framing frames: Bypassing Wi-Fi encryption by manipulating transmit queues," in 32nd USENIX Security Symposium (USENIX Security 23), 2023.
Linksys, "How to enable rogue ap detection on your linksys wireless-ac access point," https://www.linksys.com/support-article?articleNum= 135793, Accessed July 2023.

THEME: SECURITY RISKS IN CONSUMER 3D PRINTING

NAMES: ANDREW BALOTIN, RAGHAVI

3D printers are innovative tools used for creating objects by layering materials through an extruder. They are popular in industries like healthcare and aerospace, and widely used for rapid prototyping. However, their convenience often comes with security problems. This study focuses on the security weaknesses in 3D printers, specifically data exfiltration and remote manipulation.

The study identifies several security flaws in MakerBot Replicator and Replicator Mini printers, primarily due to inadequate encryption and authentication mechanisms. Key vulnerabilities include unprotected storage of design files and weak transport layer security. Attackers with network access can intercept sensitive information or manipulate printing tasks, posing significant risks to intellectual property and operational integrity. The reliance on outdated security practices worsens the issue, leaving users vulnerable to potential exploitation.

This paper mainly focuses on identifying vulnerabilities in individual consumer 3D printers. While it highlights issues like poor authentication and unencrypted traffic, it does not address how these printers interact with other devices on the network. Additionally, it doesn't provide any guidance for manufacturers to implement long-term fixes.

In contrast, the paper **"Security Analysis of Networked 3D Printers"** expands the scope by analysing how networked 3D printers are affected by their environments. It introduces a tool (C3PO) to systematically evaluate both standalone printers and their network setups. This study identifies multi-stage attack paths and points out vulnerabilities in network configurations, like printers being placed on public networks. This broader approach provides deeper insights into how these devices can be secured in real-world scenarios.

MEASURES FOR IMPROVED SAFETY

- Implement encryption and two-factor authentication for secure communication.
- Provide regular updates to fix vulnerabilities.
- Isolate printers in secure networks to limit exposure.
- Educate users on securing their devices with strong passwords and proper network setups.

By combining the findings of these studies and addressing the gaps, 3D printers can become safer and more reliable for everyone.

References

[1] Quang Do, B. Martini, and K.-K. R. Choo, "A Data Exfiltration and Remote Exploitation Attack on Consumer 3D Printers," IEEE Transactions on Information Forensics and Security, vol. 11, no. 10, pp. 2174-2186, Oct. 2016.

[2] M. McCormack, S. Chandrasekaran, G. Liu, T. Yu, S. DeVincent Wolf and V. Sekar, "Security Analysis of Networked 3D Printers," 2020 IEEE Security and Privacy Workshops (SPW), San Francisco, CA, USA, 2020, pp. 118-125, doi: 10.1109/SPW50608.2020.00035.

Group 6 : Jerry Mathew and Selwin Murzello

Theme: Security Threats and Countermeasures in IoT

IoT can be defined as a self-configuring network or system of physical devices in some virtual representation, interconnecting at any time through interoperable communication protocols. While much anticipated in transformative applications, full IoT in areas such as healthcare, smart cities, and manufacturing has equally raised new sets of concerns for data security: from critical issues like privacy vulnerabilities and authentication challenges to scalability. The increase in the number of devices easily projected to reach 41.6 billion devices by 2025 adds even more complexity. The existing literature highlights the necessity of efficient mechanisms for assuring data confidentiality, integrity, and authentication in resource-constrained environments concerning IoT. Device authentication and authentic communication of data are some of the key challenges to IoT security. Pairing models, gateway-centric models, and similar current solutions provide solutions for some of the problems but at the cost of scaling and single-point-of-failure risks. Among the new paradigms, which hold much promise in decentralized trust and integrated hierarchical naming, are the likes of Object Naming Service or ONS, Named Data Networking or NDN, and some of the new chain architecture based on trust. Besides, many of them also demand large computational resources that a lightweight IoT may not support easily. The following model completes some previous models for tackling threats on the run against the IoT with the deep learning IDS

The IDS is able to considerably implement this robust framework, independent of any specific network configuration and in promiscuous mode-monitoring traffic across protocols, including Wi-Fi, ZigBee, and Bluetooth-without disrupting any ongoing network operations. It consists basically of three phases: Network Connection Phase, which employs the Connection Prober Module and VNC to interpret and emulate the communication protocols; the Anomaly-Detection Phase uses the Data Collection and Transformation module and the DNN for traffic analysis and classification; the Mitigation Phase isolates the threats and logs incidents using the Actuator and Handler modules. The DNN, pre-trained by a DBN, detects malicious patterns based on features such as transmission rates, IP addresses, and data values. The incremental learning capability of the proposed approach makes it adapt to emerging threats, including zero-day attacks.

In the future, mitigations for these will be scant and pertain to the security of IoT; their security focuses on increasing resource efficiency and scalability. Examples include lightweight cryptographic protocols that reduce computational overheads or adaptive authentications like token-based authentication that could implement an expiration attribute. Machine learning will also boost real-time decisions in dynamic trust assessment. It also further demonstrated scalability and effectiveness, achieving over 96% in accuracy and recall for various attack types such as Blackhole, DDoS, Sinkhole, and Wormhole. This is very good compared to the traditional approaches. This is going to be integrated into IoT network security, scalability, and reliability; hence, it can further facilitate their use in wider adoption of sectors.

- *Ref: Zhang, Zhi-Kai, Michael Cheng Yi Cho, and Shiuhpyng Shieh. "Emerging security threats and countermeasures in IoT." Proceedings of the 10th ACM symposium on information, computer and communications security. 2015.(Presentation Paper)*

- *Abiodun, Oludare & Omolara, Oludare & Alawida, Moatsum & Alkhawaldeh, Rami & Arshad, Humaira. (2021). A Review on the Security of the Internet of Things: Challenges and Solutions. Wireless Personal Communications. 119. 1-35. 10.1007/s11277-021-08348-9.*