Theme: Securing the Future of Smart Healthcare
Name: Group 1 – Kajol . & Aishwarya Mehta

In an era of rapid technological advancement, the integration of Smart Healthcare Systems (SHS) brings both unprecedented benefits and new challenges. The overarching problem revolves around ensuring the security and integrity of health data within these systems. This write-up delves into the current state of SHS security, highlights emerging threats, and proposes a groundbreaking solution in the form of HealthGuard.

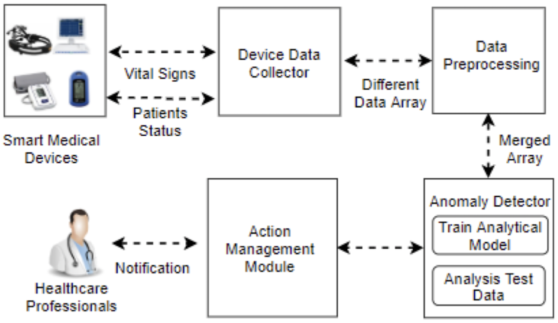


Fig. 2: HealthGuard framework.

General Problem and Research Issues:

The global healthcare market's rapid growth, driven by an aging population and increasing costs, necessitates a more efficient system. Technological advancements, especially in Smart Healthcare Systems (SHS), have shown promise but introduce cybersecurity threats. Malicious attacks, exemplified by real-world incidents, pose significant risks, highlighting the need for robust security solutions.

Current solutions, such as REBEL, NFC/RFID implementations, and sensor-based security, exhibit gaps in comprehensive protection and scalability. HealthGuard, a machine learning-based framework, addresses these concerns by focusing on interconnected body functions rather than just wearable sensors. While it achieves a commendable accuracy of 91%, challenges remain in optimizing its performance and addressing evolving threats.

Taking the Work to the Next Level:

1. Enhanced Algorithm Optimization: Explore advanced optimization algorithms tailored to healthcare data, enhancing HealthGuard's efficiency and adaptability to evolving threats. Enhancing HealthGuard involves incorporating algorithms like XGBoost and LightGBM for complex healthcare pattern decoding.
2. Incorporate Emerging Technologies: Integrate advanced technologies like federated learning to enhance model training without compromising data privacy in a distributed SHS environment.
3. Real-time Threat Intelligence: Implement a dynamic threat intelligence system to enable HealthGuard to adapt rapidly to emerging cyber threats and continuously improve its threat detection capabilities.
4. Human-in-the-loop Integration: Introduce a human-in-the-loop approach to the anomaly detection process, combining machine learning with human expertise for more accurate and contextual threat assessments.
5. Ethical Considerations and Bias Mitigation: Address ethical considerations in healthcare AI, ensuring HealthGuard is free from biases and is aligned with ethical standards, safeguarding patient rights and privacy.

Conclusion:

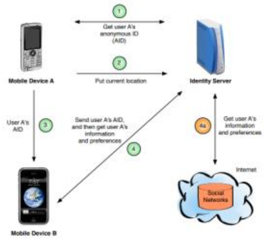
HealthGuard, while exhibiting strong performance, has potential for refinement and expansion. By incorporating advanced optimization techniques, emerging technologies, real-time threat intelligence, and ethical considerations, it can evolve into a more robust and adaptive security framework, securing the future of Smart Healthcare Systems.

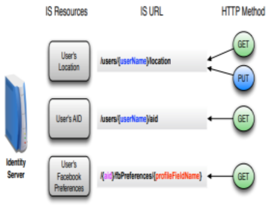
CSE 707: Wireless Network Security

Theme: Balancing privacy and utility in mobile social networking apps

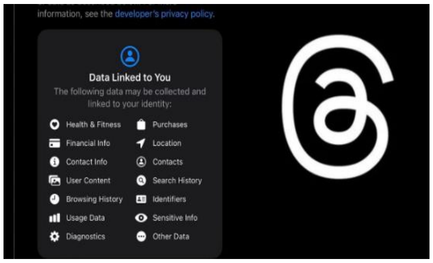
Names: Pavithra Penumuru, Nikhil Sai Sarath V

The paper discusses security and privacy issues with mobile social networking applications. Key problems highlighted include direct exposure of user identities and location data, indirect identification via attribute combinations, and wireless eavesdropping/interception attacks that exploit unencrypted communications. Solutions proposed involve an Identity Server concept to anonymize identities, apply location verification, implement access control and k-anonymity techniques. An Identity Server prototype shows promise.


1
Get user A's anonymous ID (AID)
2
Put current location
Mobile Device A
Identity Server
User A's AID
3
Send user A's AID, and then get user A's information and preferences
4
4a
Get user A's information and preferences
Internet
Social Networks
Mobile Device B



IS Resources	IS URL	HTTP Method
User's Location	/users/{userName}/location	GET PUT
User's AID	/users/{userName}/aid	GET
User's Facebook Preferences	/{aid}/fbPreferences/{profileFieldName}	GET



information, see the developer's privacy policy.

Data Linked to You

The following data may be collected and linked to your identity:

- Health & Fitness
- Financial Info
- Contact Info
- User Content
- Browsing History
- Usage Data
- Diagnostics
- Purchases
- Location
- Contacts
- Search History
- Identifiers
- Sensitive Info
- Other Data

While robust, challenges remain regarding usable security to balance strong anonymity protections and user friction. Emerging areas like decentralized trust networks and hybrid peer-to-onion routing architectures may provide alternatives focused on social groups, access policies and performance. Empowering user control and transparency around data practices also remains important.

Current social platforms still often treat privacy as secondary to growth and revenue. Rethinking incentives and system designs to treat privacy as a fundamental priority is critical as mobile social app usage continues exponential growth amidst escalating sophistication of threats. Skills gaps, policy limitations, transparency issues and misaligned economic motivations persist as obstacles. Collaborative approaches spanning technology, regulation, economics and education are essential to enable secure and user-centric mobile social ecosystem designs going forward.

References:

[1] L. Sweeney, "Uniqueness of Simple Demographics in the U.S. Population," Carnegie Mellon University, 2000.
[2] M. G. Reed and P. F. Syverson, “Onion routing,” in AIPA, 1999 [3] Wenjun Jiang et al., "Towards Environment Independent Device Free Human Activity Recognition," ACM MobiCom, 2018.
[4] R. Dingledine et al., “Tor: The secondgeneration onion router,” Naval Research Lab, 2004.

Theme: Unmasking the Threat of Unauthorized Smartphone Access by Insiders CSE731

Names: Jaswanth Reddy Angeri & Gayeethri Polamreddy

In the contemporary landscape, smartphones play an indispensable role in communication, data storage, and financial transactions, rendering them alluring targets for cyber threats. While substantial research has been directed towards identifying these insider threats and devising security solutions, several challenges persist.

Drawbacks in Current Research:

Conventional adversarial models primarily concentrate on commonplace adversaries, neglecting sophisticated entities such as physical attackers, surveillance agencies, and state-sponsored actors. The reliance on user studies as a prevalent data collection method introduces biases and may not accurately mirror the authentic threat scenario. Furthermore, adversarial models and their corresponding mitigation strategies often lack empirical validation, impeding the assessment of their efficacy. While identifying threats is crucial, research should prioritize the development of practical mitigation strategies.

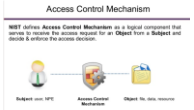
Advancing the Scope:

Broaden the adversarial model to encompass a wider spectrum of adversaries. Utilize diverse data collection methods, including the analysis of security incident reports and the implementation of surveys. Undertake empirical validation studies to gauge the effectiveness of adversarial models and associated mitigation strategies. Innovate and assess practical mitigation strategies. Recognize and rectify the limitations inherent in user studies. Collaborate with security practitioners and developers to glean insights from real-world experiences. Undertake longitudinal studies to monitor shifts in threat patterns and evaluate the enduring efficacy of mitigation strategies. Investigate the potential integration of machine learning techniques into the adversarial model to bolster predictive capabilities and facilitate real-time threat detection, anomaly identification, and adaptive mitigation strategies.

Addressing these challenges will propel smartphone security research towards a more comprehensive, empirically validated, and practically applicable approach, fostering a more secure and resilient smartphone ecosystem.

Technical Implementation: Risk Management,

Real-time analytics
Capture user behavior in real-time across systems
Behavioral monitoring
Identify high-risk activity and discover bad actors
Machine learning
Find anomalies and reduce false positive alerts
Multi-app monitoring
Data from all channels for analysis, reporting and alerts


Access Control Mechanism

NIST defines **Access Control Mechanism** as a logical component that serves to receive the access request for an **Object** from a **Subject** and decide & enforce the access decision.

Subject: user, NPE
Access Control Mechanism
Object: file, data, resource

References:

- https://www.ekransystem.com/en/blog/real-life-examples-insider-threat-caused-breaches
- https://www.youtube.com/watch?v=2BZP3J5xAHE
- https://insights.sei.cmu.edu/blog/challenges-facing-insider-threat-programs-and-hub-analysts-part-2-of-2/

CSE 707: Wireless Networks Security, Principles and Practices

Theme: Unveiling Vulnerabilities in Devices, Even in Safe Modes
Names: Shubhi Srivastava, Ramya Pachhipulusu

This paper talks about the critical vulnerabilities in Apple iPhones' Low Power Mode (LPM) features, exposing the security risks which are present even when the device is powered off. The continued operation of wireless chips like Bluetooth, NFC, and UWB during LPM allows potential attackers to exploit vulnerabilities, including manipulating the Find My feature to track the device's location and injecting malware into the Bluetooth chip by modifying Bluetooth firmware. The use of hardware-based implementation for Low Power Mode (LPM) complicates the problem, making it resistant to regular software updates. This presents a significant threat, enabling attackers to compromise sensitive information like credit card data and digital car keys.

The paper underscores the importance of recognizing that devices considered safe, even in certain modes like iPhone's Low Power Mode, may not be entirely secure. It implies that users and manufacturers should be aware of potential risks associated with specific implementations and features, and ongoing efforts are needed to identify and address vulnerabilities for a more robust security model.

While the paper uncovered vulnerabilities in iPhone security, Apple's response remains unclear, as they haven't officially addressed the findings. Determining Apple's actions is challenging due to the absence of official communication. Indirect evidence, such as the lack of subsequent research on similar vulnerabilities, regular security updates may suggest that Apple might have taken measures to mitigate risks. Third party cybersecurity assessments could also provide assurance if they find no evidence of the highlighted vulnerabilities. Further research can be done in this domain which can contribute to enhancing security. Potential options include the development of more robust firmware, the implementation of a comprehensive shutdown mode, and encouraging users to engage in regular iOS updates for the latest security patches.

While this paper talks only about iPhones, but a similar kind of issue has been found with other devices like Amazon Alexa. Researchers discovered a flaw in Amazon’s Alexa virtual assistant that enabled them to eavesdrop on consumers with smart devices and automatically transcribe every word said. They exploited this flaw using a proof-of-concept Alexa Skill, initiating voice command sessions that failed to terminate, capturing prolonged audio. The issue was reported to Amazon, leading to fixes in certification criteria to detect and reject such eavesdropping skills.

References:

https://threatpost.com/iphones-attack-turned-off/179641/
https://threatpost.com/researchers-hacked-amazons-alexa-to-spy-on-users-again/131401/
https://arstechnica.com/information-technology/2022/03/attackers-can-force-amazon-echos-tohack-themselves-with-self-issued-commands/
https://www.wired.co.uk/article/amazon-echo-alexa-hack

Theme: Utilizing NFC in securing Bluetooth Connections CSE707

Names: Sagnik Mondal, Namrata Banerjee

Our goal in choosing this seminar was to guarantee that we would have a thorough comprehension of the real-world applications of wireless network security by the end of the course. Therefore, we decided to choose a paper about "Bluetooth," which is one of the most widely used wireless technologies. But our paper's discussions were limited to its operation, security measures, and range of current attacks, but did not delve into ways it can be strengthened or mitigate its weaknesses.

Here, we're exploring blending NFC with Bluetooth pairing. NFC allows communication between devices in close range using magnetic fields, reaching speeds up to 424 kb/s. This integration tackles Bluetooth's unreliability and the risk of eavesdropping by using a stronger encryption key (LE Legacy). Its short range ensures secure credential transfer, enhancing the security of the pairing process. It gets around one of Bluetooth's main security vulnerabilities, which is "Discoverability," which frequently requires repeated tries. Also, since users seldom modify the default passkey, hackers can simply figure it out.

One Bluetooth association model offered by Bluetooth SIG is Out of Band (OOB). Unlike sharing passkeys that can be vulnerable to MITM (Man-in-the-Middle) attacks, OOB utilizes pre-shared information. NFC can aid in this process by enabling a "tap to pair" convenience for users, facilitating the secure exchange of information without the need for vulnerable numeric inputs.

In an article from “DigiKey”, the process of using NFC in SSP OOB pairing for Bluetooth devices was explained in detail. When employing SSP OOB pairing, NFC facilitates the communication of a temporary key necessary for BLE devices during the connection process. This key is embedded within a standard NDEF (NFC Data Exchange Format) message. Once the OOB data exchange occurs, developers can utilize additional features outlined in the Bluetooth specification to expedite the connection setup. For instance, the Generic Access Profile (GAP) supports fast connection establishment, outlining procedures for Bluetooth devices to advertise, locate, establish connections, and manage security measures.

Passive NFC tags allow important information to be transferred to a device before it is powered on, such as network settings and passkeys required for secure device connections. This is because the tags can communicate with a reader even when the main system is off. The new device can be tapped against a hub, such as a home automation system, or any smartphone that supports NFC to initiate this transfer. The device can securely connect to the network using the received key once it has been powered on. The key is taken out of the tag after each use in order to preserve security and avoid interception.

We came across another paper 'A hybrid NFC–Bluetooth secure protocol for Credit Transfer among mobile phones' which introduces a mobile solution for peer-to-peer money transfer using NFC and Bluetooth . This hybrid protocol combines Bluetooth's faster (2.1 Mbps) data transfer rates with the security benefits of NFC. The Credit Transfer app is more user-friendly since it doesn't require infrastructure to facilitate cash transfers between mobile devices thanks to NFC technology. Two devices with NFC chips and Bluetooth adapters are part of the system setup, which offers a quick and safe way to transfer credit between mobile devices.

References:

Monteiro, D.M., Rodrigues, J.J.P.C., Lloret, J. and Sendra, S. (2014), A hybrid NFC–Bluetooth secure protocol for Credit Transfer among mobile phones. Security Comm. Networks, 7: 325-337. https://doi.org/10.1002/sec.732

Leveraging Near Field Communication (NFC) to Connect with BLE Smart Sensors - https://www.digikey.com/en/articles/leveraging-nfc-to-connect-with-ble-smart-sensors

Group No. 6
Topic: A.6

Theme: Accidents in Autonomous Vehicles
Names: Sai Saran Putta, Sarthak Jain, Shrishti Karkera

The paper primarily focuses on two categories of sensors: vehicle dynamics sensors and environment sensors. These sensors are crucial components of modern vehicles, particularly autonomous driving. They collect data about the vehicle's dynamics and the surrounding environment. The authors discuss various cybersecurity threats that these sensors could face, including unauthorized access, data tampering, and DOS attacks. They also highlight the need for robust security measures against these threats.

There have been no widely reported incidents of autonomous vehicles being hacked in a manner that caused accidents or led to significant safety concerns in real-world situations. However, researchers and cybersecurity experts have conducted experiments and demonstrations showing potential vulnerabilities in autonomous vehicle systems which we studied in our presentation. In this presentation, let’s explore one phenomenon known as phantom braking which caused multiple accidents in Tesla autopilot.

Phantom braking in Tesla vehicles refers to situations where the car's Autopilot initiates sudden braking without an apparent obstacle or hazard present. This issue has been reported by some Tesla drivers, and it has led to safety concerns and frustration among users. According to the KGW report, there have been documented cases where phantom braking caused crashes. In one case, a Tesla Model S suddenly braked in traffic triggering an eight-vehicle pile-up in San Francisco. The November 2022 crash left nine people injured, including a two-year-old child. In February 2022, a 74-year-old man died after being rear-ended on Interstate 70 in Independence, Missouri. Police reports obtained by KGW showed his Tesla Model 3 unexpectedly slowed from 61 to 12 miles per hour in the middle of a busy interstate.The causes of phantom braking incidents can be complex and multifaceted: 1) *Sensor Interpretation:* Tesla vehicles rely on a suite of sensors, including cameras, radar, and ultrasonic sensors, to perceive the surrounding environment. Sometimes, these sensors might misinterpret objects or environmental conditions, leading to false detections. 2) *Software Algorithms:* The algorithms interpreting sensor data and making decisions might occasionally misinterpret situations. Changes in lighting conditions, reflections, or road debris could confuse the system, causing it to perceive a false threat and initiate braking. 3) *Complex Environments:* Certain scenarios, like transitioning between different road types (e.g., from a brightly lit area to a tunnel), complex intersections, or situations with unconventional traffic patterns, can challenge the vehicle's interpretation and response. It is advised to remain attentive and be prepared to take manual control whenever using Tesla's automated driving features to ensure safety, especially in situations where unexpected behaviors, such as phantom braking, might occur.

Cyber attackers exploiting phantom braking in Tesla or similar vehicles haven't been reported. While there's no known malicious use of this issue, the potential for cyber threats remains a concern. Any system reliant on sensors and networks could be vulnerable to attacks. Automakers constantly bolster security measures, including encryption and software updates, to safeguard against unauthorized access. Ethical hacking and ongoing research help identify vulnerabilities, aiding manufacturers in fortifying their systems. The automotive industry maintains vigilance to ensure the safety and security of autonomous driving technology amidst evolving cyber threats.

References:

Iboshi, Kyle. “Tesla ‘phantom braking’ could endanger drivers and those following them. So why aren't they being warned?”. KGW, 11 October 2023, link

ChatGPT

Theme: Wireless Wearable Security
Names: Dhayaneshwar Balusamy, Sowmiya Murugiah

In our presentation, we emphasized the necessity for robust security within the rapidly expanding domain of wireless wearable devices. The paper delineated the development of an automated security evaluation prototype, focusing on device fingerprinting and identifying vulnerabilities, both passive and active, through the utilization of software-defined radio. The research underscored the escalating prevalence of wearable devices and the accompanying security risks due to their capacity to store and transmit sensitive personal data.

The concept introduces a novel approach to assessing wearable device security by leveraging sophisticated techniques, such as machine learning-assisted fingerprinting and black-box fuzz testing. However, several challenges were identified, including the absence of an open-source, low-level Bluetooth protocol stack. This limitation complicates the analysis and interaction with wearable device protocols, which are integral aspects of comprehensive security evaluation. Furthermore, the diverse nature of wearable devices, each with its unique hardware and software configurations, adds complexity to the security evaluation process, necessitating a highly adaptable and scalable approach.

To elevate this work, addressing these challenges is imperative. One potential improvement could involve developing or adapting an open-source Bluetooth protocol stack that permits necessary modifications and interactions for comprehensive security assessments. This would facilitate more effective fuzz testing and protocol analysis, crucial for uncovering potential vulnerabilities. Enhancing the prototype's data handling capabilities, including more efficient data capture, storage, and processing techniques, would bolster the overall efficacy of the security evaluation process.

Moreover, broadening the prototype's scope to encompass various types of wearable devices could amplify its applicability and relevance in real-world scenarios. Collaboration with manufacturers and leveraging their insights into device operations could provide a deeper understanding of potential security risks.

Finally, integrating more advanced machine learning techniques and algorithms into the finger printing process could significantly enhance the prototype's ability to accurately identify and assess devices. Deep learning models, such as Convolutional Neural Networks, can extract features from complex signal patterns emitted by wearable devices. A pertinent study in this context is by Sankhe et al., presented at IEEE INFOCOM 2019.

References:

Sankhe, Kunal, et al. "ORACLE: Optimized radio classification through convolutional neural networks." IEEE INFOCOM 2019-IEEE Conference on Computer Communications. IEEE, 2019.

Song, Congxi, et al. "SPFuzz: a hierarchical scheduling framework for stateful network protocol fuzzing." IEEE Access 7 (2019): 18490-18499.

Theme: Secure Multipath Routing Protocol for Wireless Sensor Networks

Team Members: Rahul Kulkarni, Sai Vineeth Arumalla

The presented paper centers on challenges faced by routing protocols in wireless sensor networks, so the paper introduces SEER protocol as a potential solution. The paper highlights the need for an energy-efficient and secure routing protocol for WSN applications operating in unattended and hostile environments. Low power consumption is crucial, but network lifetime is a more meaningful metric for protocol performance. However, SEER simultaneously addresses both energy efficiency and security concerns and uses principle similar to the Client/Server software architectures. The base station does the route discovery and maintenance as well as route selection. Instead of a single path, the base station periodically selects a new path from multipath based on current energy level of nodes along each path compared to other proposed routing protocols in WSN, SEER considers energy-efficiency and security simultaneously for the first time. The feature makes SEER distinct is that it takes full advantage of the predominance of the base station, i.e., it lets the base station select a path from multipaths for source and sink nodes. As a result, the network throughput, communication overhead and network lifetime are preferable and works well against some attacks, compared to other proposed protocols. The base station begins topology construction through ND message broadcasts, nodes build a neighbors list. Subsequently, a broadcast of an NC message gathers neighbor data, and nodes respond with NCR messages. So, the base station forms a weighted directed graph to choose paths with maximum available energy on each node. Edge weights represent available energy, diminishing as nodes transmit and receive packets. This enables efficient routing in the sensor network. The base station selects the routing path to defend against attacks like Wormhole, Sinkhole and Selective Forwarding attacks.

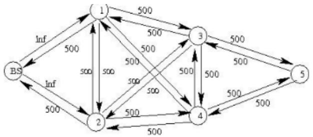
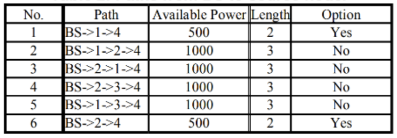


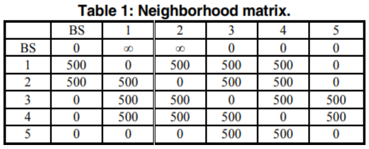
Figure 3: The weighted directed subgraph derived from network topology.

Table 2: Paths from BS to source node.



No.	Path	Available Power	Length	Option
1	BS->1->4	500	2	Yes
2	BS->1->2->4	1000	3	No
3	BS->2->1->4	1000	3	No
4	BS->2->3->4	1000	3	No
5	BS->1->3->4	1000	3	No
6	BS->2->4	500	2	Yes

Table 1: Neighborhood matrix.



	BS	1	2	3	4	5
BS	0	∞	∞	0	0	0
1	500	0	500	500	500	0
2	500	500	0	500	500	0
3	0	500	500	0	500	500
4	0	500	500	500	0	500
5	0	0	0	500	500	0

In the assessment of performance, SEER surpasses the Directed Diffusion protocol in terms of throughput, control overhead, and network lifetime, even when confronted with 20% malicious nodes. The paper provides simulation findings that confirm SEER's performance, leading to the conclusion that SEER outshines other suggested routing protocols in Wireless Sensor Networks. Few of the latest works in WSN we went through are: SASC: Secure and Authentication-Based Sensor Cloud Architecture for Intelligent Internet of Things, Secret Sharing-Based Energy-Aware and Multi-Hop Routing Protocol for IoT Based WSNs. Both these papers have taken the security in WSN to another level by introducing machine learning, cloud computing and computer security concepts.

The protocol's security measures introduce computational overhead, potentially compromising sensor nodes' energy efficiency. Additionally, its adaptability to dynamic networks and scalability across large WSNs needs attention. Future research should focus on optimizing energy consumption without sacrificing security, exploring machine learning for adaptive responsiveness, and assessing scalability in real-world deployments. Advanced cryptographic techniques could enhance the protocol and benchmarking against other security solutions would bolster its credibility and effectiveness.

REFERENCES:

[1] K. Akkaya, M. Younis, A Survey on Routing Protocols for Wireless Sensor Networks, 2006.

[2] Secure and Authentication-Based Sensor Cloud Architecture for Intelligent Internet of Things

[3] Secret Sharing Based Energy-Aware and Multi-Hop Routing Protocol for IoT Based WSNs,(Khalid Haseeb and team)

Theme: Enhancing Smartphone Password Manager Usability and Security: Beyond Basic Adoption
Names: Rahul Nimbalkar. && Anurag.
CSE 707SEM UPAD: Seminars - Wireless Networks Security

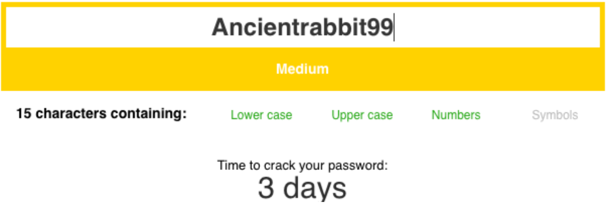
In our presentation, we discussed the usability issues of popular smartphone password managers (PMs). The paper we analyzed, titled "I don't see why I would ever want to use it": Analyzing the Usability of Popular Smartphone Password Managers, focuses on the low adoption rates of PMs on smartphones. The authors identify that usability is a key factor affecting this, with significant issues in integration with external applications, user mistrust due to security concerns, and lack of effective user guidance and interaction.

While the paper did a good job of pointing out the problems, it didn't really dive into how PMs could actually make our digital lives more secure. Imagine if PMs could recognize you just by your fingerprint or the way you tap on the screen—that could make people a lot more comfortable using them. There's also a missed chance to connect PMs with all the smart gadgets we have at home now. The paper mentions that using PMs can be a bit of a brain teaser, especially when you have to jump through several hoops to get something done. But it doesn't really get into how this affects different kinds of people, like those who didn't grow up with all this tech.

Then there's this whole world of smart tech like AI and machine learning that PMs haven't really taken advantage of yet. These could make PMs predict what you need before you even ask for it or check your security without you having to lift a finger. The paper also skips over how teaching people about PMs could actually get more of them to use these apps—like if phone companies and service providers joined the effort.

Wrapping up, the paper gives us some good food for thought on making PMs better for phone users, but there's a whole lot more ground to cover. We're talking about making PMs smarter and more in tune with our daily lives, catering to everyone no matter their age or tech-savviness, and maybe even teaming up with the folks who make our phones to spread the word.

And here's something the paper missed— A straightforward tactic such as adding spaces between words in your password can effectively disrupt a hacker's strategy. It might seem like just a few additional presses on the space bar wouldn't make a big difference, but here's an interesting fact: a password that's all squished together might take a hacker about three days to crack, but throw in a couple of spaces, and suddenly it's like trying to break into a bank vault—it could take them 84 years to figure it out using brute force! That just goes to show, PMs should be more than a digital locker; they ought to be the savvy buddy who shows us how to make passwords so tough, they're practically hacker-proof.

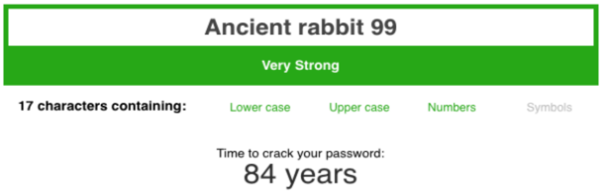


Ancientrabbit99

Medium

15 characters containing:

Time to crack your password:
3 days



Ancient rabbit 99

Very Strong

17 characters containing:

Time to crack your password:
84 years

Recent developments have marked a significant transformation in the protection of password managers (PMs), highlighted by the widespread adoption of encrypted password vaults, decentralized authentication methods to prevent central points of failure, and the incorporation of zero-knowledge proof systems to boost user confidentiality. This shift in PM technology signifies a pivotal change in our approach to and engagement with our digital keys, signaling an era where the dual goals of security and user-friendliness unite seamlessly in our daily use. This updated content introduces the behavior-based authentication and underscores the significance of zero-knowledge proofs and decentralized authentication techniques, all integral components of the latest innovations in the PM sector. Moreover, the content underscores the necessity for PMs to play an active role in educating users about crafting robust passwords.

Theme: ONE KEY TO RULE THEM ALL **CSE707**
SECURE GROUP PAIRING FOR HETEROGENEOUS IoT DEVICES.

Names: Sai Abhilash Kondepati, Pavithra Nallamothu.

In our presentation, we talked about types of IOT devices, attacks possible on them, current solution for group pairing and IoTCupid, a secure group pairing system for Heterogeneous IoT devices. Authors of the paper focused on the solution for group pairing of heterogeneous IoT devices using inter event timings between the events, overcoming the limitations of context based pairing systems, in which, devices would be paired using common physical qualities between them. By using the inter event timings between the events, it is easier to pair devices with different/varying physical qualities.

Using IoTCupid helps in achieving faster pairing time, pairing instant and continuously influenced devices, and supports dynamic device addition and removal. However, there are some limitations like, it fails to pair in larger spaces like industries and impact of environmental noises might affect pairing.

To reduce the failures while pairing in larger spaces, we could implement Mesh networking or have multiple access points for pairing. We could implement advanced noise cancellation algorithms like Least Mean Squares and Spectral Subtraction on the device that is responsible for processing the microphone input. These algorithms can help filter out background noises and focus on the relevant signals. This process can be used to overcome the impact of environmental noise.

References:

H. Farrukh, M. O. Ozmen, F. Kerem Ors and Z. B. Celik, "One Key to Rule Them All: Secure Group Pairing for Heterogeneous IoT Devices," 2023 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 2023

P. Han, A. J. Chung, M. K. Sinha, M. Harishankar, S. Pan, H. Y. Noh, P. Zhang, and P. Tague, “Do you feel what i hear? enabling autonomous IoT device pairing using different sensor types,” in IEEE Symposium on Security and Privacy (S&P), 2018.

Theme : IntelligentChain: Blockchain and Machine Learning based Intelligent Security Application for Internet of Vehicles (IoV)

Names : **Jayadhar Gandham** **Ithihas Reddy Basireddy** **CSE 707SEM**

The research paper by A. Kumar and D. Das, titled "IntelligentChain: Blockchain and Machine Learning based Intelligent Security Application for Internet of Vehicles (IoV),"delves into the critical intersection of blockchain, machine learning, and Internet of Vehicles (IoV).

General Problem and Current Research Issues:

The Internet of Vehicles (IoV) promises a connected and efficient transportation system, but it also raises significant security concerns. Traditional security measures often fall short in addressing the dynamic and interconnected nature of IoV. Kumar and Das propose a novel solution, IntelligentChain, which integrates blockchain and machine learning to enhance the security of IoV. The paper explores how these technologies can collaboratively secure vehicular communications, prevent cyber-attacks, and ensure the integrity of data in IoV ecosystems.

One primary challenge in the IoV landscape is the susceptibility to malicious attacks, including data manipulation and unauthorized access. Current security frameworks struggle to keep pace with the evolving threat landscape, necessitating innovative solutions like IntelligentChain. However, the paper does not extensively delve into the scalability and real-world implementation challenges associated with deploying such a sophisticated security system in large-scale IoV environments.

Suggestions and Advancements :

One notable limitation is the lack of detailed insights into the scalability of the proposed solution. Large-scale IoV environments involve a massive number of interconnected devices, and the paper could benefit from an in-depth discussion on how IntelligentChain can efficiently handle the increased computational and communication overhead.

Additionally, the integration of machine learning algorithms raises questions about the model's adaptability to evolving attack patterns. Future research could focus on developing dynamic machine learning models capable of continuous learning and adapting to emerging threats in real-time.

Use Case: *IntelligentChain can be applied to track and validate environmental data, such as air quality and pollution levels. This ensures the accuracy and reliability of the collected information, supporting environmental monitoring initiatives and policy-making.*

Moreover, the paper could explore the potential energy consumption implications of deploying IntelligentChain in resource-constrained IoV devices. A comprehensive analysis of the energy efficiency of the proposed security solution would provide valuable insights for practical implementation.

In conclusion, while the IntelligentChain framework presents a promising step towards securing the Internet of Vehicles, addressing scalability, adaptability, and energy efficiency concerns is crucial for its practical viability. Future research should strive to refine and optimize the proposed model, ensuring it meets the demands of large-scale IoV deployments and remains resilient to the ever-evolving landscape of cyber threats.

References:

1.Chen, M., et al. (2021). "Machine Learning for Internet of Things Data Analysis: A Survey." IEEE Internet of Things Journal, 8(5), 3570-3588.

2. Wang, C., et al. (2019). "Blockchain-based Internet of Vehicles: A Review, Challenges, and Solutions." IEEE Access, 7, 173669-173681.

Theme: Usable user authentication on a smart watch using vibrations
Names : Naren Kassyap Subramanian & Yashwanth Rama Krishna Reddy

This paper introduces a approach to user authentication on smartwatches by leveraging low frequency vibrations available in a smartwatch as a unique biometric identifier. The proposed system utilizes the intrinsic characteristics of users' touch interactions with the smartwatch's surface, translating these patterns into distinct vibration signatures for individual authentication. Through machine learning techniques, the system aims to provide a secure and convenient method for user authentication on smartwatches.

Unlike existing methods that primarily rely on traditional authentication mechanisms such as PINs, passwords, or biometric sensors, our approach capitalizes on the haptic feedback capabilities of smartwatches. By extracting and analyzing the subtle variations in vibrations caused by users' touch interactions, our system offers a non-intrusive and continuous authentication process. This approach provides an additional layer of security, as it is less susceptible to common vulnerabilities associated with traditional authentication methods.This approach also uses low frequency vibrations which makes this approach scalable to all the smartwatches in the market.

Future work: Investigate the integration of multiple modalities, such as touch gestures, accelerometer data, and heart rate variability, to create a more robust and adaptive authentication system. This multi-modal approach aims to enhance security while accommodating diverse user behaviors and environmental conditions.Explore the feasibility of extending the haptic-based authentication system to support cross-device authentication. Investigate methods for securely connecting smartwatches with other devices, such as smartphones or smart glasses, to create a unified and secure authentication ecosystem.

External factors such as background noise and vibrations from everyday activities can introduce noise into the system, impacting the accuracy of user authentication. Mitigating the effects of environmental noise on the smartwatch's vibration sensor is a research challenge.Continuous monitoring of vibrations for authentication purposes may consume significant battery power on smartwatches. Research is needed to optimize algorithms and implement energy-efficient solutions to ensure practical usability without compromising on security

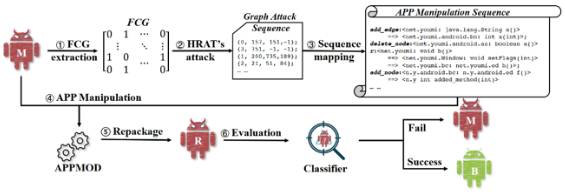
References:

Vhaduri, S., & Poellabauer, C. (2019). Multi-Modal Biometric-Based Implicit Authentication of Wearable Device Users. IEEE Transactions on Information Forensics and Security

Liu, S., & Wei, S. (2021). Recent Advances in Biometrics-Based User Authentication for Wearable Devices: A Contemporary Survey. Digital Signal Processing, 125(1), 103120.

Theme: Structural Attack against Graph Based Android Malware Detection
Names: Rishab Aggarwal, Mehul Mittal

In our presentation, we talked about malware detection techniques, integrating a heuristic optimization model with a reinforcement learning framework. This approach, termed HRAT, includes four types of graph modifications that correspond to manipulations in Android apps. Through extensive experiments on over 30,000 Android apps, HRAT showed high attack success rates in both feature space and problem space, and the results indicated that combining multiple attack behaviours strategically enhances the effectiveness and efficiency of the attack.



```
add_edge:<net.youmi: java.lang.String a()>
    ==> <net.youmi.android.bn: int a(int)>;
delete_node:<net.youmi.android.az: boolean a()>
r:<net.youmi: void b()>
    ==> <net.youmi.Window: void setFlags(int)>
    ==> <net.youmi.bc: net.youmi.ed h()>;
add_node:<n.y.android.bc: n.y.android.ed f()>
    ==> <n.y int added_method(int)>
--
```

While the paper focuses on structural attacks against Android malware detection, it might benefit from a broader discussion on the application of GNNs in diverse fields and the intricate relations between different trustworthiness aspects like privacy and fairness, especially in adversarial settings.

The DMalNet framework's approach to generating insights through ablation studies could be a valuable addition to the paper. This could involve exploring how different components of their malware detection system are affected by structural attacks and what insights can be gained about the system's robustness and effectiveness.

A more comprehensive discussion on balancing high performance with challenges like adversarial vulnerability, resource consumption, and potential discrimination might provide a more holistic view of the problem space. Evaluating the impact of HRAT in real-world scenarios, beyond the controlled experimental setup, would provide valuable information about its practical implications.

This could involve collaborating with cybersecurity firms or app developers. Regarding ethical and legal considerations, given the nature of the work, it's important to address these related to the creation and use of malware or malware-like structures, even in a research context. Expanding the dataset and testing environments could provide deeper insights into the model's robustness and scalability, ensuring no affect the public while adding value to the security research.

References:

1. Zhang, H., Wu, B., Yuan, X., Pan, S., Tong, H., & Pei, J. (2022). Trustworthy graph neural networks: Aspects, methods and trends. *arXiv preprint arXiv:2205.07424*.
2. Li, C., Cheng, Z., Zhu, H., Wang, L., Lv, Q., Wang, Y., ... & Sun, D. (2022). DMalNet: Dynamic malware analysis based on API feature engineering and graph learning. *Computers & Security*, *122*, 102872.
3. Zhao, K., Zhou, H., Zhu, Y., Zhan, X., Zhou, K., Li, J., ... & Luo, X. (2021, November). Structural attack against graph based android malware detection. In *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security* (pp. 3218-3235).