IoT vulnerabilities security project

Islam Tahina

0211105

Introduction

The Internet of Things (IoT) has transformed from a concept of connecting everyday objects like fridges and thermostats to the internet into a ubiquitous network that permeates various aspects of our lives. This revolution began with simple connected devices and has now evolved into complex systems impacting entire industries. IoT's integration into modern technology marks a significant shift in how we interact with the digital world.

The journey of IoT encompasses a range of advancements including faster connectivity through 5G networks, data processing at the edge for reduced latency, and AI-powered decision-making. These technological advances aided in IoT's growth enabling real-time data analysis and more reliable responsive devices. The number of connected IoT devices is estimated to surpass 29 billion by 2030 illustrating the scale and impact of this technology.

IoT offers numerous benefits such as enhanced efficiency in business operations, improved customer experiences with smart home devices, and resource conservation in smart cities. Its data collection and analysis capabilities enable informed decision-making, leading to more successful outcomes.

However, despite the advantages, the rapid expansion of IoT has led to significant security challenges. The diversity of IoT devices creates multiple points of vulnerability making them targets for various cyberattacks. Two primary methods of attack are brute-forcing weak passwords and exploiting network service vulnerabilities. These methods have been used in significant attacks, with the first large-scale IoT malware recorded in 2008. The dark web has seen an increase in services related to IoT attacks including DDoS attacks and the sale of exploits for zero-day vulnerabilities. These services demonstrate the evolving nature of threats targeting IoT devices. IoT malware is diverse with families like Mirai discovered in 2016, leading to a plethora of modified versions. These malwares are used for DDoS attacks, ransomware targeting user data, and even crypto mining attempts. Consumer IoT devices such as webcams and smart pet feeders have been targeted for various purposes including snooping and data theft. Inadequate security measures in these devices have led to incidents of private footage being leaked or devices being used as tools for cybercrimes.

To address these challenges, studying IoT vulnerabilities is crucial due to the ever-increasing reliance on these devices in both personal and industrial contexts. The need for effective cybersecurity measures is important to safeguard against the threats in the IoT landscape. This study aims to explore these vulnerabilities and develop a countermeasure to enhance IoT security contributing to a safer digital ecosystem.

Problem Definition: Visibility in IoT Data Exchange

The challenge in IoT security within households is the lack of visibility of data transmission. This issue extends to the frequency of device connections, the volume of data transmitted, and the specific destinations of this data. For example, a household camera connecting repeatedly within a short time

could be operating normally or indicating a security breach. Without transparency in these data flows, distinguishing between routine operation and potential security threats becomes difficult.
IoT devices often transmit sensitive data such as personal information, usage patterns, and sometimes even biometric data. This can include everything from basic operational data from smart appliances to intimate details captured by security cameras or health monitors. The lack of visibility in how this data is managed, stored, or shared poses significant privacy and security risks.

The lack of visibility into IoT data exchanges poses significant risks:

- Security Vulnerabilities: As Thales Group points out, IoT ecosystems face increased security vulnerabilities due to factors like weak passwords, insufficient updates, and poor device management. IoT devices may become increasingly vulnerable over time without regular updates. Additionally, IoT devices are often targeted for industrial espionage, ransomware attacks, and eavesdropping, making them a conduit for sensitive data leaks and operational disruptions.
- Unrecognized Device Activities: A study highlights risks like shadow IoT where devices operate without IT knowledge leading to compliance violations and the use of recalled risky devices. Surprisingly, many IT teams lack awareness of the smart objects active on their networks. This lack of control over 'Shadow IoT' devices creates a significant security gap, as these devices can be used maliciously without detection.
- Increased Risk and Incidents: Help Net Security notes an increasing visibility gap in IoT initiatives leading to increased risk and security incidents. This gap is worsened by insufficient inventories and the slow challenging process of obtaining comprehensive visibility. Also, IoT devices, being vulnerable to botnet attacks, complicate this risk as demonstrated by the Mirai botnet incident.
- Challenges in Security Management: The increase of unprotected IoT devices poses serious security concerns. Tools for IoT device discovery, threat detection, and endpoint profiling are essential yet not often used. Also, the existence of the dark web criminals focusing on IoT-related services like DDoS attacks and zero-day exploits further complicates their security.

Considering these expanding threats, it's clear that enhanced visibility and control in IoT data exchange are necessary. This project aims to address these challenges by developing methods to illuminate hidden data flows and equip users with the means to protect their digital privacy and security in the ever-evolving IoT landscape.

List of Possible Approaches:

Potential strategies to address the problem:

- Security Integration in R&D: Integrating security considerations during the research and development stage which ensures the development of robust solutions capable of protecting each network layer from potential threats.
- Robust Authentication Mechanisms: Implementing strong authentication systems, such as digital certificates and Public Key Infrastructure (PKI), guarantees the authenticity and integrity of data transmissions from IoT devices.

- End-to-End Security Measures: Ensuring the confidentiality of data exchanged between IoT devices through encryption and decryption processes is critical to prevent unauthorized interception.
- Data Integrity Assurance: Utilizing methods like blockchains, Message Integrity Codes (MIC), and hash functions can significantly enhance the integrity and trustworthiness of data from IoT devices.
- Device Responsiveness and Availability: Maintaining the operational readiness and responsiveness of individual IoT devices and nodes is key to enhancing network resilience against attacks.
- Replay Protection Mechanisms: Protecting IoT networks from the playback of previously transmitted data packets, which could be exploited to infiltrate the network.

Layer-Specific Security Measures:

- IoT Perception Layer Security: Addressing vulnerabilities in the physical network components, such as node capture attacks, malicious code injection, jamming, and sleep deprivation attacks, is essential for securing the perception layer.
- Network Layer Protection: Mitigating risks at the network layer, including eavesdropping, selective-forwarding attacks, denial of service (DoS), and Man in the Middle attacks maintains secure data transmission.
- Application Layer Defense: Tackling vulnerabilities at the application layer, such as malicious scripts, code injections, and data distortion attacks protects user-facing IoT applications.

Addressing Specific Device Vulnerabilities like Single Antenna Device Security requires special attention. Employing strategies like multipath signal propagation or antenna polarization can limit specific vulnerabilities related to these devices.

In summary, a comprehensive approach to IoT security involves a multi-layered strategy that addresses vulnerabilities across all network layers, implements robust authentication and encryption, and stays updated with evolving attack patterns and countermeasures. This broad perspective is essential for developing effective solutions that enhance IoT security and contribute to a safer digital ecosystem.

Proposed Solution: IoT Data Visibility Tool (IDVT)

My proposed solution is an innovative IoT Data Visibility Tool (IDVT) designed to enhance transparency in IoT data exchanges within household environments. This tool is structured to meticulously monitor, analyze, and visually represent the data transmitted to and from the household IoT devices. It encompasses key features like detailed packet monitoring, which tracks the number, frequency, and type of packets sent to specific entities such as vendors, websites, or devices. Moreover, it incorporates an advanced data analysis module to identify unusual patterns or potential security vulnerabilities. A significant emphasis is placed on developing a user-friendly interface ensuring that users can easily comprehend and interact with their IoT data flows.

The IDVT directly tackles the core challenge of visibility in IoT data exchanges, addressing a fundamental gap in household IoT security. Its design is rooted in the principle of empowering users, providing them with the necessary tools to understand and control their digital privacy and security. By offering a clear

visualization of data flows, this tool enables users to become actively involved in their IoT ecosystem. This proactive and preventive approach to security allows users to identify and mitigate potential vulnerabilities before they can be exploited.

Implementing the IDVT promises a multitude of benefits. Primarily, it significantly enhances users' awareness of their IoT interactions and digital footprint promoting better security practices. T This increased awareness is essential for early threat detection which helps to stop possible security breaches. Furthermore, the tool facilitates informed decision-making regarding device usage and security measures allowing users to gain control over their digital environment.

The development of the IDVT does not aim to resolve a specific security vulnerability but it addresses the overarching issue of ignorance and lack of control in personal data management within the IoT landscape. Through this tool, we envision a future where users are not only aware of but also empowered to manage their digital privacy and security effectively.

Implementation of the IoT Data Visibility Tool (IDVT):

My implementation of the IDVT involves a multi-component system focused on capturing, analyzing, and visualizing network packet data. At the core of this system is a server set up to utilize TCPdump, a powerful command-line packet analyzer. This tool is specifically chosen for its reliability and efficiency in capturing network traffic. It operates by collecting all packets on the network and saving them into a pcap file, a format widely used for packet analysis.

Once the data is captured, it undergoes a transformation process. I emplyed Tshark, the command-line version of Wireshark to analyze the pcap file and convert the packet data into a more manageable JSON format. The rationale behind using Tshark lies in its detailed analysis capabilities and the flexibility it offers in converting data into JSON. This conversion is an important step in preparing the data for further analysis and visualization.

The next stage involves the front-end interface where the JSON data is sent for processing where an analysis takes place, filtering the data through various parameters such as source and destination, and categorizing the requests as inbound or outbound. This approach to data handling allows for an organized and clear visualization that helps with identification of abnormal patterns in network traffic.

One of the key features of my implementation is its ability to display the activity of each IoT device connected to the network which is achieved by showing a count of the incoming and outgoing calls for each device. This method serves as a proof of concept providing a straightforward way to detect potential security issues for example, a device that is typically inactive but shows unexpected network activity could be a sign of a security breach.

During the implementation phase, several challenges were encountered like the large volume and complexity of the data captured by TCPdump required efficient data parsing and management strategies. Additionally, ensuring real-time analysis with minimal delay was crucial to the effectiveness of the IDVT demanding significant optimizations in both packet capturing and data processing techniques.

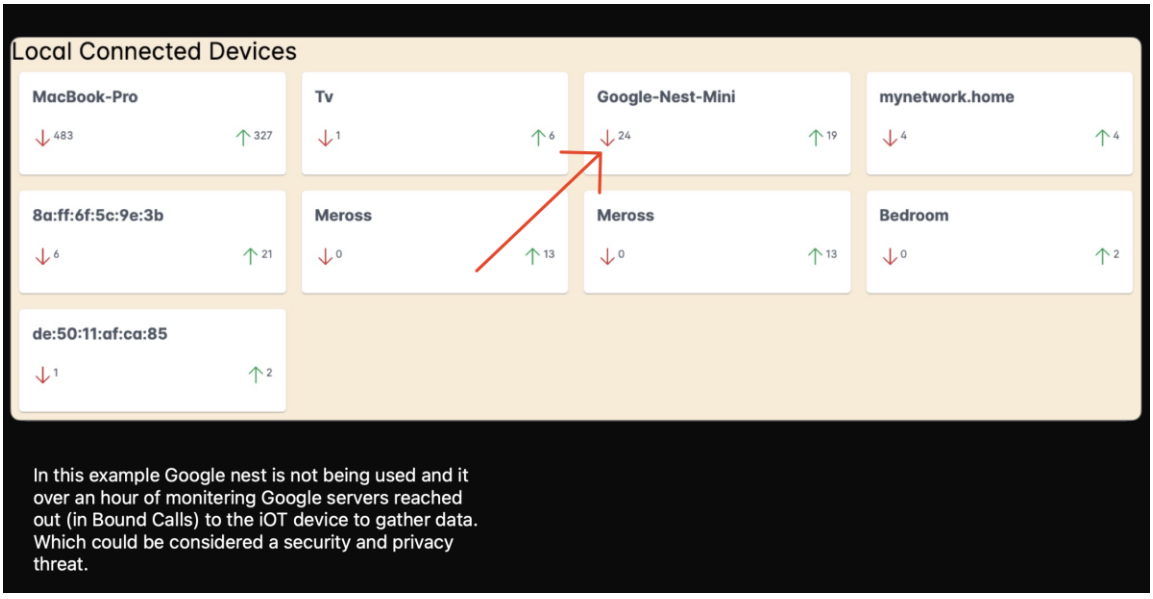
To validate the IDVT's effectiveness, I first tested it on diverse networks including my home network with numerous IoT devices. This initial phase aimed to establish a baseline of normal activity for each device. By monitoring these devices' regular usage patterns it helps us recognize standard operational behaviors. This was crucial for setting a reference point to later identify potential security threats and anomalies.

Looking forward, there is potential for expanding the capabilities of the IDVT like integrating more advanced analysis tools to study the data further and highlight potential threats. Also, investigation of the actual content of packets with a focus on maintaining privacy considerations. It's important to note that this system does not provide a security issue as it is designed to run on the local network only and all the data is internal.

Results and Discussion:

The test phase of the IoT Data Visibility Tool (IDVT) revealed intriguing insights into the behavior of multiple smart devices within my household network. A notable observation was the high number of inbound calls from Google servers to our Google Nest that have not been used for months, it showed 19 outbound requests, indicating some form of data exchange or status updates occurring without out active engagement with the device. This could raise potential privacy concerns as it suggests data transmission to external servers without user activity but knowing Google's policy makes it understandable.

An Easel that I created when I was testing:



While the Meross devices that were a smart light and a garage opener displayed a different pattern. These devices regularly sent status updates to the home kit with both showing a count of 13 outbound requests, unlike the Google device, they had no external inbound calls. This indicates that their communication was confined within the local network which is generally a safer practice in IoT security.

This dichotomy highlights the importance of understanding and monitoring IoT device behavior. While some activities might be expected (as per terms and conditions of the device), others might be indicative of underlying security risks. The IDVT's ability to illuminate these patterns is key in fostering a more secure and privacy conscious IoT environment.

In conclusion, my solution demonstrates significant potential in enhancing the security and privacy of IoT environments. Its ability to visualize unusual device behavior offers users an insightful perspective into their home IoT ecosystem. Such visibility empowers users to identify and address potential security threats, thereby contributing to a safer digital landscape. The IDVT's approach and findings open the way for further research and development in this area of cybersecurity.

Conclusion:

The IoT Data Visibility Tool (IDVT) have provided valuable insights into the network behaviors of IoT devices within a household environment. This tool has revealed diverse patterns of activity among different devices showcasing the complexities of IoT interactions. A notable finding is the varied communication patterns, such as the Google device's unexpected external communications compared to the Meross devices' internal-only communication. This highlights the need for greater visibility and control in IoT networks to identify and lessen potential security and privacy risks.

The findings from this project carry significant implications for the wider cybersecurity community. First, there is a clear need for user-centric security tools that empower users to understand and manage their digital environments effectively. This approach enhancs the security position of IoT ecosystems. Second, my project highlights the importance of data transparency in IoT devices suggesting a need for industry standards and regulatory frameworks that ensure robust privacy and security practices. Finaly, this study serves as a reminder of the ongoing security risks associated with IoT devices emphasizing the need for caution from both manufacturers and consumers.

Looking forward, several avenues for further research and development emerge from this project. Enhancing the IDVT with advanced machine learning algorithms could improve its detection capabilities potentially predicting and preventing security breaches. Expanding the tool's scope to encompass a broader range of IoT devices and integrating it with cloud services could offer a more comprehensive network analysis. Long-term studies would be beneficial to gain deeper insights into IoT device behavior over extended periods. Additionally, a focus on user education with the development of educational resources to raise awareness about IoT security encouraging users to take proactive steps in safeguarding their digital privacy and security.

In conclusion, the IoT Data Visibility Tool represents a significant step forward in addressing the challenges of IoT security. The insights gained from this study not only highlight the need for improved security measures in IoT environments but also open up new opportunities for further research in this area of cybersecurity. The project has laid a foundation for enhancing IoT security and user privacy contributing to the development of more secure and resilient digital ecosystems.

References

Authors Vitaly Morgunov Yaroslav Shmelev Kaspersky Security Services Kaspersky ICS CERT, Vitaly Morgunov Yaroslav Shmelev Kaspersky Security Services Kaspersky ICS CERT, Name, Legezo, B. L. D., John Hultquist Brian Bartholomew Suguru Ishimaru Vitaly Kamluk Seongsu Park Yusuke Niwa Motohiko Sato, Marco Preuss Denis Legezo Costin Raiu Kurt Baumgartner Dan Demeter Yaroslav Shmelev, Ivan Kwiatkowski Maher Yamout Noushin Shabab Pierre Delcher Félix Aime Giampaolo Dedola Santiago Pontiroli, Dmitry Bestuzhev Costin Raiu Pierre Delcher Brian Bartholomew Boris Larin Ariel Jungheit Fabio Assolini, Kaspersky, GReAT, Amr, Nikita Nazarov Kirill Mitrofanov Alexander Kirichenko Vladislav Burtsev Natalya Shornikova Vasily Berdnikov Sergey Kireev, Igor Kuznetsov David Emm Marc Rivero Dan Demeter Sherif Magdy, Anufrienko, A. K. S., Dmitry Galov Dan Demeter Mohamad Amin Hasbini David Emm, & Gerling, V. D. S. (2021, May 13). *IOT threats in 2023*. Securelist English Global securelistcom. https://securelist.com/iot-threat-report-2023/110644/

Contributor, C. (2023, October 26). *Top 5 IOT security risks in 2023*. ThriveDX. https://thrivedx.com/resources/article/top-5-iot-security-risks-in-2023

Evolution of internet of things : Past, present and future. TechAhead. (2023, September 15). https://www.techaheadcorp.com/knowledge-center/evolution-of-iot/

Gerardi, R. (n.d.). *An introduction to using tcpdump at the Linux Command Line*. Opensource.com. https://opensource.com/article/18/10/introduction-tcpdump

Home: Tcpdump & libpcap. Home | TCPDUMP & LIBPCAP. (n.d.). https://www.tcpdump.org/

IOT security challenges and problems. Balbix. (2022, May 26). https://www.balbix.com/insights/addressing-iot-security-challenges/

IOT security: Key internet of things trend for 2023. Data. (n.d.). https://www.data-alliance.net/blog/iot-security-key-internet-of-things-trend-for-2023/

Kaspersky. (2023, September 21). *Kaspersky unveils an overview of IOT-related threats in 2023*. www.kaspersky.com. https://www.kaspersky.com/about/press-releases/2023_kaspersky-unveils-an-overview-of-iot-related-threats-in-2023

Sheldon, R. (2020, December 16). *5 tools to help improve IOT visibility, device security: TechTarget*. IoT Agenda. https://www.techtarget.com/iotagenda/feature/5-tools-to-help-improve-IoT-visibility-device-security

Tshark(1) Manual Page. tshark(1). (n.d.). https://www.wireshark.org/docs/man-pages/tshark.html