Securing the Future: Key Takeaways and Next Steps in IoT Security

Raveen Wijewickrama

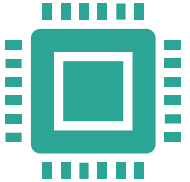
UTSA

SPrITE LAB

Internet of Things

A network of physical objects

—devices, vehicles, buildings, and other items

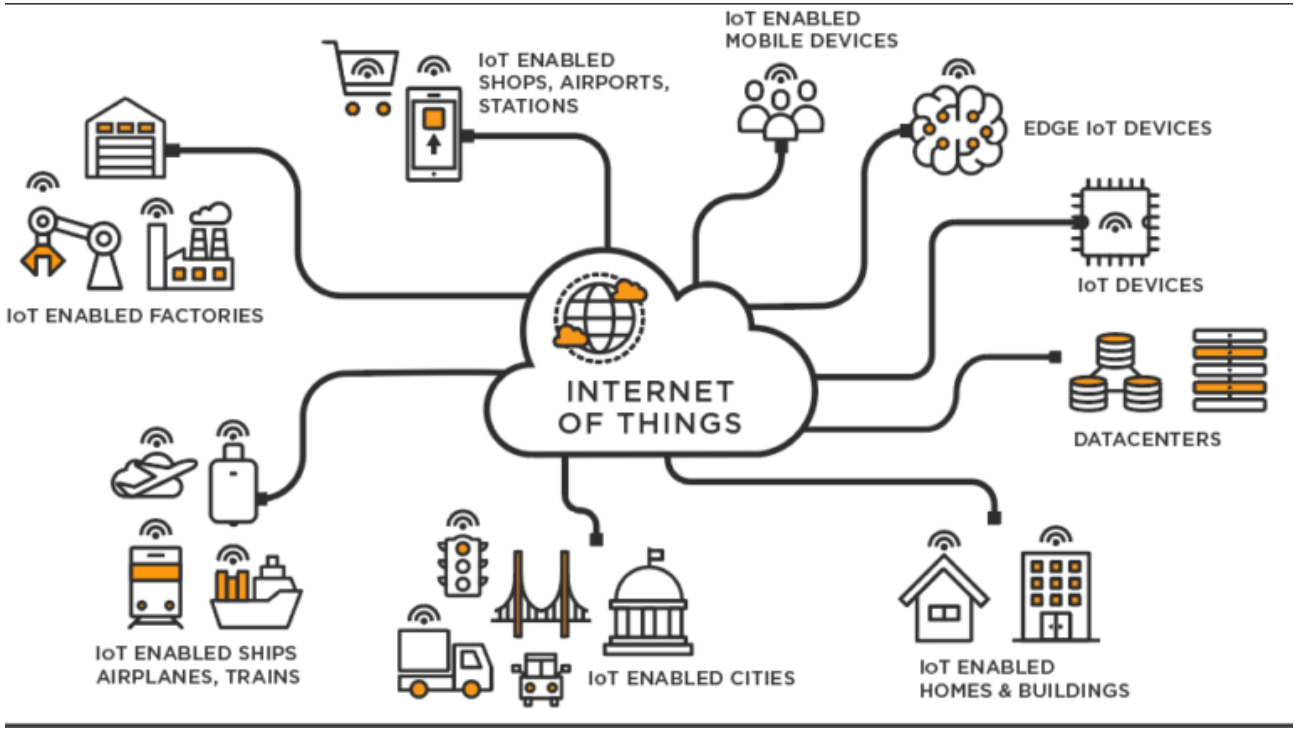


—embedded with sensors, software, and other technologies

with the goal of connecting and exchanging data with other devices and systems over the internet.

Growth and Impact

- **Proliferation of Devices:**
  - 25 billion devices by 2030 (financesonline.com, 2024).
- **Diverse Applications:**
  - smart homes, healthcare, industrial automation, transportation, and agriculture.



(umich.edu, 2023)

Challenges in IoT Security

Massive Attack Surface:

The sheer number of connected devices increases the potential points of attack.

Heterogeneity:

Different manufacturers with varying standards and security protocols, leading to interoperability issues.

Resource Constraints:

Limited processing power, memory, and battery life, making it challenging to implement robust security measures.

Data Privacy:

Collects vast amounts of data, raising concerns about data privacy and the potential misuse of personal information.

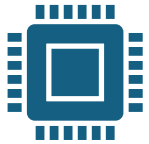
Security Threats

Unauthorized Access:

Attackers gaining access to devices or networks without permission.

Data Breaches:

Exposure of sensitive data due to vulnerabilities in the devices or communication protocols.



Malware and Botnets:

Being infected with malware, often becoming part of botnets used for large-scale attacks like DDoS.

Physical Attacks:

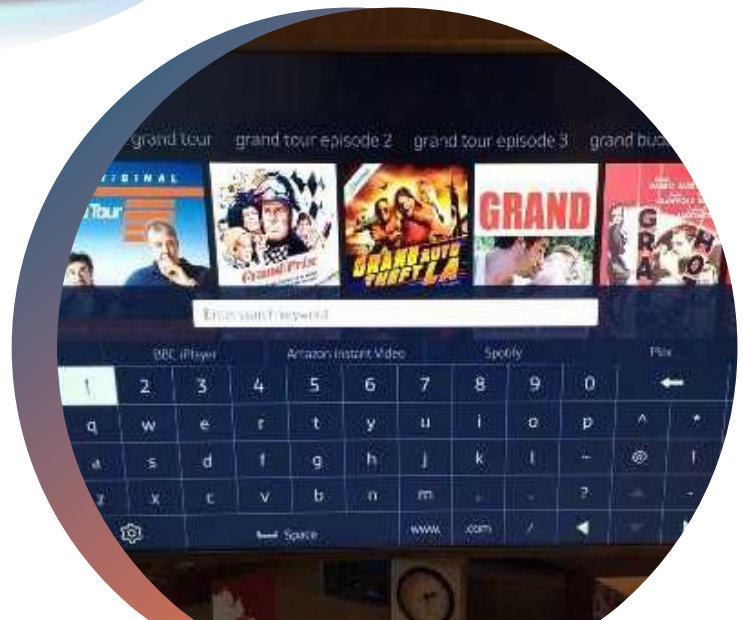
Direct physical access to devices, allowing tampering or extraction of sensitive information.

Attacks on Household Devices

- LightEars (Maiti et al., 2018)
  - Inferring what song/video the user is playing by analyzing the changing light intensities/colors of the smart light.

Attacks on Household Devices

- OverHear (Wijewickrama et al., 2024)
  - Keystroke inference via smart headphones.



Attacks on Household Devices

- Acoustic Keystroke Leakage on Smart Televisions (Kannan et al., 2024).
  - Keystroke inference of smart TV virtual keyboards by using microphones of nearby smart devices such as Alexa or Google Home Assistants.

Attacks on Household Devices

- Ring Home – Security Camera Breach.
- Eufy Security Camera Breach.

The New York Times

Somebody's Watching: Hackers Breach Ring Home Security Cameras (Published 2019)

Ring users can monitor the cameras on the company's smartphone app and speak to people inside their home and at their front door using a two-way...

Jan 29, 2024

9to5Mac

Eufy camera security breach admission, but many more questions

The doorbell's camera was uploading facial recognition data from the camera to Eufy's cloud servers with identifiable information attached, and...

Dec 21, 2022

Fast Company

FTC to pay Ring customers millions over video privacy breach

The Federal Trade Commission is sending more than $5.6 million in refunds to consumers as part of a settlement with Amazon-owned Ring,...

Apr 26, 2024

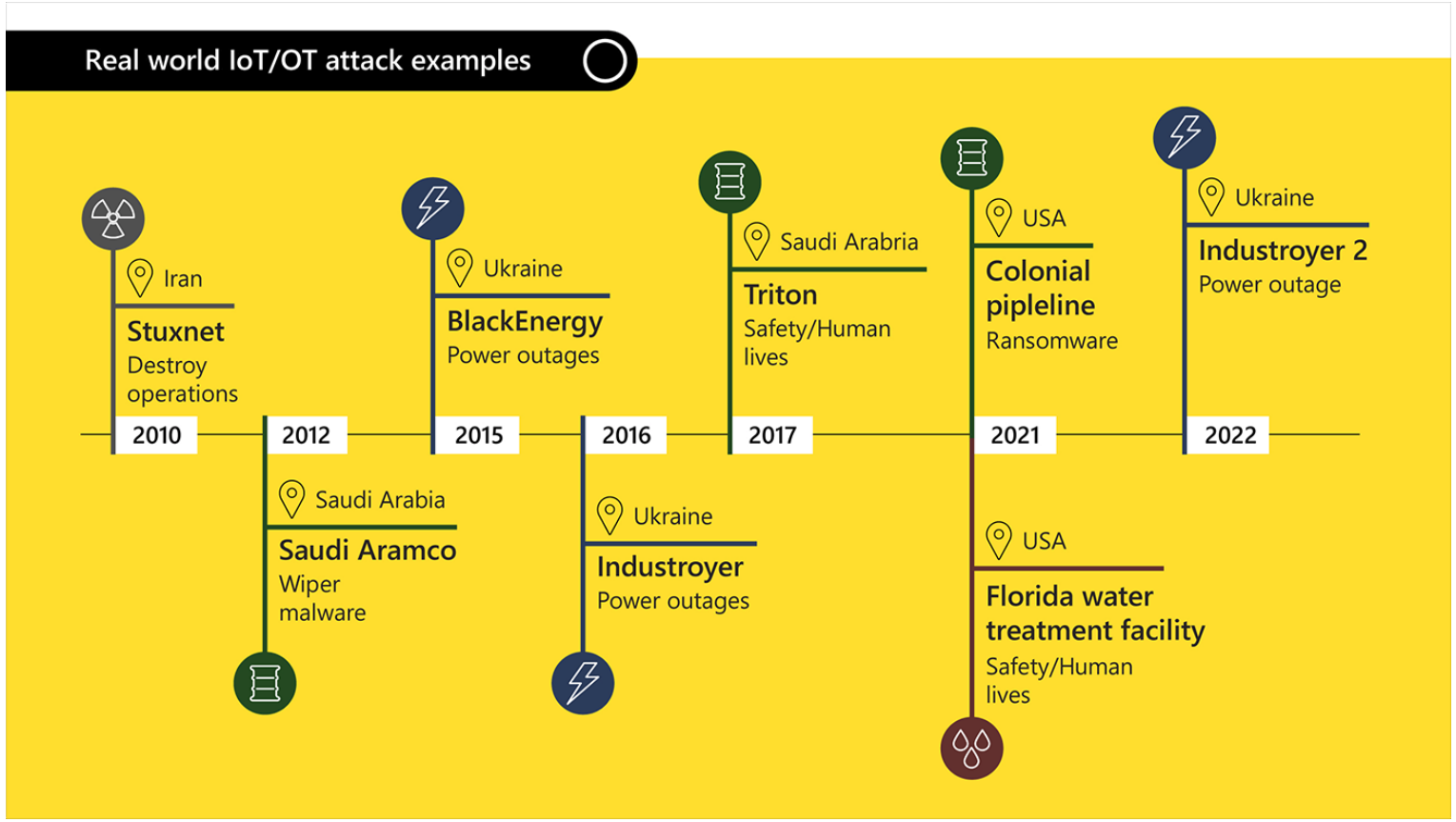
ZDNET

Anker admits Eufy security cameras were not natively encrypted

It's been a few months since customers learned Eufy had been uploading data to cloud servers without user permission, and now the company is...

Feb 1, 2023

Risks to Critical Infrastructure



(Microsoft.com, 2024)

Defenses

Strong Authentication:

Robust authentication mechanisms to ensure that only authorized users and devices can access the system.

Encryption:

Using encryption to protect data both in transit and at rest, safeguarding it from interception and unauthorized access.

Regular Updates and Patching:

Ensuring that devices and software are regularly updated to patch known vulnerabilities.

Network Segmentation:

Segregating IoT devices from critical network resources to limit the potential impact of a compromised device.

Advanced AI Based Monitoring:

Using Large Language Models (LLMs) (e.g., GPT-4) to analyze vast amounts of IoT device data for detecting anomalies and potential security threats in real-time.


OUR DEVICES ARE NOW 100% SECURE.
I TURNED THEM ALL OFF.
HOW DID YOU DO THAT?
© D.Fletcher for CloudTweaks.com

Conclusion

- **Key Points:**
  - Growing Importance.
  - Diverse Threats.
  - Innovative Defenses.

References

- Maiti, A., & Jadliwala, M. (2019). Light ears: Information leakage via smart lights. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, *3*(3), 1-27.
- Kannan, T., Wang, S., Sunog, M., de Mesquita, A. B., Feamster, N., & Hoffmann, H. (2024). Acoustic keystroke leakage on smart televisions. In Network and Distributed System Security Symposium. Internet Society.
- Wijewickrama, R., Abbasihafshejani, M., Maiti, A., & Jadliwala, M. (2023). OverHear: Headphone based Multi-sensor Keystroke Inference. *arXiv preprint arXiv:2311.02288*.
- Intelligence, M. T. (2024, January 31). *Cyber signals issue 3: The convergence of it and OT and the risks to cybersecurity*. Security Insider. https://www.microsoft.com/en-us/security/business/security-insider/reports/cyber-signals/cyber-signals-issue-3-the-convergence-of-it-and-ot.
- Jay, A. (2024, June 6). *Number of internet of things (IOT) connected devices worldwide 2024: Breakdowns, Growth & Predictions*. Financesonline.com. https://financesonline.com/number-of-internet-of-things-connected-devices.
- Lee, I. (2024, May 13). *What are IOT attacks? vectors examples and prevention*. RSS. https://www.wallarm.com/what/iot-attack.
- *Tech 101: Internet of things - U-M Ross Business+Tech*. U. (2023, January 30). https://businesstech.bus.umich.edu/uncategorized/tech-101-internet-of-things.