CYSE 425W CYBERSECURITY STRATEGY AND POLICY

PROF. DEMIREL

RAHIL PATEL

ANDREW HODGES

LEAH DREW

OCT 29, 2022

MIDTERM PROJECT PART I - VIDEO

▶ National governments should impose restrictions on the production, distribution and/or the use of *Internet of Things* devices because powerful companies could easily get access to users' personal information without their knowledge and consent.

▶ Group Alpha will argue in favor of this cybersecurity strategy/policy.

What is IOT?

- The foundation for connecting things, sensors, actuators, and other smart technologies.

- Enabling person-to-object and object-to-object communications.

- 26.6 billion active IoT devices.

- Expected to be 75 billion by 2025.

Communication:

- Driven by various technological forces.
    - Smart devices.
    - Wireless network.
    - Pervasive connectivity.
- More "things or object" connected to the internet than people from anytime.
- Uniquely identifiable objects or "things" with a digital presence

IOT Cloud Platform Vendors

- Three big vendors:
  - Microsoft Azure
    - Azure App Service
  - Amazon Web Services
    - Google IoT Core.
  - Google Cloud
    - Cloud storage to comprehensive development tools

Impacts of IoT on Human life

- IoT has gradually saturated all parts of present-day human life.
  - Needs insurance against dangers and vulnerabilities.
  - IoT devices can be harnessed to wreak havoc on data security.
  - Compromise the privacy of their owner.

Government Consequences of IoT

- Capability to deploy emerging digital technologies is extreme.

- Sensing the needs of the public and the communities.

- Share connections (MAC and IP address).

- Lack of encryption.

- Personal Data Violation.

The risks of Unsecured IoTs

- Losing over $400 billion per year.
- Vulnerabilities in Web Applications.
- Insecure Firmware and Software.
- Extreme amount of Data Generation.
- Critical Terms & Agreement.

Resources

- Chatfield, A. T., & Reddick, C. G. (2019). A framework for Internet of Things-enabled smart government: A case of IoT cybersecurity policies and use cases in US federal government. Government Information Quarterly, 36(2), 346-357.

- Ajiji, Y. M. (2020). Internet of thing (IOT): data and information (gadget protection). Journal of Applied Science, Engineering, Technology, and Education, 2(2), 194-203.

- C. Kotas, T. Naughton and N. Imam, "A comparison of Amazon Web Services and Microsoft Azure cloud platforms for high performance computing," 2018 IEEE International Conference on Consumer Electronics (ICCE), 2018, pp. 1-4, doi: 10.1109/ICCE.2018.8326349.

- Abdel-Basset, M., Manogaran, G., & Mohamed, M. (2018). Internet of Things (IoT) and its impact on supply chain: A framework for building smart, secure and efficient systems. Future Generation Computer Systems, 86(9), 614-628.

- P. Pierleoni, R. Concetti, A. Belli and L. Palma, "Amazon, Google and Microsoft Solutions for IoT: Architectures and a Performance Comparison," in IEEE Access, vol. 8, pp. 5455-5470, 2020, doi: 10.1109/ACCESS.2019.2961511.

THANK YOU

PREPARED BY: RAHIIL PATEL, ANDREW HODGES & LEAH DREW