แบบเสนอหัวข้อ

หัวข้อเทคโนโลยี

ชื่อภาษาไทย: โครงข่ายดาวเทียม

ชื่อภาษาอังกฤษ: Starlink

แหล่งอ้างอิง

1. https://www.digitaltrends.com/computing/what-is-starlink/

2. https://spaceth.co/what-is-spacex-starlink/

3. https://www.starlink.com/technology

สรุปเนื้อหา

Elon musk ผู้นำในวงการเทคโลยีและบริษัท SpaceX ต้องการปฏิวัติระบบเครือข่ายอินเทอร์เน็ตทั่วโลกด้วยนวัตกรรมที่เรียกว่า starlink งานนำเสนอนี้จะอธิบายถึงความเป็นมาและเป้าหมายของ starlink ตามด้วยการอธิบายแนวคิดและภาพรวมหลักการทำงาน รวมถึงวิเคราะห์ข้อดี-ข้อเสียและเปรียบเทียบ starlink กับเครือข่ายประเภทอื่น สรุปสุดท้ายด้วยความเห็นของผู้บรรยายว่า starlink ส่งผลต่อวงการ tech อย่างไร คนธรรมดาอย่างเราจำเป็นจะต้องใช้งานหรือไม่ ปิดท้ายด้วยการคาดเดาอนาคตของนวัตกรรม starlink

เนื้อหาในการนำเสนอภายใน 10 นาที

1. ประเด็นที่ 1 starlink technology คืออะไร, เป้าหมายของ starlink –> ใช้เวลา 2 นาที

2. ประเด็นที่ 2 แนวคิด/หลักการทำงานของ Starlink –> ใช้เวลา 2 นาที

3. ประเด็นที่ 3 ข้อดี – ข้อเสีย –> ใช้เวลา 1 นาที

4. ประเด็นที่ 4 เปรียบเทียบ Starlink กับเครือข่ายประเภทอื่น เช่น fiber optic, 4G-5G, Wi-Fi ใช้เวลา 2 นาที

5. ประเด็นที่ 5 เราทุกคนจำเป็นจะต้องใช้ starlink หรือไม่ + คาดเดาอนาคตของ starlink 1 นาที

แบบเสนอหัวข้อ

หัวข้อเทคโนโลยี

ชื่อภาษาไทย: เทคโนโลยีเครือข่ายแบบไร้สาย มาตรฐาน IEEE 802.11be

ชื่อภาษาอังกฤษ: Wi-Fi 7, IEEE 802.11be

แหล่งอ้างอิง

1. https://www.tp-link.com/th/wifi7/

2. https://www.intel.com/content/www/us/en/products/docs/wireless/wi-fi-7.html

3. https://www.digitaltrends.com/computing/what-is-wifi-7/

สรุปเนื้อหา

Wi-Fi 7 เป็นเทคโนโลยีเครือข่ายไร้สายรุ่นล่าสุดที่พัฒนาต่อจาก Wi-Fi 6 ด้วยเทคโนโลยีที่ล้ำสมัยตามเวลาที่ผ่านไป งานนำเสนอนี้มีเป้าหมายเพื่ออธิบายเทคโนโลยีใน Wi-Fi 7 รวมถึงวิเคราะห์สาเหตุของความหน่วงและระบบความปลอดภัยภายในเครือข่าย พร้อมทั้งเปรียบเทียงความแตกต่างระหว่าง Wi-Fi 7 และเครือข่ายประเภทอื่น ทางผู้จัดทำต้องการอธิบายถึงจุดประสงค์ของ Wi-Fi 7 คือการแก้ไขในสิ่งที่ Wi-Fi 6 ไม่สามารถทำได้ และนำเสนอความเห็นเกี่ยวผลลัพธ์ที่เกิดจากาการเข้ามาของ Wi-Fi 7

เนื้อหาในการนำเสนอภายใน 10 นาที

1. ประเด็นที่ 1 (2 นาที): อธิบายที่มาของ Wi-Fi 7 และความสำคัญของเครือข่าย Wi-Fi

2. ประเด็นที่ 2 (2 นาที): อธิบายเทคโนโลยีที่ใช้ในการพัฒนาความเร็วในการถ่ายโอนข้อมูลของ Wi-Fi 7

3. ประเด็นที่ 3 (2 นาที): วิเคราะห์ความล่าช้า/หน่วง ที่ Wi-Fi 7 จะแก้ไข, ระบบความปลอดภัย

4. ประเด็นที่ 4 (2 นาที): เปรียบเทียบ Wi-Fi 7 กับ Wi-Fi 6 และเครือข่ายประเภทอื่น เช่น 4G-5G, Fiber Optic

5. ประเด็นที่ 5 (1 นาที): การเปลี่ยนแปลง/ผลที่เกิดจากการเข้ามาของ Wi-Fi 7

หัวข้องานวิจัย

ชื่อภาษาไทย: ภัยคุกคาม/ความเสี่ยงที่เกิดจากการใช้เครือข่ายอินเทอร์เน็ต

ชื่อภาษาอังกฤษ: Internet of Threats

แหล่งอ้างอิง

1. https://link.springer.com/article/10.1007/s10669-020-09792-x
2. https://www.researchgate.net/publication/351652228_Internet_of_Things_Meet_Internet_of_Threats_New_Concern_Cyber_Security_Issues_of_Critical_Cyber_Infrastructure

สรุปเนื้อหา

ในช่วงปี 2020-2023 เทคโนโลยีได้พัฒนาและก้าวหน้าในแต่ละวัน นำความสะดวกสบายและความเจริญเข้ามาในชีวิตประจำวัน ยิ่ง IoT ขยายตัวมากขึ้น ความเสี่ยงที่เกิดจากการโจรกรรมยิ่งมีเพิ่มมากขึ้นตาม งานนำเสนอนี้ต้องการที่อธิบายวิธีการประเมินความเสี่ยงที่เกิดจาก IoT ในชีวิตประจำวัน, สรุป 10 อันดับความอันตรายที่เกิดจาก Iot ในปี 2020-2023, อธิบายเทคโนโลยีที่แต่ละองค์กรใช้และวิเคราะห์เหตุการณ์จริงที่เกิดขึ้น พร้อมทั้งนำเสนอความคิดเห็นของผู้บรรยายต่อการจัดการความเสี่ยง

เนื้อหาในการนำเสนอภายใน 10 นาที

1. ประเด็นที่ 1 (2 นาที): เกณฑ์และวิธีที่ใช้ในการวัดความเสี่ยงที่เกิดจาก IoT

2. ประเด็นที่ 2 (1 นาที): สรุป 10 อันดับ IoT Threats ในปี 2020-2023

3. ประเด็นที่ 3 (2 นาที): เทคโนโลยีที่แต่ละองค์กรใช้เพื่อรับมือกับ

4. ประเด็นที่ 4 (2 นาที): วิเคราะห์ Case Study 2 กรณีที่เกิดขึ้นจริง

5. ประเด็นที่ 5 (1 นาที): นำเสนอความเห็นของผู้บรรยายต่อการรับมือความเสี่ยงเหล่านี้

โครงสร้างรายงาน

1. บทนำ ที่มาของปัญหา แรงบันดาลใจ (Introduction)

1.1. ประเด็นที่ 1 (1 หน้า): ที่มาและสาเหตุในการเกิดภัยทาง IoT

1.2. ประเด็นที่ 2 (1 หน้า): เกณฑ์และวิธีที่แต่ละองค์กรใช้ในการคาดการณ์และรับมือความเสี่ยง

2. การทบทวนผลงานที่เกี่ยวข้อง (Related Work)

2.1. ประเด็นที่ 1 (1 หน้า): บทวิเคราะห์การประเมินความเสี่ยงทางอินเทอร์เน็ต (FAIR 2020)

2.2. ประเด็นที่ 2 (1 หน้า): สรุประบบ SCADA Architecture

3. หลักการหรือขั้นตอนวิธีที่ใช้ (Methodology)

3.1. ประเด็นที่ 1 (1 หน้า): Network-based Linear Dependency Modelling.

3.2. ประเด็นที่ 2 (ครึ่งหน้า A4): Functional dependency

3.3. ประเด็นที่ 3 (1 หน้า): Goal-oriented approach with the IoT Micro Mort (IoTMM) model

4. การทดลองและวิเคราะห์ผล (Results)

4.1. ประเด็นที่ 1 (1 หน้า): อธิบายเทคโนโลยีที่แต่ละองค์กรใช้รับมือ

4.2. ประเด็นที่ 2 (2 หน้า): วิเคราะห์เหตุการณ์ที่เกิดขึ้นจริง 2 กรณี

5. บทสรุป ข้อจำกัดของงาน การพัฒนาต่อยอด (Discussion/Conclusion) รวมถึงข้อคิดเห็นที่นิสิตมีต่องานที่อ่านมา

5.1. ประเด็นที่ 1 (ครึ่งหน้า A4): อนาคตของวิธีการรับมือความเสี่ยงบนอินเทอร์เน็ต

5.2. ประเด็นที่ 2 (ครึ่งหน้า A4): ความเห็นของผู้บรรยายที่มีต่อหัวข้อนี้

6. บรรณานุกรม (References)

6.1 Petar Radanliev, David De Roure, Max Van Kleek, Uchenna Ani, Pete Burnap, Eirini Anthi, Jason R. C. Nurse, Omar Santos, Rafael Mantilla Montalvo & La'Treall Maddox (22 November 2020). Environment Systems and Decisions, Dynamic real-time risk analytics of uncontrollable states in complex internet of things systems: cyber risk at the edge. [สืบค้นเมื่อ 10 กรกฎาคม 2566]. https://link.springer.com/article/10.1007/s10669-020-09792-x

6.2 Amir Djenna, S. Harous, Djamel Eddine Saidouni (17 May 2021). Applied Sciences, Internet of Things Meet Internet of Threats: New Concern Cyber Security Issues of Critical Cyber Infrastructure. [สืบค้นเมื่อ 10 กรกฎาคม 2566]. https://www.researchgate.net/publication/351652228_Internet_of_Things_Meet_Internet_of_Threats_New_Concern_Cyber_Security_Issues_of_Critical_Cyber_Infrastructure

6.3 Parag Pathak (23 January 2020). Intelligence & Analytics, What is threat management? [สืบค้นเมื่อ 11 กรกฎาคม 2566]. https://securityintelligence.com/posts/what-is-threat-management-common-challenges-and-best-practices/?_ga=2.187659240.1154429630.1626698768-874142799.1626302503

6.4 Geeta Yadav, Kolin Paul (9 January 2020). Architecture and Security of SCADA Systems : A Review. [สืบค้นเมื่อ 11 กรกฎาคม 2566]. https://www.researchgate.net/publication/338500163_Architecture_and_Security_of_SCADA_Systems_A_Review