Cybersecurity Essentials and Management (Energy Sector)

CSP001

Topic 7/10: Data security and Privacy by design (SDPbd) for the Energy Sector

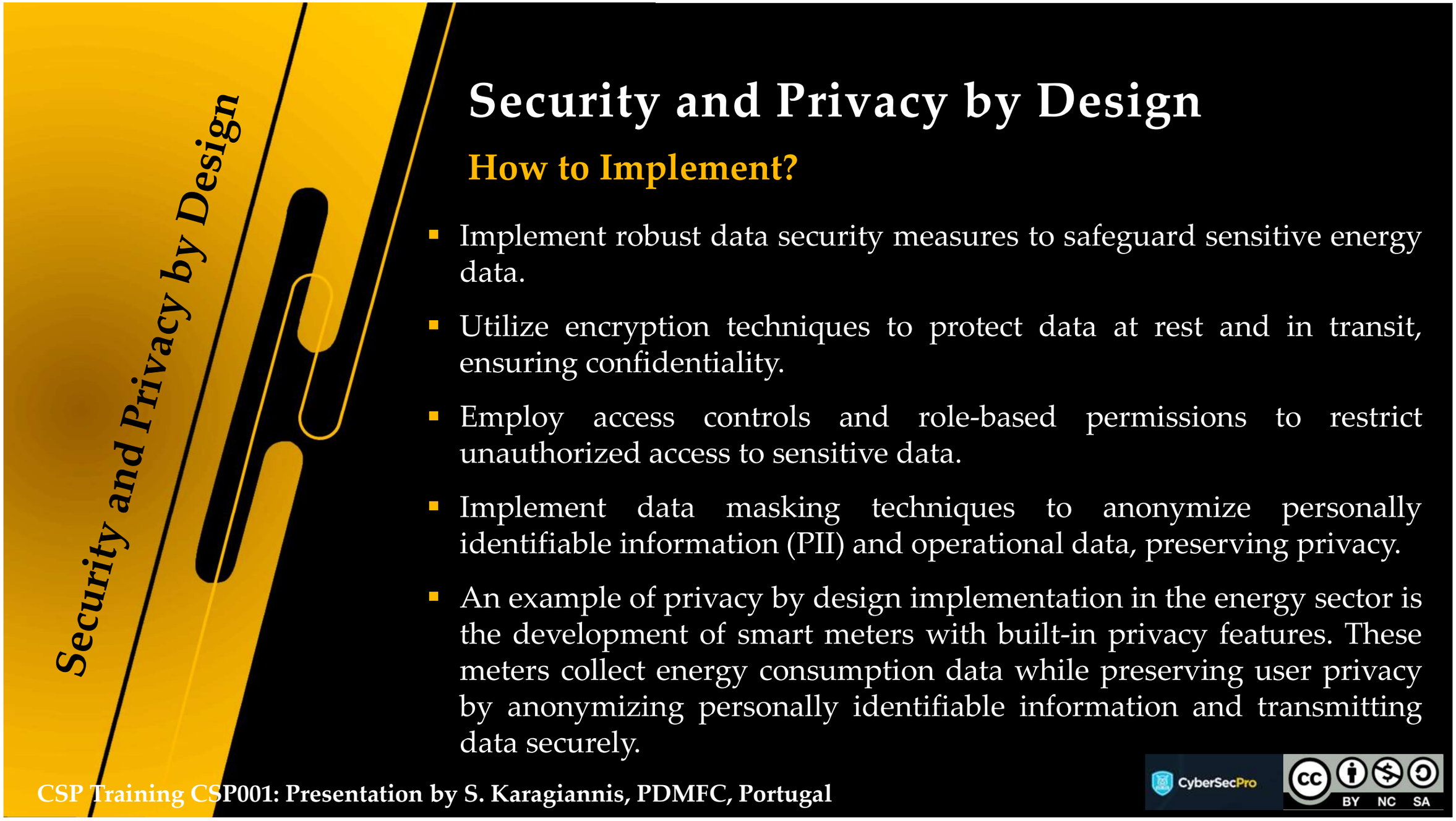
PRESENTATION BY: STYLIANOS KARAGIANNIS (PDMFC, PORTUGAL)

Introduction to SDPbd

Introduction to SDPbd

Data Security and Privacy by Design (SDPbd)

- Data Security and Privacy by Design (SDPbd) is a proactive approach that integrates data security and privacy measures into the design and operation of energy systems right from the outset.
- **Purpose:** The primary goal of SDPbd is to protect sensitive energy data, including personal information and operational data, while ensuring compliance with relevant data privacy regulations and energy cybersecurity guidelines.
- **Importance:** By embedding security and privacy measures into the design phase, SDPbd helps minimize the risk of data breaches and privacy violations, ultimately enhancing trust and confidence in energy systems.



Security and Privacy by Design

How to Implement?

- Implement robust data security measures to safeguard sensitive energy data.
- Utilize encryption techniques to protect data at rest and in transit, ensuring confidentiality.
- Employ access controls and role-based permissions to restrict unauthorized access to sensitive data.
- Implement data masking techniques to anonymize personally identifiable information (PII) and operational data, preserving privacy.
- An example of privacy by design implementation in the energy sector is the development of smart meters with built-in privacy features. These meters collect energy consumption data while preserving user privacy by anonymizing personally identifiable information and transmitting data securely.

Privacy and Threat Intelligence

Importance of Privacy in Threat Intelligence

- Energy companies collaborate through Information Sharing and Analysis Centers (ISACs) to share threat intelligence. However, they must ensure that sensitive information about critical infrastructure vulnerabilities is anonymized or shared selectively to prevent adversaries from exploiting weaknesses.
- **Strategies for Protecting Privacy in Threat Intelligence Sharing:** An energy company participating in an ISAC shares threat indicators related to malware targeting SCADA systems but anonymizes specific details about its own infrastructure to prevent identification by threat actors.

Federated Learning and Privacy

Federated Learning in Energy Domain

- An energy company wants to improve its predictive maintenance system for wind turbines. Instead of centralizing data from all turbines, which could compromise sensitive operational information, they deploy a federated learning approach where models are trained locally on each turbine and only aggregated model updates are shared with the central server.
- Advantages of Federated Learning in Preserving Privacy: By using federated learning, an energy company can train AI models for predicting electricity demand across different regions without accessing individual customer data, preserving consumer privacy while still benefiting from accurate demand forecasting.
- Application of Federated Learning in Energy Sector AI Models: A smart grid operator leverages federated learning to analyze real-time data from distributed sensors across its grid infrastructure to detect anomalies and predict maintenance needs without transmitting sensitive sensor readings over the network, ensuring data privacy and security.

Compliance with Regulations and Guidelines

Regulatory Compliance and Domain Considerations

- Ensure compliance with relevant data privacy regulations such as the General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA), and energy cybersecurity guidelines like the National Institute of Standards and Technology (NIST) Cybersecurity Framework and the International Electrotechnical Commission (IEC) 62443.
- Establish a comprehensive cybersecurity governance framework for energy organizations to effectively manage cybersecurity risks.
- Define roles and responsibilities, policies, and procedures for managing cybersecurity within the organization.
- Designate a cybersecurity champion or team responsible for overseeing and managing cybersecurity initiatives within the organization.
- Select cybersecurity champions with expertise in the energy sector, including knowledge of energy-specific protocols such as Modbus and DNP3, to address domain-specific cybersecurity challenges effectively.

Thank you

Presenter: Stylianos Karagiannis (PDMFC, Portugal)

Please send all questions to:
stylianos.karagiannis@pdmfc.com