CYBERSECURITY: PRINCIPLES AND PRACTICE

Course Description

This course offers a comprehensive overview of essential cybersecurity principles, addressing contemporary security and privacy issues. Participants will gain both theoretical knowledge and practical experience in cryptographic methods, authentication mechanisms, secure access control, and database protection.

Students will also learn to identify and mitigate threats such as malicious software, denial-of-service attacks, and vulnerabilities prevalent in networked environments. Practical laboratory sessions, conducted in an NSA-certified facility, provide hands-on experiences that reinforce key cybersecurity practices.

Designed specifically for Tomas Bata University students, the course prepares participants with essential cybersecurity competencies to effectively manage cyber threats in various professional contexts.

Course Topics

1. Computer Security Concepts
2. User Authentication
3. Cryptographic tools
    - Classical Encryption Techniques
    - Block Ciphers and the Data Encryption Standard (DES)
    - Advanced Encryption Standard (AES)
    - Block Cipher Operation
    - Public-Key Cryptography and RSA
    - Other Public-Key Cryptosystems
    - Cryptographic Hash Functions
    - Message Authentication Codes
    - Digital Signatures
4. Access Control
5. Database and Data Center Security
6. Malicious Software
7. Denial-of-Service Attacks
8. Intrusion Detection
9. Firewalls and Intrusion Prevention Systems
10. Buffer Overflow

Labs

- Lab 1: Run SEED VM on VirtualBox
- Lab 2: Cryptography and Public Key Infrastructure (PKI)
- Lab 3: Linux Capability

- Lab 4 - Port Scanning & Enumeration
- Lab 5: SQL Injection
- Lab 6: XSS Attack
- Lab 7: Attacks on TCP/IP Protocols
- Lab 8: IDS (Snort)
- Lab 9: Linux Firewall
- Lab 10: Buffer Overflow

MACHINE LEARNING

Course Description

In this course, students will gain a solid foundation in machine learning, exploring fundamental concepts such as supervised and unsupervised learning, model evaluation, and algorithm selection. The course covers key techniques including regression, classification, clustering, and dimensionality reduction, with an emphasis on both theoretical understanding and practical application. Students will learn to implement machine learning algorithms using programming languages like Python, applying popular libraries such as scikit-learn and TensorFlow to real-world datasets. Through hands-on projects, students will develop the skills to build, train, and optimize machine learning models. By the end of the course, students will be prepared to tackle machine learning challenges across diverse industries and pursue further study or careers in machine learning and AI.

Course Topics

Completion of at least one programming course, or instructor approval.

(The student should have learned, but not limited to, the following):

1. Introduction to Machine Learning

- What is machine learning?
- Types of learning: Supervised, Unsupervised, Semi-supervised, Reinforcement learning
- Applications of ML

2. Mathematical Foundations

- Linear algebra: vectors, matrices, matrix multiplication
- Calculus: gradients, partial derivatives (for optimization)
- Probability and statistics: distributions, Bayes' theorem
- Optimization: cost/loss functions, gradient descent

3. Data Preprocessing

- Data cleaning and normalization
- Feature scaling (standardization, normalization)
- Feature selection and extraction
- Handling categorical variables (one-hot encoding)
- Train-test split and cross-validation

4. Supervised Learning

Regression

- Linear regression
- Polynomial regression
- Regularization

Classification

- Logistic regression
- k-Nearest Neighbors (k-NN)

- Support Vector Machines (SVM)
- Decision Trees
- Naive Bayes
- Ensemble methods (Random Forests and Gradient Boosting)

5. Model Evaluation and Selection

- Evaluation metrics for regression (MSE, RMSE, R^2)
- Evaluation metrics for classification (Accuracy, Precision, Recall, F1 score)
- Confusion matrix
- Cross-validation
- Bias-variance tradeoff
- Overfitting and underfitting

6. Unsupervised Learning

- Clustering (k-Means)
- Dimensionality reduction (PCA)
- Anomaly detection

7. Neural Networks and Deep Learning

- Perceptron and multilayer perceptrons
- Backpropagation and optimization
- Activation functions
- Deep learning frameworks (TensorFlow, PyTorch basics)

8. Machine Learning Tools and Libraries

- Scikit-learn
- Pandas, NumPy
- Matplotlib, Seaborn
- TensorFlow, Keras, or PyTorch (for deep learning)