# AMHE24 SECURITY ENGINEERING

**UNIT-1 INTRODUCTION TO SECURITY ENGINEERING USABILITY AND PSYCHOLOGY**

1.1 Introduction, A Framework, Example 1–A Bank, Example –A Military Base, Example –A Hospital, Example –The Home, Definitions.

1.2 Attacks Based on Psychology, Pretexting, Phishing, Social Psychology Passwords Naive Password Choice, User Abilities and Training, Design Errors, Operational Issues ,

1.3 Social-Engineering, Attacks, Trusted Path, Phishing Countermeasures, Password Manglers, Client Certs or Specialist Apps, Browser's Password Database ,

1.4 Soft Keyboards, Customer Education, Microsoft Passport, Phishing Alert Toolbars, Two-Factor Authentication, Trusted Computing, Fortified Password Protocols,

1.5 Two-Channel Authentication, The Future of Phishing, System Issues, Attacks on Password Entry, Interface Design, Eavesdropping, Technical Defeats of Password Retry Counters,

1.6 Attacks on Password Storage, One-Way Encryption , Password Cracking

**UNIT-2 ACCESS CONTROL**

2.1 Operating System Access Controls,

2.2 Groups and Roles, Access Control Lists, Unix Operating System Security,

2.3 Apple's OS/X, Windows- Basic Architecture,

2.4 Capabilities, Windows-Added Features Middleware, Database Access Controls, General Middleware Issues, ORBs and Policy Languages,

2.5 Sandboxing and Proof-Carrying Code, Virtualization, Trusted Computing.

**UNIT-3 MULTILEVEL SECURITY**

3.1 Security Policy Model,

3.2 The Bell-LaPadula Security Policy Model ,

3.3 Classifications and Clearances, Information Flow Control, The Standard Criticisms of Bell-LaPadula, Alternative Formulations

3.4 The Biba Model and Vista, Historical Examples of MLS Systems, SCOMP, Blacker MLS Unix and Compartmented Mode Workstations , The NRL Pump ,

3.5 Logistics Systems, Sybard Suite, Wiretap Systems Future MLS Systems, Vista, Linux, Virtualization, Embedded Systems, Composability.

**UNIT-4 MULTILATERAL SECURITY**

4.1 Compartmentation, the Chinese Wall and the BMA Model Compartmentation and the Lattice Model, The Chinese Wall,

4.2 The BMA Model, The Threat Model, The Security Policy, Pilot Implementations

4.3 Current Privacy Issues, Inference Control,

4.4 Basic Problems of Inference Control in Medicine,

4.5 Other Applications of Inference Control, The Theory of Inference Control ,

4.6 Query Set Size Control, Trackers, More Sophisticated Query Controls,

4.7 Cell Suppression, Maximum Order Control and the Lattice Model, Audit Based Control,

4.8 Randomization, Limitations of Generic Approaches, Active Attacks, The Value of Imperfect Protection, The Residual Problem

**UNIT-5 EMISSION SECURITY**

5.1 Technical Surveillance and Countermeasures, Passive Attacks Leakage through Power and Signal Cables, Red/Black Separation, Timing Analysis.

5.2 Power Analysis , Leakage Through RF Signals , Active Attacks, Tempest Viruses , Nonstop , Glitching , Differential Fault Analysis , Combination Attacks ,

5.3 Commercial Exploitation, Defenses, Optical, Acoustic and Thermal Side Channels.

**UNIT-6 SYSTEM EVALUATION AND ASSURANCE**

6.1 Assurance, Perverse Economic Incentives, Project Assurance, Security Testing, Formal Methods, QuisCustodiet, Process Assurance, Assurance Growth,

6.2 Evolution and Security Assurance Evaluation Evaluations by the Relying Party, The Common Criteria, Ways Forward, Hostile Review.

**Reference Book:**

1. Ross Anderson, "Security Engineering - A Guide to Building Dependable Distributed Systems", Wiley, 2nd, 2008.

.