Computer Security and The Internet

CHAPTER 1
SECURITY CONCEPTS AND PRINCIPLES

PRESENTED BY

18701013
18701015
18701019
18701021
18701029
18701043
18701046

Department
Computer Science & Engineering

1.1 Fundamental Goals of Computer Security

What is Computer Security

- Reliability
- Redundancy

Six High-Level Computer Security Goals

- Confidentiality
- Integrity
- Authorization
- Availability
- Authentication
- Accountability

1.2 Computer Security Policies and Attacks

Distinguishing between Two Terms

- Trusted VS Trustworthy
- Confidentiality Vs Privacy and Anonymity

Security-specific terminology

- Assets
- Theory
- Attacks
- Threat
- Controls

Risk: Depends on threat agent, probability of attack, and expected loss.
Risk equation: $R = T.V.C$

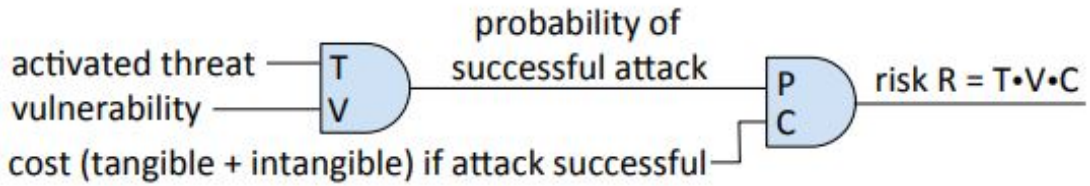

Figure 1: Risk Equation

- Risk Assessment Challenge
- Risk Rating Matrix

C (cost or impact)	P (probability)				
	V.LOW	LOW	MODERATE	HIGH	V.HIGH
V.LOW (negligible)	1	1	1	1	1
LOW (limited)	1	2	2	2	2
MODERATE (serious)	1	2	3	3	3
HIGH (severe or catastrophic)	2	2	3	4	4
V.HIGH (multiply catastrophic)	2	3	4	5	5

Figure 2: Risk Rating Matrix

Adversarial modeling is the technique of **identifying attackers** based on mal-intent and **suspicious behaviors**.

Adversary attributes:

- Objectives
- Methods
- Capabilites
- Funding levels
- Outsider vs Insiders

Security evaluation:

- Black Box Testing
- White Box Testing

Security analysis:

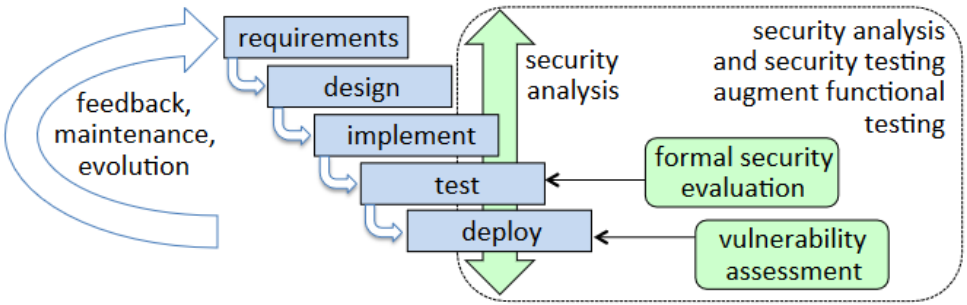

Figure 3: Security analysis and the software development lifecycle.

A threat model identifies **threats**, **threat agents**, and **attack vectors** that the target system considers in scope to defend against—known from the **past**, or **anticipated**.

- Architectural diagrams
- Attack trees
- Stride
- Checklists

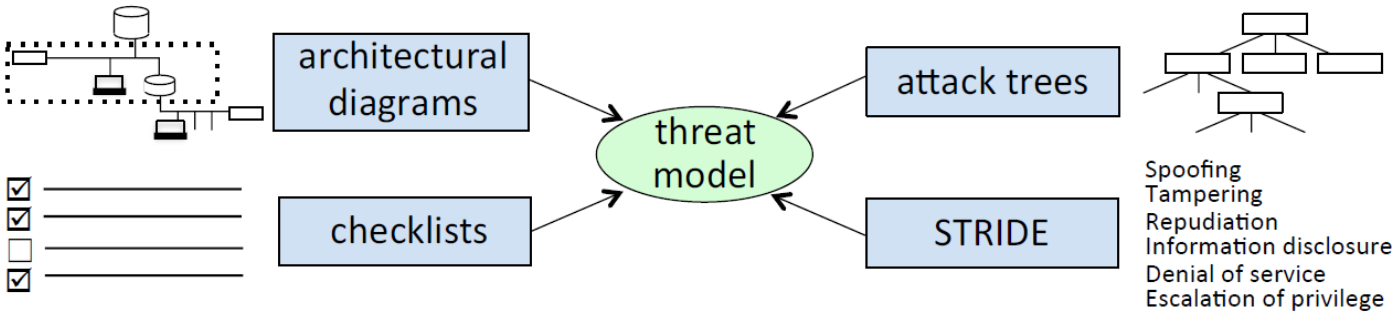

Figure 4: Examples of threat modeling approaches.

Architectural Diagram

- Data flow diagram
- User workflow
- Lifecycle

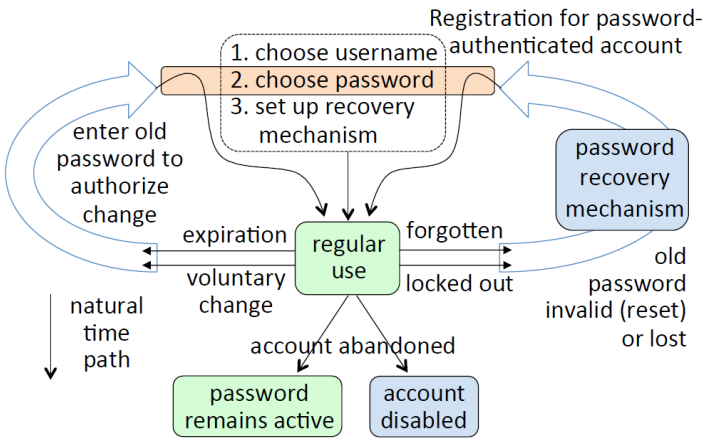

Figure 5: Password-authenticated account lifecycle.

Attack trees

- Attack goal
- Attack vector

Others: Checklist, STRIDE...

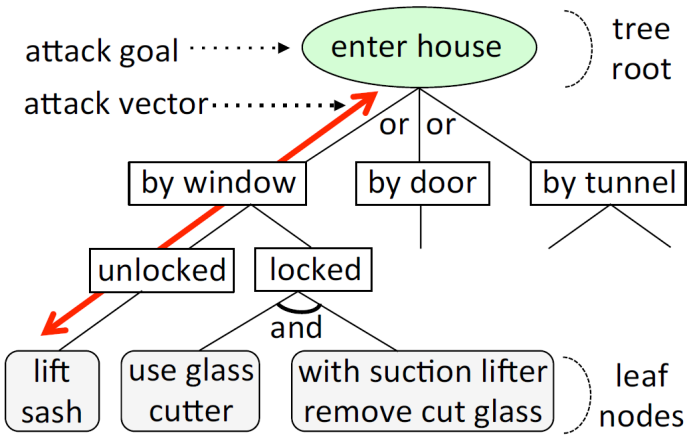

Figure 6: Attack tree.

1.6.Model-reality gaps and real-world outcomes

Quality of a Threat Model

- Invalid assumptions
- Focus on the wrong threats
- Hotel safebox

What is your Threat Model

- Online trading fraud, Phishing one-time passwords, Bypassing perimeter defenses
- Iterative Process: Hard and soft keyloggers

Real Outcomes and Security Analysis

- The security goal is not met
- The resulting system is secure
- An unanticipated simple attack still succeeds

UNIVERSITY OF CHITTAGONG

Security Analysis and Key Questions

- What assets are valuable?
- What potential attacks put them at risk?
- How can potentially damaging actions be stopped?

Others

- Testing is Necessarily Incomplete
- Security is Unobservable
- Assurance is Difficult, Partial

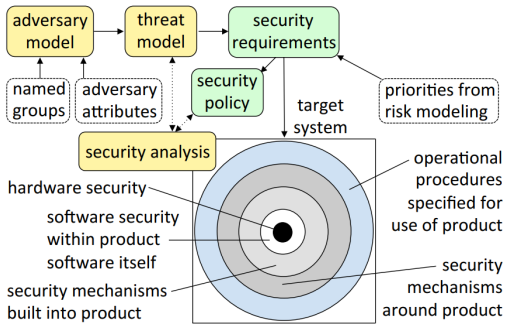

Figure 7: Security analysis in context.

1.7 Design principles for computer security

- Simplicity and Necessity
- Safe Defaults
- Open Design
- Complete Mediation
- Isolated Compartments
- Least Privilege
- Modular Design
- Small Trusted Bases
- Time Tested Tool
- Least Surprise
- User By In
- Sufficient Work Factor
- Defense In Depth
- Evidence Production
- Datatype Validation
- Remnant Removal
- Trust Anchor Justification
- Independent Confirmation
- Request Response Integrity
- Reluctant Allocation

1.8.Why computer security is hard

- intelligent, adaptive adversary
- no rulebook
- defender-attacker asymmetry
- scale of attack
- connectivity
- pace of technology evolution
- software complexity
- developer training and tools
- cost beats quality
- managing secrets is difficult
- non-expert users (human factors)
- security not designed in
- introducing new exposures
- government obstacles


THANK
YOU