Daniel Garcia

ECE 548

Homework 1

1.5 Consider the following general code for allowing access to a resource:

DWORD dwRet = IsAccessAllowed(...);

If (dwRet == ERROR\_ACCESS\_DENIED) {

// Security check failed.

// Inform user that access is denied.

} else {

// Security check OK.

}

1. The security flaw is that the code only denies access for one kind of error, and lets the user in on any other result. How access is allowed is unknown, however it is possible the code to error in unforeseen ways would easily be exploitable by an attacker and allow access to the resource.

DWORD dwRet = IsAccessAllowed(...);

If (dwRet == ACCESS\_GRANTED) {

// Security check OK.

} else {

// Security check failed.

// Inform user that access is denied.

}

This improved version only allows the correct access to the resource. If the IsAccessAllowed function returns any value except for success, then there will be no access to the resource

1.7

Consider a company whose operations are housed in two buildings on the same property, one building is headquarters, the other building contains network and computer services. The property is physically protected by a fence around the perimeter. The only entrance to the property is through the fenced perimeter. In addition to the perimeter fence, physical security consists of a guarded front gate. The local networks are split between the Headquarters’ LAN and the Network Services’ LAN. Internet users connect to the Web server through a firewall. Dial-up users get access to a particular server on the Network Services’ LAN.

Develop an attack tree in which the root node represents disclosure of proprietary secrets. Include physical, social engineering, and technical attacks. The tree may contain both AND and OR nodes. Develop a tree that has at least 15 leaf nodes.

Propriety Secrets

Physical Entrance

Cut Through Fence

Distract Guards

Impersonate Personnel

Web Interface

User Credential Compromise

User surveillance

Theft of token and handwritten notes

Malicious Software Installation (email)

Brute Force attack with PIN calculators

Sniffing

Social Engineering

Spear Phishing

Firewall Compromise

Worm

Trojan

Vulnerability Exploit

Dial-up interface

Man-in-middle attack dial-up connection

Brute Force Credentials