Vienna University of Technology

Department of Software Technology
and Interactive Systems (IFS)

Mag. Dipl.-Ing. Dr. techn. Edgar Weippl

188.366 VU 2.0 Internet Security—A

schriftlich

Nachname																	
Vorname																	
Matrikelnummer								Studienkennzahl				Punkte		Note			

Füllen Sie die obigen Felder aus (Name, Matrikelnummer) und geben Sie die Studienkennzahl der Studienrichtung an, für die Sie diese Prüfung ausgestellt haben wollen. Mit den Fragen auf den nächsten drei Seiten gibt gesamt 50 Punkte zu erreichen.

Viel Glück!

Hinweis: Ein Verlassen der Prüfung nachdem Sie die Angaben bekommen bzw. gesehen haben, ohne Abgabe der Ausarbeitung, wird als negativer Antritt gewertet (Hochschulstudiengesetz).

Wenn Sie Ihre Studienkennzahl auf diesem Bogen falsch angeben, kann kein Zeugnis ausgestellt werden.

1. List and explain some problems with WEP (3pt)

2. Describe SYN cookies! What are SYN cookies needed for? What do they prevent? (3pt)

3. Describe a Smurf attack. (3pt)

4. Describe DNS cache poisoning (3pt)

5. This is the coding construct in DCOM that led to the Blaster worm. What is the problem? Describe the problem and a possible solution. (10pt)

```
HRESULT GetMachineName(WCHAR *pwszPath) {
    WCHAR  wszMachineName[N + 1])
    LPWSTR pwszServerName = wszMachineName;
    while (*pwszPath != L'\\' )
        *pwszServerName++ = *pwszPath++;
    ...
}
```

6. This pseudocode reflects a somewhat common flaw. Imagine this is multithreaded, code-handling sensitive data to be encrypted prior to writing to disk or a network connection. Also, assume that all functions raise exceptions on failure. What is the problem? Describe what can happen and how it can be prevented. Hint: Think Race Condition (FYI: This basically caused a minor bug in the SSL implementation of IIS 4.0) (13pt)

```
Try {
   Byte [] text = AccessPlaintextData();
   Byte [] password = GetPassword();
   Byte [] salt = GetSalt();

   EncryptData(text,password);
   SendEncryptedData(text, salt);

   ScrubSecret(password);
   ScrubSecret(salt);
   ScrubSecret(text);

} Catch() {
   // exception code
}
```

7. ARP (3pt)

   (a) What does ARP mean? What is it for? (1pt)

   (b) On which OSI layer does it operate? (1pt)

   (c) What is RARP? (1pt)

8. HTTP (7pt)

(a) Explain the difference between HTTPS and S-HTTP. (5pt)

(b) On which OSI layers do these protocols operate? (2pt)

9. Firewall (5pt)

(a) On which level does a packet filter operate? What is it do? (2pt)

(b) What is the advantage of stateful inspection? (1pt)

(c) What is SOCKS? (2pt)