

Übung 6

27. November 2007

Aufgabe 1 Schutzziele

Klassifizieren Sie nachfolgende Aussagen als eine Verletzung von Authentizität, Integrität, Vertraulichkeit, Verbindlichkeit, Verfügbarkeit, Privatheit oder eine Kombination derer. Geben Sie eine kurze Begründung an.

1. Ronald schreibt Adis Hausaufgaben ohne dessen Wissen ab.
2. Sascha bringt Christians System zum Absturz.
3. Lars ändert den Betrag auf Claudias Scheck von €100 auf €1000.
4. Frederic fälscht Karlas Unterschrift auf einem Kaufvertrag.
5. Thomas fälscht die IP Adresse von Christophs Rechner, um dessen Daten auf seinen Rechner umzuleiten.
6. Henny registriert die Domain www.eckert.de und lehnt es ab sie an Prof. Eckert zu übertragen.
7. Wolfgang hört das Telefongespräch zwischen Angela und Helmut ab.

Aufgabe 2 Sicherheitsstrategie / Security Policy

Eine Sicherheitsstrategie (engl. Security Policy) legt Schutzziele, Mechanismen, Regeln und Maßnahmen fest, um ein angestrebtes Sicherheitsniveau zu erzielen. Geben Sie für die nachfolgenden Ziele eine geeignete Policy an und durch welche Maßnahmen sie erreicht werden können.

Beispiel:

Die Rechte der Datei die Adis Hausaufgaben enthält, verhindern, dass Ronald sie kopieren und somit betrügen kann.

Policy: Auf Dateien eines Nutzers darf nicht von anderen Nutzern zugegriffen werden.

Mechanismen: Der Administrator gibt nur dem Nutzer Rechte um auf sein privates Verzeichnis zugreifen zu können; z.B. mittels Zugriffskontrollmechanismen wie Access Control Lists (ACLs). Weiterhin können Hausaufgaben Dateien nur im eigenen Verzeichnis des Nutzers abgelegt werden.

1. Nutzer der RBG-Rechner sollen bei ihrem Account Passwörter verwenden, die mindestens fünf Zeichen lang sind und nicht in einem Wörterbuch vorhanden sind.
2. Nach dreimaliger Falscheingabe seines Passworts, darf sich ein Nutzer nicht mehr an den Rechnern der RBG anmelden.
3. Ein Hausaufgabeneinreichungsprogramm schaltet sich automatisch ab, nachdem die Einreichfrist verstrichen ist.
4. Ein Systemadministrator soll in der Lage sein, Studenten die Programme verwenden die das System nach Schwachstellen untersuchen, zu erkennen.

Aufgabe 3 Klassifikation von Sicherheitsmaßnahmen

Sicherheitsmaßnahmen lassen sich grob in drei Klassen einordnen: (1) Prävention, (2) Erkennung und (3) Reaktion.

1. Geben Sie ein Beispiel für eine Situation an, bei dem durch *Prävention* Schäden verhindert werden. Gehen Sie hierbei davon aus, dass falls ein Schaden eingetreten ist, eine nachträgliche Erkennung und Reaktion den Schaden nicht wieder beheben kann.
2. Intuitiv würde man sagen, dass man mit ausreichender Prävention "auf der sicheren Seite ist". In einigen Fällen ist es aber nicht möglich eine ausreichende Prävention durchzuführen und deshalb tritt primär die *Erkennung* (und nachfolgend die Reaktion) in den Vordergrund. Geben Sie hierzu eine Situation an.
3. Geben Sie nun eine Situation an, bei der Prävention und Erkennung eine eher untergeordnete Rolle spielen und die *Reaktion* die wichtigste Komponente darstellt.

Aufgabe 4 Hausübung: Sicherheitsprobleme

In dieser Aufgabe werden Sicherheitsprobleme die durch mangelhafte Identitätsprüfung (Teil 1) und durch fehlende Eingabeüberprüfung (Teil 2) verursacht werden, betrachtet. Als Beispiele dienen hierzu Smurf und Buffer Overflow Angriffe.

Teil 1 Smurf Angriff

Der Smurf Angriff ist ein typisches Beispiel für einen Angriff basierend auf mangelnder Identitätsprüfung. Machen Sie sich mit diesem Angriff vertraut und beantworten Sie folgende Fragen:

1. Wie funktioniert der Smurf Angriff? Erläutern Sie kurz den Ablauf!
2. Was ist das Ziel eines Smurf Angriffs? Welche Schutzziele werden bei einem Smurf Angriff verletzt?
3. Warum ist dieser Angriff möglich?
4. Überlegen Sie sich eine Möglichkeit, wie man solch einen Angriff verhindern könnte!

Teil 2 Buffer Overflow

Der Buffer Overflow (BO) ist eine der am häufigsten auftretende Schwachstelle bei Servern, Routern und PCs. Bei einem BO werden Speicherbereiche (z.B. auf dem Stack oder Heap), die für eine Variable (z.B. Array oder Integer) reserviert sind, mit einem zu großen Wert überschrieben. Dies führt bei dem Speicherbereich (buffer) zu einem Überlauf (overflow). Verursacht werden BOs durch Programmierfehler, bei denen Eingaben unzureichend auf ihre Länge hin überprüft werden.

Auf der nächsten Seite ist ein C-Programm dargestellt, welches anfällig für Buffer Overflows ist. Beantworten Sie folgende Fragen:

1. An welcher Stelle des Programms kann ein BO auftreten?
2. Korrigieren Sie obiges Programm so, dass kein BO mehr auftreten kann!
3. Was ist durch einen BO alles möglich? Welche Schutzziele werden dadurch angegriffen? Geben Sie zu jedem identifizierten Schutzziel ein Beispiel an wie es durch einen BO gefährdet werden kann!

```
int checkPassword( const char *user )
{
    unsigned char givenHash[20];    /* SHA-1 hash of given password */
    unsigned char userHash[20];    /* SHA-1 hash of user password */
    unsigned char pw[64];          /* Given password */

    /* Load the hash value of the user's password
       from the system preferences */
    getUserHash( user, userHash );

    /* Read the password from standard input */
    gets( pw );

    /* Calculate the hash (without preceding newline) */
    SHA1( pw, strlen(pw)-1, givenHash );

    /* Compare the two hashes and return the result */
    return !memcmp( userHash, givenHash, 20 );
}
```

Plagiarismus Der Fachbereich Informatik misst der Einhaltung der Grundregeln der wissenschaftlichen Ethik großen Wert bei. Mit der Abgabe einer Lösung (Hausaufgabe, Programmierprojekt, Diplomarbeit, etc.) bestätigen Sie, dass Sie/Ihre Gruppe der alleinige Autor/die alleinigen Autoren des gesamten Materials sind. Falls Ihnen die Verwendung von Fremdmaterial gestattet war, so müssen Sie dessen Quellen deutlich zitiert haben. Weiterführende Informationen zu diesem Thema finden Sie unter <http://www.informatik.tu-darmstadt.de/Plagiarism>.