Methodische Grundlagen des Software Engineering - Übung 11

11 Dependabilty und IT Security

Abgabe der Hausaufgaben am Anfang der jeweiligen Präsenzübung am 28.06.2011 bzw. 29.06.2011.

11.1 Dependability

11.1.1 Nenne die 4 grundlegenden Verlässlichkeitseigenschaften.

11.1.2 Nenne 2 weitere Systemeigenschaften die manchmal der Verlässlichkeit zugeordnet werden

11.1.3 Erkläre warum ein relativ unzuverlässiges System trotzdem ein hohes Maß an Verfügbarkeit haben kann.

11.1.4 Was ist der Hauptunterschied zwischen den beiden Klassen von unfallsicherheitskritischen Systemen.

11.1.5 Gegeben ist ein medizinisches System das zur Bekämpfung von Tumoren mit gezielter Bestrahlung. Skizziere eine mögliche Gefahr während der Nutzung dieses Geräts und überlege was für eine Softwarefunktionalität das eintreten eines Unfalls auf Basis dieser Gefahr verhindern könnte.

11.2 IT Security

11.2.1 Die in der Vorlesung genannten Sicherheitsanforderungen sind im Allgemeinen unabhängig voneinander. Finde je 3 verschiedene Beispiele aus der physikalischen und digitalen Welt, sodass in jedem dieser 6 Beispiele eine der Anforderungen erfüllt ist, aber die anderen nicht.

11.2.2 Gebe zwei der genannten Sicherheitsanforderungen an, die sich gegenseitig ausschließen.

11.3 Netzwerksicherheit

11.3.1 Nenne 3 Angriffe auf die Netzwerksicherheit die im Internet möglich sind und erkläre sie kurz.

11.3.2 Was versteht man unter der Reichweite von Verschlüsselung und welche Arten kennst du?

11.4 Kryptografie

11.4.1 *Wenn man bedenkt, dass die Menge der möglichen zu verschlüsselnden Texte sehr klein sein kann (z.B. nur die Nachrichten "ja" oder "nein"), welches Problem ergibt sich bei einem deterministischen Public-Key-Verfahren ?*

11.4.2 *Wie kann man das Problem lösen aus 11.4.1?*

11.4.3 *Wieder angenommen, man hat ein deterministisches Verschlüsselungsverfahren, der Verschlüsselungsschlüssel bleibt diesmal geheim. Wenn man annimmt, dass der Schlüssel selten gewechselt wird, und dass sich Plaintexte öfters wiederholen, können teilweise Informationen über einen verschlüsselten Text bekannt werden?*

11.4.4 *Wie kann man das Problem lösen aus 11.4.3?*

11.4.5 *Wie funktionieren digitale Signaturen, welche Probleme gibt es dabei?*

11.4.6 *Der RSA-Signaturalgorithmus D hat die Homomorphie-Eigenschaft, dass gilt:*
D(M1::M2)=D(M1)::D(M2)
für alle Nachrichten M1, M2. Wenn man kein Hash verwenden würde - wie könnte dann ein Angreifer den Geldbetrag in der Signatur D ("Ich schulde Dir 10 EUR.") auf 100 EUR erhöhen, ohne den Algorithmus brechen zu müssen (wenn Zeichenketten Konkatenationen von Zeichen sind)?

Hausaufgabe

11.5 Dependability

11.5.1 Zuverlässigkeit und Unfallsicherheit sind verwandte aber unterschiedliche Eigenschaften. Erkläre die Hauptunterschiede und erläutere wieso ein unfallsicheres System unzuverlässig sein kann und umgekehrt.

1 P

11.6 IT Security

11.6.1 Zeichne einen Angriffsbaum für den unautorisierten Zugriff auf ein Konto beim Internet-Banking. Begründe jeweils warum ein du eine Aktivität als möglich oder unmöglich einstufst und gehe dabei von einem externen Angreifer ohne Insiderwissen aus.

2 P

11.7 Kryptographie

11.7.1 Bei Verwendung von symmetrischer Verschluesselung und gegen einen passiven Angreifer: Wenn man annimmt, dass K1 und K2 verschiedene Schluessel sind, wird die Vertraulichkeit von m...

1. bei Versenden von $\{\{\mathrm{m}\}_{K1}\}_{K2}$::K1 bewahrt ?
2. bei Versenden von $\{\mathrm{m}\}_{K1}$::$\{\mathrm{m}\}_{K2}$::K1 bewahrt ?
3. bei Versenden von $\{\{\mathrm{m}\}_{K1}\}_{K2}$::$\{\mathrm{K1}\}_{K2}$ bewahrt ?

1 P

11.7.2 Die Nachrichten aus 11.7.1 enthalten unnötige Informationen und Verschlüsselungsschritte. Wie sehen die Nachrichten aus wenn man diese weg lässt?

1 P