technische universität dortmund

Prof. Dr. Jan Jürjens, Thomas Ruhroth
Lehrstuhl 14 – Software Engineering
Fakultät für Informatik
SFL – 15.10.2012

# Sicherheit: Fragen und Lösungsansätze – Übung 1

**AUFGABE 1 (Isolation):**

Auf den Folien "Physical/programming-based isolations" wird die Idee der (physikalischen) Isolation am Beispiel eines (vernetzten) Rechensystems vorgestellt. Beschreiben bzw. diskutieren Sie jeweils möglichst präzise,

- was an den mit einem Fragezeichen markierten Stellen voneinander isoliert wird,
- in wessen Verantwortung es liegt, dass diese Isolationen den gewünschten Zweck erfüllen,
- wie ein Angreifer die Isolationen möglicherweise überwinden kann.

**AUFGABE 2 (Ununterscheidbarkeit: Verschlüsselung und Authentifizierung):**

Als Beispiele für Ununterscheidbarkeit haben Sie informationstheoretisch perfekte Verschlüsselung "Example for superimposing randomness: encryption" und Authentifizierung "Example for superimposing randomness: authentication" kennen gelernt.

1. Erläutern Sie möglichst genau, was Ununterscheidbarkeit im Kontext der Verschlüsselung bedeutet. Wie kann für ein Verschlüsselungsverfahren die Eigenschaft der Ununterscheidbarkeit formal gezeigt werden?
2. Betrachten Sie das Verschlüsselungsverfahren in Abbildung 1.
   (a) Zeigen Sie, dass dieses Verschlüsselungsverfahren nicht informationstheoretisch perfekt sicher ist, indem Sie die Ununterscheidbarkeit der Klartexte auf Basis der Schlüsseltexte widerlegen.

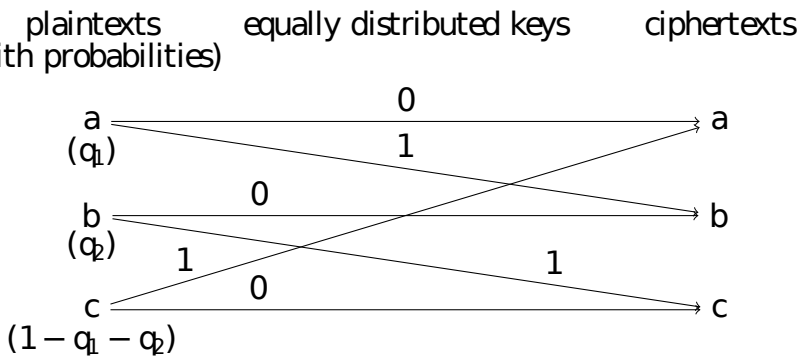


Abbildung 1: Verschlüsselung

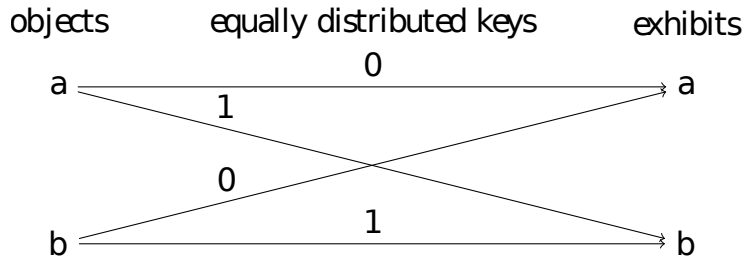


Abbildung 2: Authentifizierung

(b) Erläutern Sie, wie das Verfahren modifiziert werden muss, um informationstheoretisch perfekte Sicherheit zu erreichen.

3. Betrachten Sie das Authentifizierungsverfahren in Abbildung 2, das im Gegensatz zu dem in der Vorlesung vorgestellten Verfahren mit 2 Schlüsseln auskommt. Diskutieren Sie, wie und warum dieses Verfahren angegriffen werden kann. Erläutern Sie dabei genau, was Angriff in diesem Kontext bedeutet.

**AUFGABE 3 (Technische Durchsetzung von Sicherheit):**

Für die drei wichtigsten Grundideen ( "key ideas") zur technischen Durchsetzung von Sicherheit (Redundanz, Isolation und Ununterscheidbarkeit) wird in der Tabelle "Interests and enforcing mechanisms: summary" stichpunktartig dargestellt, welche Sicherheitsinteressen sich jeweils mit welcher kombinierten Technik durchsetzen lassen. Geben Sie zu jedem Interesse zusammen mit der jeweiligen Grundidee und der kombinierten Technik ein konkretes Beispiel an, das die Durchsetzung des Interesses illustriert. Diskutieren Sie auch, wie Ihre Beispiele technisch realisiert werden können.

**AUFGABE 4 (Kontrolle und Überwachung):**

Diskutieren Sie, inwiefern bei dem folgenden Szenario das Konzept der Kontrolle und Überwachung eingesetzt werden kann. Beziehen Sie sich dabei insbesondere auf die Abbildung auf Folie "Local control and monitoring" und versuchen Sie, zu jedem dort verwendeten Begriff eine Entsprechung in dem Szenario zu finden. Der (fiktive) Anbieter Jombo vertreibt Klingeltöne für Mobiltelefone über das Internet. Jeder Benutzer, der Jombo bekannt ist, darf sich pro Monat einen kostenlosen Klingelton herunterladen. Darüber hinaus kann ein Benutzer weitere Klingeltöne käuflich erwerben. Dazu überweist er Geld an Jombo, das dann seinem virtuellen Konto gutgeschrieben wird. Sofern dieses virtuelle Konto gedeckt ist, darf der Benutzer weitere Klingeltöne kaufen und herunterladen.