

IT-Sicherheit in Netzwerken – Praktische Aufgaben 5

Schutzziele, die eng mit der Frage nach Datensicherheit verbunden sind, sind Integrität und Authentizität. Zuerst ist die Zuordnung von Anforderungen zu technisch eingesetzten Lösungen verlangt, die diese Schutzziele gewährleisten sollen. Nach dem Lösen dieser Aufgabe haben Sie eine Übersicht, welche datensichereren Strategien Sie einsetzen können, um das jeweilige Schutzziel zu garantieren.

Um die Gewährleistung von Integrität und Authentizität von Nachrichten genauer zu studieren soll die Anwendung eines symmetrischen und eines asymmetrischen Verschlüsselungsverfahrens studiert werden. Als ein Beispiel für ein symmetrisches Verschlüsselungsverfahren wird der so genannte „Data Encryption Standard“ (DES) betrachtet. Im Rahmen einer Programmieraufgabe lernen Sie etwas über die „Java Cryptography Architecture“. Nach Erledigung der Aufgaben können Sie auf Ihrem Rechner einen Client und einen Server starten, so dass zwischen diesen zwei Teilnehmern eine (daten-)sichere Verbindung aufgebaut werden kann. Des Weiteren haben Sie gelernt, welchen Mehraufwand eine kryptographische Verbindung benötigt. Sie können die Schwachstellen eines symmetrischen Verschlüsselungsverfahrens benennen.

Schutzziele und Datensicherheit

Schutzziele, die im engen Zusammenhang mit der Forderung nach Datensicherheit stehen sind: Integrität und Authentizität. Wenn Integrität und Authentizität zusammen betrachtet werden, dann stellen sie Vertraulichkeit her. Um diese geforderte Vertraulichkeit zwischen zwei Kommunikationspartnern zu gewährleisten sind, müssen verschiedene Elemente eines IT-Systems (im Verbund mit einem Netzwerk) betrachtet werden; d.h. zu untersuchen sind

- i) Integrität von
 - a. Nachrichten
 - b. Clients (Kunden oder Kommunikationspartnern)
 - c. Diensten (die innerhalb eines Netzes oder über das Web bereitgestellt werden)
- ii) Authentizität von
 - a. Nachrichten
 - b. Clients
 - c. Diensten

Vervollständigen Sie die folgende Tabelle, die eine Zuordnung von Verfahren zu Anforderungen aus den Schutzzielen
(Hinweis: Mehrfachnennungen von Verfahren sind möglich)

Tabelle: Zuordnung von Anforderungen zu technischen Lösungen zur Gewährleistung von Schutzzielen – Integrität und Authentizität

Schutzziel	Elemente	Verfahren
Integrität	<i>Nachrichten</i>	DES,
	<i>Clients</i>	Digitale Signaturen,
	<i>Dienste</i>	
Authentizität	<i>Nachrichten</i>	Digitale Signaturen,
	<i>Clients</i>	Zertifizierungen von Schlüsseln,
	<i>Dienste</i>	Autorisierung durch Rechtevergabe (z.B. Schutzmatrix),

Gewährleistung von Datensicherheit – Verschlüsselungsmethoden für Nachrichten

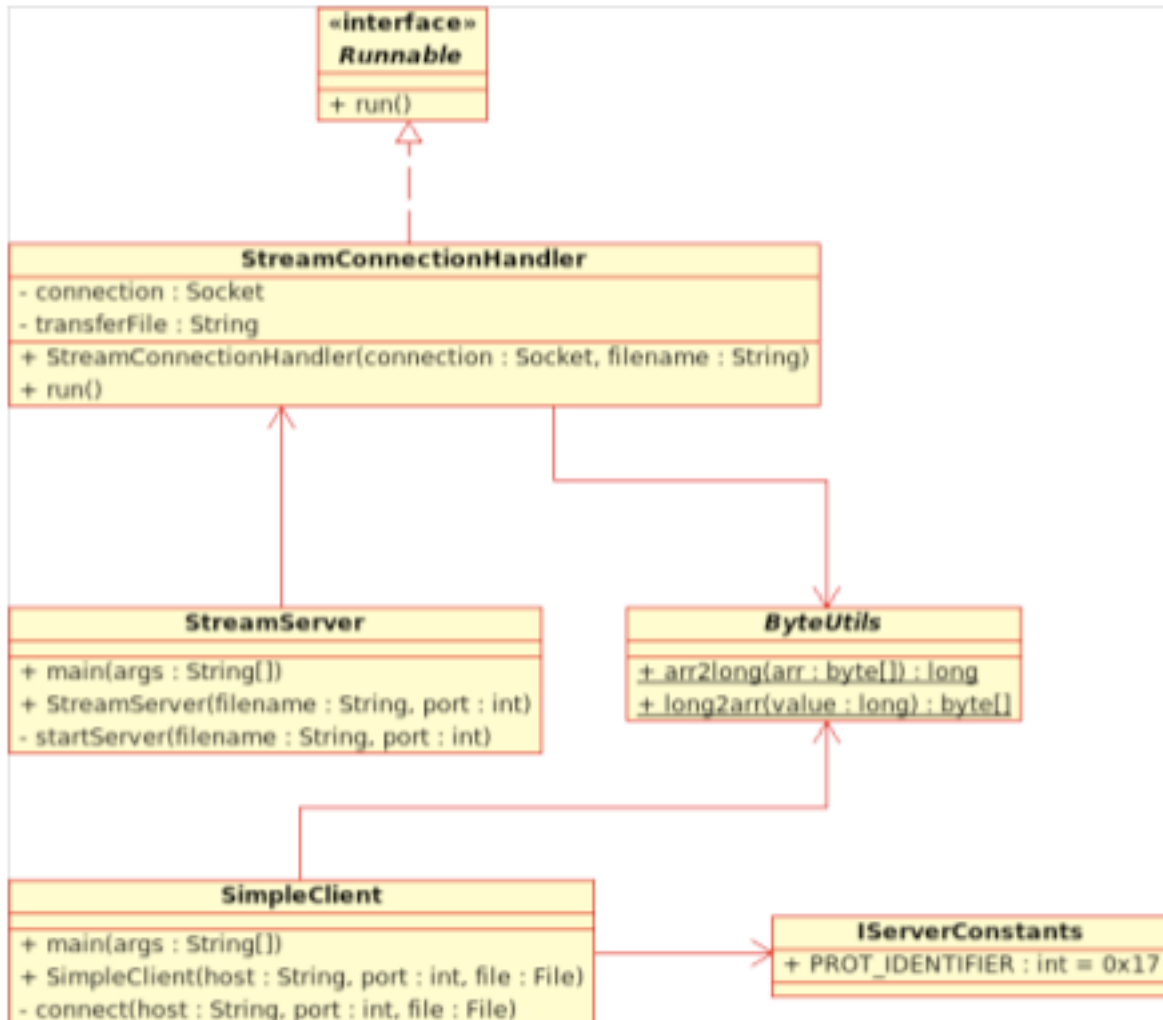
Formen von Angriffen auf Nachrichten

Die Angriffe auf Nachrichten können in aktive und passive Angriffe unterteilt werden. Passive Angriffe beziehen sich auf die Beobachtungen von Kommunikationsflüssen. Einerseits möchte der Angreifer das Kommunikationsverhalten analysieren („wer mit wem wie oft?“) und andererseits vielleicht auch den Inhalt von Nachrichten in Erfahrung bringen. Aktive Angriffe zielen auf vorsätzliche Täuschung und Eindringen in den Kommunikationsprozess. Dabei werden Zugangsschranken (zu einem IT-System und/oder einem Netzwerk) durchbrochen. Weitere Ziele können das Verfälschen des Nachrichtenstroms (Verändern, Vernichten Erzeugen, Vertauschen, Verzögern usw. von Nachrichten). Gleichzeitig werden falsche Identitäten vorgespiegelt. Nach dem Durchbruch von Zugangsschranken ist oftmals auch die mißbräuliche Nutzung von Diensten angestrebt.

Um Nachrichten zu schützen, kann die Strategie gewählt werden, dass eine Verfälschung auffällig wird.

Data Encryption Standard

Betrachten Sie das folgende Java-Programm.



Wie Sie in dem oben angegebenen Klassendiagramm sehen können, besteht das Programm aus zwei wesentlichen Teilen: einem Client und einem Server. Das Programm kann benutzt werden, um Dateien in einem Netzwerk zwischen Client und Server zu versenden, wenn die Kommunikationsstruktur durch TCP unterstützt wird. Wenn Sie den Programmcode analysieren, werden Sie schnell herausfinden, dass der Kommunikationsfluss unsicher ist. Die Daten die zwischen Server und Client geschickt werden, können z.B. „gesniff“ werden. Damit können diese Daten von jedem interpretiert werden, der diese Verbindung abhört.

- 1) Laden Sie den Quellcode von diesem Programm von der ISEC-Seite. Lassen Sie den Client und den Server Code auf der gleichen Maschine laufen. Das Hauptprogramm (main) des Servers ist `nl.fontys.isec.StreamServer`, die main-Klasse des Clients ist `nl.fontys.isec.clientSimpleClient`.

- 2) Nachdem Sie eine Datei unter Benutzung der gegebenen Programme versenden können, analysieren Sie den Quellcode. Betrachten Sie genauer die Klassen `nl.fontys.isec.StreamConnectionHandler` und `nl.fontys.isec.client.SimpleClient`. In diesen beiden Klassen finden Sie die Definition des verwendeten Protokolls und die Übertragungslogik. Beschreiben Sie mit eigenen Worten die proprietäre Protokollstruktur „Simple Single File Transfer Protocol“, die in dieser Implementierung benutzt wird.
- 3) Erweitern Sie das Programm, um die Verwendung eines symmetrischen Verschlüsselungsverfahrens. Für diese Erweiterung ergänzen Sie den `SimpleClient` um die Methode `private InputStream decrypt(InputStream crypteStream)`. Entsprechend muss im `StreamConnectionHandler` des Servers die Methode `private CipherOutputStream encryptStream(OutputStream plainStream)` ergänzt werden.

Hinweis: Wenn Sie Probleme mit der Beispielimplementierung der Anbindung des Clients an den Server haben, dann besteht auch die Möglichkeit ein eigenes Client-Programm zu schreiben. Kennen Sie andere symmetrische kryptographische Verfahren, die ebenfalls hier eingebunden werden könnten?

- 4) Lassen Sie das Programm erneut mit einem jetzt verschlüsselten Kommunikationsfluss laufen. Können Sie eine signifikante zeitliche Differenz bei der Übertragung Ihrer Daten feststellen? Ermitteln Sie entsprechende prozentuale Werte.
- 5) Wo sind die Probleme bei der Anwendung eines symmetrischen kryptographischen Verfahrens? Können Sie sich Angriffsszenarien ausdenken?
- 6) Wenn Sie jetzt eine asymmetrische Verschlüsselung für ein Protokoll zur Dateiübertragung einsetzen, was könnten die Vorteile sein? Welche Probleme würden Sie erwarten? Machen Sie eine Liste, der möglichen Probleme bei Verwendung eines asymmetrischen Verfahrens und überlegen Sie, wie Sie auch diese Probleme lösen können, ohne Sicherheitseinbußen zu haben. Finden Sie ein Beispiel für einen asymmetrischen kryptographischen Algorithmus.