UNIVERSITÄT ZU LÜBECK
INSTITUT FÜR IT-SICHERHEIT

Übungsblatt 1

Cryptography

Abgabe bis 25. April 2023 um 12:00 Uhr im Moodle

Cybersecurity im Sommersemester 2023

Thomas Eisenbarth, Jan Wichelmann, Anja Köhl

Organisatorisches

Der wöchentliche Übungszettel ist spätestens nach der zugehörigen Vorlesung am Dienstag im Moodle verfügbar. Für die Bearbeitung ist eine Woche Zeit, die Lösungen sind als PDF im Moodle einzureichen. Falls neben der eigentlichen Lösung noch andere Dateien abzugeben sind, sollen letztere vorm Hochladen in ein ZIP-Archiv gepackt werden. Die Aufgaben sollen hierbei in Gruppenarbeit zu zweit bearbeitet und abgegeben werden (Dreiergruppen sind nicht möglich). Es genügt, wenn jeweils ein Gruppenmitglied die Abgabe hochlädt.

In den Übungen am Freitag wird dann auf die Lösung einiger Aufgaben des bis dahin korrigierten Übungszettels eingegangen. Diese Übungen bieten ebenfalls die Möglichkeit, Fragen zu Vorlesungsinhalten und kommenden Übungsaufgaben zu klären. Im Anschluss findet dann die Präsenzbearbeitungszeit für das jeweilige Praktikum statt.

Zum Erhalt der Klausurzulassung müssen auf allen außer zwei Übungszetteln jeweils mindestens 50% der möglichen Punkte erreicht werden. Bei der 8-KP-Variante des Moduls ist zusätzlich eine erfolgreiche Teilnahme an den Praktika notwendig.

Einige Aufgaben werden bereits durch das Praktikum abgedeckt und müssen nicht bearbeitet werden, wenn stattdessen das zugehörige Praktikum bestanden wird. Diese Aufgaben sind dann entsprechend markiert. Weitere Details finden sich auf den jeweiligen Übungsblättern.

Einführung

Der Vorstand des Unternehmens *Immature Technical Solutions* (ITS), einem mittelgroßen Anbieter von Cloud- und Hosting-Services mit zahlreichen Industriekunden, bittet Sie um Beratung bei der Umsetzung der neuen und groß angepriesenen *IT-Sicherheits-Offensive*, sprich der Modernisierung der Firmensysteme und -abläufe nach aktuellsten Maßstäben. Die meisten Konzepte und Implementierungen sollen hierbei von firmeneigenen Fachkräften, also meistens unbezahlten Praktikanten, erarbeitet und anschließend von Ihnen auf Tauglichkeit überprüft werden.

Aufgabe 1 Begriffe erklären (6 Punkte)

Bevor überhaupt mit der Modernisierung der Systeme begonnen werden kann, müssen einige Grundbegriffe geklärt werden.

1. Alex und Sam waren neulich bei einer Kryptographie-Fortbildung und sind nun Feuer und Flamme für das Thema. Leider etwas zu feurig und es ist ein erbitterter Streit zwischen ihnen über *symmetrische* und *asymmetrische* Verschlüsselungsverfahren entbrannt, und welches davon besser ist. Schaffen Sie einen Ausgleich, indem Sie jeweils einen Vorteil und einen Nachteil der Verfahrensarten nennen.
2. Erklären Sie den beiden das Konzept hybrider Verschlüsselung. Was ist hierbei der Vorteil?
3. Mackenzie konnte nicht an der Fortbildung teilnehmen und bittet Sie nun die Begriffe MAC und HMAC zu erklären.

Aufgabe 2 Authenticated Encryption (6 Punkte)

Neben den Grundbegriffen muss auch verstanden werden, wie bestimmte kryptographische Techniken einzusetzen sind. In diesem Fall ist die Frage aufgetaucht, wie sich sicherstellen lässt, dass eine verschlüsselte Nachricht auch tatsächlich vom angegebenen Absender stammt und seitdem nicht verändert worden ist – also sowohl vertraulich als auch authentifiziert ist.

Ein Mitarbeiter von ITS hat hier zwei Ansätze entwickelt, die sowohl einfach als auch effizient zu implementieren sind. Er bittet Sie um eine Einschätzung, ob die Verfahren in der Tat beweisbar sicher sind: Die Kollegen in der Implementierungsableitung sind nämlich manchmal etwas eigenwillig und kreativ bei der Wahl konkreter kryptographischer Primitive, was selbst bei kleinen Ungenauigkeiten in der formalen Spezifikation zu einem nicht mehr ganz so kleinen Desaster führen kann.

1. Das einfachste Verfahren, das ihm einfiel, nutzt eine Stromchiffre, um eine Konkatenation von Nachricht m und deren Hashwert zu verschlüsseln und anschließend zu verschicken:

   $$c \leftarrow \mathrm{Enc}_k(m \parallel h(m)).$$

   Hierfür sei $\mathrm{Enc}_k(p) \coloneqq F(k) \oplus p$ eine perfekte symmetrische Stromchiffre, die aus einem festen initialen Schlüssel k einen Schlüsselstrom $F(k)$ generiert und diesen über XOR mit dem Klartext p verknüpft, sodass absolute *Confidentiality* gegeben ist; weiterhin sei h eine kryptographische Hashfunktion.

2. Bei dem zweiten, von ihm *Encrypt-and-Authenticate* genannten Verfahren werden Chiffretext c und eine MAC t parallel abhängig von der Nachricht m berechnet und als Paar $\langle c, t \rangle$ verschickt:

   $$c \leftarrow \mathrm{Enc}_{k_\mathrm{E}}(m), \quad t \leftarrow \mathrm{MAC}_{k_\mathrm{A}}(m).$$

   Hierfür sei $\mathrm{Enc}_{k_\mathrm{E}}$ eine beliebige perfekte Verschlüsselungsfunktion, die ohne Kenntnis des Schlüssels absolute *Confidentiality* bietet; weiterhin stelle $\mathrm{MAC}_{k_\mathrm{A}}$ perfekte *Integrity* und *Authenticity* sicher.

Erfüllen diese Verfahren die *Confidentiality*-Eigenschaft? Betrachten Sie auch den Fall, dass einmal versehentlich ein Nachricht/Chiffretext-Paar $\langle m, c \rangle$ öffentlich wird. Geben Sie jeweils einen Beweis bzw. ein Gegenbeispiel an.

Aufgabe 3 Diffie Hellman (8 Punkte)

Bevor authentifizierte symmetrische Verschlüsselung stattfinden kann, muss erstmal ein Schlüssel ausgetauscht werden. Hierzu bietet sich beispielsweise das Diffie Hellman Key Exchange (DHKE) Verfahren an. Der schon benannte kryptographisch bewanderte Mitarbeiter bittet Sie darum, das Verfahren kurz vorzustellen.

1. Berechnen und beschreiben Sie das DHKE-Verfahren anhand eines Beispiels: $q = 23$, $g = 5$, $A = 4$, $B = 5$.
2. Welche Ordnung hat das Element 2 in $\mathbb{Z}_{23}^*$? Ist es damit ein Generator für $\mathbb{Z}_{23}^*$?
3. Entwerfen und beschreiben Sie ein einfaches asymmetrisches Verschlüsselungsverfahren, das auf demselben Prinzip wie das DHKE-Verfahren beruht.

   Hinweis: Wählen Sie g^A als Alice' Public Key, und A als ihren geheimen Schlüssel. Wie kann Bob ihr nun eine Nachricht senden, die nur sie entschlüsseln kann?