Verschlüsselung

Verschlüsselung ist ein sehr umfangreiches Thema, wir wollen aber hier nicht allzu sehr auf die Details eingehen.

Grundsätzlich bezeichnet Verschlüsselung einen Vorgang, bei dem Daten so verändert werden, dass sie nur noch von Personen wieder in den ursprünglichen Zustand zurückversetzt werden können, die ein passendes Geheimnis haben. Dieses Geheimnis wird üblicherweise als Schlüssel bezeichnet.

Anwendungsfall: Übertragungsverschüsselung

Die Verschlüsselung kann helfen wenn ihr Informationen (wie z.B. ein Passwort oder personenbezogene Daten oder ein Bekenner:innenschreiben) an eine Website sendet. Bei der Übertragung von Daten im Internet ist es nämlich so, dass diese Daten ein kleine Pakete zerteilt werden und dann von einem Gerät im Internet zum nächsten weitergegeben werden. Alle diese Zwischenstationen können sich das Paket genau ansehen. Deswegen werden diese Pakete heutzutage im Web in der Regel verschlüsselt- das seht ihr an dem 'https' (das s steht für secure (sicher) und wird viele Browser zeigen noch ein Schlosssymbol an, um das deutlich zu machen). Diese Art der Verschlüsselung wird 'Übertragungsverschlüsselung' (encryption in transit) genannt- das bezieht sich darauf, dass die Daten bei der Übertragung im Internet verschlüsselt sind. So Übertragungsverschlüsselung gibt es nicht nur im Web sondern auch bei anderen Internetanwendungen, wie zum Beispiel Mail. Hier kommen dann manchmal so Begriffe wie SSL, TLS oder STARTTLS vor. Wenn nun also jemand eure Internetverbindung abhört kann von dem/derjenigen nur nachvollzogen werden, dass ihr eine verschlüsselte Verbindung zu einem bestimmten Server aufbaut, aber nicht mehr welche Daten ihr dort hinschickt oder welche Daten zu euch zurückgeschickt werden. Das können Behörden sein, die wissen wollen was ihr so ans Internet schickt oder welche Artikel ihr online lest. Es kann aber auch euer Internetanbieter sein, der Datenpakete auf dem Weg zu euch verändern will um Werbung einzublenden. Mit Übertragungsverschlüsselung wird der Versuch der Behörden erschwert, weil sie nur noch sehen, welche Seiten ihr euch anseht, aber nicht welche Artikel ihr dort lest (und es wird daran gearbeitet, dass sie auch bald nicht mehr sehen welche Seiten ihr euch anseht). Das Einschleusen von Werbung wird verunmöglicht, weil euer Internetanbieter genau wissen muss wie die Websiten aussehen, um Werbung einzubinden.

Anwendungsfall: Ende-zu-Ende Verschlüsselung

Bei der Übertragungsverschlüsselung werden jedoch nur die einzelnen Verbindungen verschlüsselt. Das heisst, wenn euer Computer zu einem Server Daten schickt, sind diese verschlüsselt, werden dann aber vom Server entschlüsselt, bevor sie verarbeitet oder weitgeschickt werden. Das heisst aber auch, dass der Server die Daten lesen kann. Um das zu verhindern, hat sich das Konzept von Ende-zu-Ende Verschlüsselung durchgesetzt. Hierbei wird dafür gesorgt, dass wirklich nur die Person, an die die Nachricht addressiert ist, diese auch lesen kann. Diese Art der Verschlüsselung ersetzt die Übertragungsverschlüsselung nicht, wird aber oft obendrauf noch zusätzlich verwendet.

Anwendungsfall: Verschlüsselung von 'ruhenden' Daten

Im Gegensatz zu Übertragungsverschlüsselung ist es auch wichtig, Daten zu verschlüsseln wenn sie einfach nur auf einem Datenträger gespeichert werden. Das verhindert, dass eure privaten Urlaubsfotos in die falschen Hände geraten wenn ihr einen USB-Stick verliert oder dass die Behörden sehen, was ihr so auf eurem Computer oder Smartphone treibt wenn sie den mal mitnehmen. In der Regel werden dabei die Daten so verschlüsselt, dass sie nur mit einem Passwort gelesen werden können.

Verschlüsselungsverfahren

Bei der Verschlüsselung von Daten wird zwischen zwei unterschiedlichen Verfahren unterschieden, nämlich der symmetrischen Verschlüsselung und der asymmetrischen Verschlüsselung (eigentlich wird von symmetrischer und asymetrischer Kryptographie gesprochen, die Verschlüsselung ist dabei nur eine mögliche Anwendung der Kryptographie). Bei symmetrischer Verschlüsselung ist das Geheimnis, mit dem die Daten verschlüsselt und entschlüsselt werden dasselbe. Diese Art kommt üblicherweise bei 'ruhenden' Daten zum Einsatz- zum Beispiel wenn ihr eure Festplatte verschlüsselt oder wenn oft auch wenn Programme die Möglichkeit bieten, eine Datei mit einem Passwort zu schützen. Die symmetrische Verschlüsselung hat aber einen grossen Nachteil: wenn ich mit vielen Menschen verschlüsselt kommunizieren will, muss ich mir für jede Kommunikationspartner:in einen eigenen Schlüssel ausmachen. Deswegen wurde asymmetrische Kryptographie erfunden, um dieses Schlüsselchaos zu vereinfachen: hierbei hat jede Person einen öffentlichen und einen geheimen Schlüssel. Der öffentliche ist dazu da, um Daten zu verschlüsseln, der geheime ist dazu um die Daten die mit dem öffentlichen verschlüsselt wurden zu entschlüsseln. Der öffentliche Schlüssel kann (und soll) hierbei auch wirklich öffentlich sein, also z.B. im Internet veröffentlicht werden. Dieser kann dann von wem auch immer verwendet werden um Nachrichten für die Person, zu der dieser öffentliche Schlüssel gehört, zu verschlüsseln. Entschlüsselt werden können diese Nachrichten nur mit dem geheimen Schlüssel. Dieses Verfahren wird üblicherweise bei Übertragungsverschlüsselung und Ende-zu-Ende-Verschlüsselung angewandt.

Hintergrund zum Thema Kryptographie

Verschlüsselung ist ein wichtiges Mittel um Daten vor unbefugem Zugriff zu schützen. Verschlüsselung ist Teil des Themenfeldes Kryptographie und da Kryptographie sich auch mit anderen Punkten beschäftigt, die in der IT Sicherheit von Bedeutung sind, wollen wir hier noch etwas genauer darauf eingehen.

Viele Menschen beschäftigten sich über die Jahrunderte mit dem Thema der Informationssicherheit und wie Informationen übertragen werden können, ohne das Unberechtigte darauf Zugriff erlangen können. Meist wurden diese Mittel von Militär und Staat genutzt und dementsprechend kam auch lange Zeit ein Grossteil der Forschung zu Kryptographie aus diesem Feld. Erst seit dem Ende des 20. Jahrhunderts und mit dem Aufkommen der Digitalisierung und der Verbreitung des Internets beschäftigen sich immer mehr Forscher:innen mit dem Thema.

Lange Zeit war es üblich, dass die Verfahren, wie die Verschlüsselung funktioniert, geheim gehalten wurden. Ende des 19. Jahrhunderts wurde das Kerckhoffsche Prinzip formuliert. Dieses besagt, dass sie Sicherheit eines kryptographischen Verfahren NICHT davon abhängen darf, dass das Verfahren selbst geheimgehalten wird, sondern nur von der Geheimhaltung des Schlüssels. Alle heutzutage

üblichen kryptographischen Algorithmen sind öffentlich. Welche Verschlüsselungsalgorithmen verwendet werden wird meist von Standardisierungsorganisationen in einem öffentlichen Verfahren beschlossen. Teilweise gibt es hier sogar Wettbewerbe, bei denen verschiedene Algorithmen von Wissenschafter:innen eingereicht werden und diese dann gegenseitig geprüft werden. Zum Beispiel wurde des Verfahren AES (Advanced Encryption Standard) in so einem Ausschreibungsverfahren Ende der 90er Jahre gefunden und ist seitdem sozusagen der Standardalgorithmus für symmetrische Verschlüsselung. AES ist so gängig, dass die Prozessoren die in heutigen Computern eingebaut sind so gebaut sind, dass sie eine spezielle Funktion haben um AES schneller zu berechnen. AES ist auch bei den meisten Programmen für Festplattenverschlüsselung das Standardverfahren. Dennoch gibt es auch einige andere Verfahren, die Möglicherweise in gewissen Situationen Vorteile bringen können. Üblicherweise sollten aber die Standardverfahren die meiste Sicherheit bringen. Auch bei der asymmetrischen Kryptographie gibt es Algorithmen die weiter verbreitet sind, wie zum Beispiel der Algorithmus RSA. Hier tut sich etwas mehr, da in den letzten Jahrzehnten neue Verfahren gefunden wurden die auf anderen mathematischen Prinzpien beruhen.

Anwendungsfälle von Kryptographie abseits von Verschlüsselung

Kryptographische Algorithmen können nicht nur für Verschlüsselung verwendet werden. Zwei weitere wichtige Vorteile die Kryptographie bieten kann sind die Überprüfbarkeit von Authentizität sowie von Integrität von Nachrichten. Authentizität bedeutet, dass eine Nachrichte kryptographisch 'signiert' werden kann, damit die Empfänger:in sich über die Absender:in sicher sein kann. Integrität hingegen bedeutet, dass die Nachricht bei der Übertragung nicht verändert wurde. Meistens werden verschiede Algorithmen kombiniert um Vertraulichkeit, Integrität und Authentizität zu erreichen.

Das grosse Problem der Schlüsselverwaltung

Wenn Nachrichten verschlüsselt und signiert übertragen werden sollen, müssen die Beteiligten irgendwie zunächst die Schlüssel austauschen. Hierfür gibt es verschiedene Ansätze- einige von euch kennen vielleicht die Schlüsselserver die bei der Emailverschlüsselung verwendet werden. Hier können Anwender:innen ihre öffentlichen Schlüssel hochladen und andere können diese dann herunterladen und gleich verschlüsseln beziehungsweise Signaturen überprüfen. Aber wie überprüfen sie ob sie den richtigen Schlüssel heruntegeladen haben? Dafür muss dann der Fingerabdruck des Schlüssels überprüft werden. Das ist ein sehr mühsames Konzept und hat immer wieder zu Problemen geführt. Mittlerweile gehen viele Programme dazu über immer den eigenen öffentlichen Schlüssel mitzuschicken und die Gegenseite importiert den dann automatisch und markiert ihn als gültig. Nur wenn dann eine Nachricht mit einer anderen Signatur kommt, gibt es eine Warnung.

Empfehlenswerterter Artikel (eng): zu Verschlüsselung:
https://ssd.eff.org/en/module/what-should-i-know-about-encryption