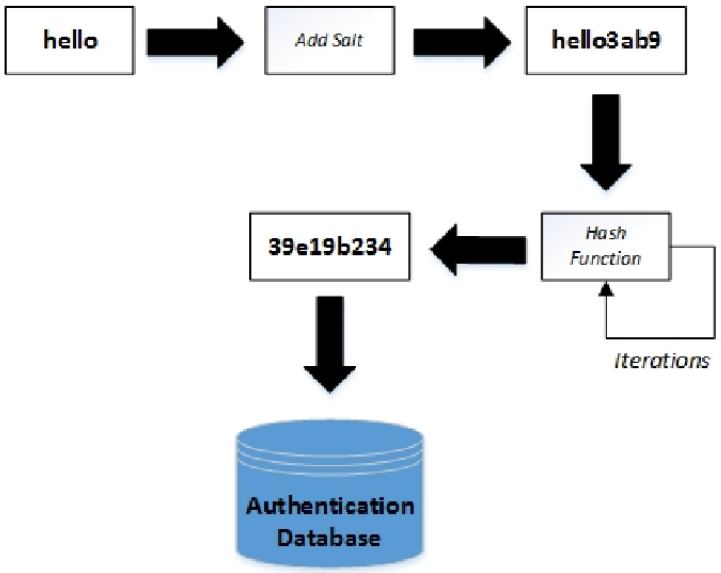
Salt:

Einführung:
Salts kommen zum Einsatz, um Angriffe auf gehashte Passwörter und Informationen zu erschweren wie z.B durch Rainbow Tables. Bei Salts handelt es sich um eine zufällige Zeichenkette, die vor das gehashte Passwort (Klartext) hinzugefügt wird. Die erzeugten Hash-Werte unterscheiden sich von den ohne Salt hinzugefügten Hash-Werten und so damit nicht vom Rainbow-Table ermittelt werden kann.

Definition:
Salt, ist eine zufällige Zeichenkette, die für kryptografische Hashfunktionen zum Einsatz kommt. Typisch wird Salt beim Hashen von Passwörtern verwendet, welche es Angriffen erschweren, diese zu knacken, da der Hash sich vom vorherigen Hash ohne Salt unterscheidet, dies ist auch bekannt als “versalzen”.

Die Passwörter, welche einen Salz-Hash-Zusatz besitzen, werden auch teilweise als gesalzene Passwörter bezeichnet. In der Datenbank befinden sich dann nur der Hash-Wert und der Salt und kein Klartext Passwort.



Einsatz von Salts:
Das Hashing schützt leider nicht vor dem Ermitteln von Passwörtern durch Rainbow-Tabellen. Ein Angreifer muss nur die Hash-Werte aus der Tabelle mit den Werten aus der Datenbank verglichen und hat damit Zugriff auf die Daten.

Ein Salt schützt genau vor dieser Angriffsmethode. Indem vor dem Anwenden der Hashfunktion dem Klartextpasswort eine zufällig erzeugte Zeichenkette angefügt wird, womit man den Rückschluss über Rainbow-Tabellen unmöglich macht.

Salt kann auch in der Kombination mit Pepper auftreten. Pepper ist gleich wie Salt eine zufällige Zeichenkette, die beim Hashing angehängt wird. Allerdings wird ein Pepper im Gegensatz zum Salt getrennt von den Daten und den Hash-Werten an einem sicheren Ort gespeichert. Bei einem Angriff bleibt daher der Pepper vom Angreifer unbekannt.

Probleme:

Salt bildet anhand eines Programmierfehlers oder fehlerhafter Implementierung nur eine Anzahl von 1000 unterschiedlichen Salts, weshalb sich auch die Rainbow Tabelle immer noch lohnen. Diese Fälle werden als “schwache” Salts bezeichnet. Diese Probleme fanden oft in Windows-Systemen statt, wie Windows Vista und XP, wobei der Benutzername gesalzen wurde und man durch Rainbow Tabellen Zugriff auf den Computer sich schaffen konnte.

Gegen Brute-Force-Angriffe oder Wörterbuchangriffe, bei denen für verschiedene Eingaben geprüft wird, ob sie zum Hashwert passen, hat ein Salt keine sicherheit steigernde Wirkung. Weshalb Salt bei diesen Angriffen wenig wirksam ist.

Praxis

In der Praxis sieht es jedoch leider so aus, dass viele Entwickler zwar bewusst sind, dass sie Passwörter salzen sollten, doch weicht die Meinung der Umsetzung stark voneinander ab und teilweise führt es dann zu falsch verwendeten Salts, welche sich dann negativ auswirken können, obwohl es als gut gemeinten Schutz verwendet werden sollte.

Angriffe:

Angriffe aufgrund der Softwareimplementierung:

Rainbow Tabellen - Benutzt einen spezielle Datenstruktur um das gehashte Passwort in der Datenbank zu knacken. Rainbow Table beinhalten eine Vielzahl von vorberechneten Paaren bestehend aus Passwörtern und zufälligen Hash-Werten.

Pufferüberlauf - Durch das Senden von zu großen Dateien wird über den Puffer hinaus geschrieben und dabei womöglich andere Daten überschrieben

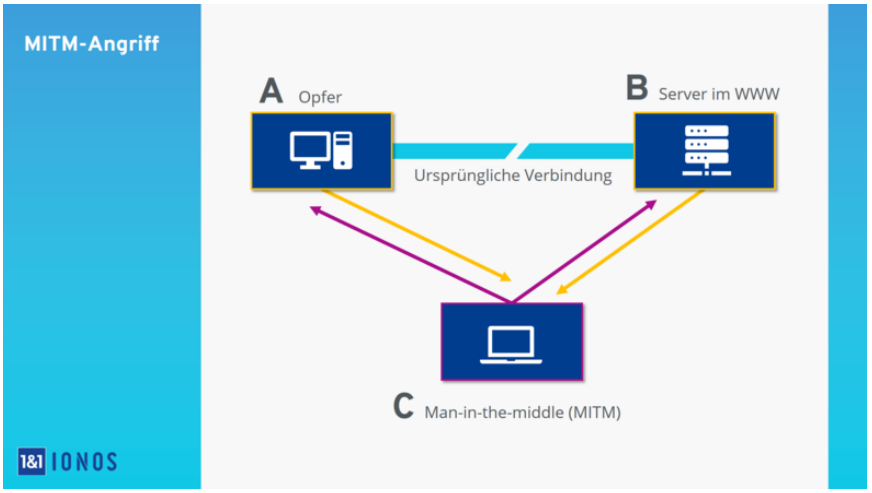
Stack Smashing - Hierbei werden durch den Pufferüberlauf Routinen eingeschleust und es kann zu Exploits kommen

Formatstring-Angriffe - Bei der Eingabe von Benutzerinformationen kann man diese Eingaben nutzen um bestimmte Prozesse im Hintergrund zu starten (SQL-injection)

Wörterbuchangriff - Bei einem Wörterbuchangriff wird eine Wörterliste systematisch durchprobiert, um in den Computer oder Server einzubrechen. Wörterbuchangriffe können auch genutzt werden, um Schlüssel für eine verschlüsselte NAchricht oder ein verschlüsseltes Dokument zu finden

Angriffe auf Netzwerkprotokolle:

Man-in-the-Middle - Der Angreifer sitzt physisch bzw. logisch zwischen zwei kommunizierenden Komponenten, wobei der Angreifer die Informationen erhält und andere Informationen weiter schicken kann. Der Angreifer probiert die Informationen unbemerkt abfangen, zu lesen und Falschinformationen weiter zu schicken.



Tunneling - Ein gesamter Datenverkehr wird wie in einem Tunnel abgeschirmt und die “Unterhaltung” wird gehalten als wäre sie in einem bestimmten Protokoll.

Angriffe auf Netzstrukturen:
DOS - Überlasten eines Netzes durch zu viele Angriffe
DDOS ist der Angriff durch mehrere Rechner auch genannt Botnetz

Tarnung eines Angriffes:
Spoofing: verfälschen der Absenderadresse
Fragmentieren von Paketen -> Der Angreifer kann schwerer gefunden werden.

Weitere Möglichkeiten des Angriffs:

- Social Engineering
- Nicht-prüfung externer Dateien -> Einschleusung Schadsoftware
- Spam-mails
- Phishing
- Würmer, Trojanische Pferde, Dialer oder Viren