ISF HS 2019

Victor Fernández
Pavaskar Parameswaran

Dezember 2019

Vorwort

Diese Zusammenfassung entstand in einer Gruppe während der Lernphase des HS 2019. Alle Fragen aus der Stoffabgrenzung tragen eine blaue Farbe und stehen als Unterkapitel. Das Dokument ist Open Source und jeder der möchte und signifikant beiträgt, darf sich als Autor anhängen. Die Source ist dieses GitHub-Repo[1]. Dies ist mein erstes LaTeX-Dokument überhaupt. Nichts desto trotz wurde auf eine klare Strukturierung und Lesbarkeit des Dokumentes Wert gelegt.

Inhaltsverzeichnis

[1] https://github.com/vigi86/HSLU_Zusammenfassungen/tree/master/ISF_HS19

Teil I
Einführung (SW 01)

1 Einführung

Einführung in das Thema „Management von Informationssicherheit“

Daten, Information und Wissen Information ist die Verknüpfung von Daten in Form von Zahlen, Worten und Fakten zu interpretierbaren Zusammenhängen. Durch die Vernetzung von Informationen entsteht Wissen, das zunächst personenbezogen ist.

Missbrauch Informationen müssen vor Missbrauch geschützt werden

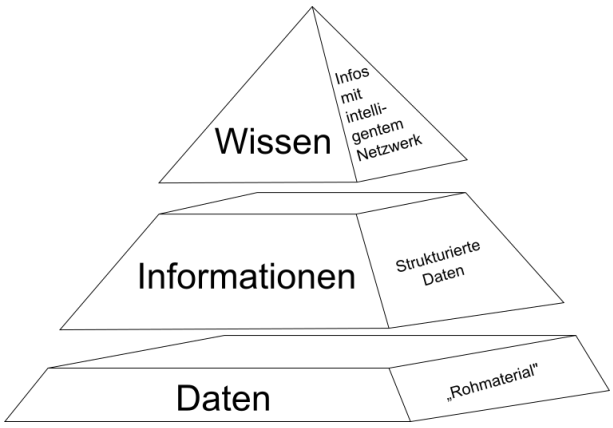

Abbildung 1: Wissenspyramide (Wikipedia)

Motivation / Bedrohungen

Was gefährdet die Informationen? Welche Gefährdungen/Bedrohungen gibt es?

- Nicht vorsätzliche (zufällige) Gefährdungen/Bedrohungen
  - Naturgewalten (Blitz, Hagel, Unwetter, Erdrutsche, Hochwasser, etc.)
  - Ausfall von Strom oder Telekommunikation
  - Technische Pannen, z.B. Fehler von Hard- und/oder Software
  - Bedienerfehler / Fahrlässigkeit der Mitarbeitenden
- Vorsätzliche Gefährdungen/Bedrohungen
  - Bösartiger Code (Viren, Würmer, Trojaner, etc.)
  - Informationsdiebstahl
  - Angriffe (von Skript-Kiddies bis Hacker)
  - Wirtschaftsspionage („was die Konkurrenz wissen möchte“)
  - Missbrauch der IT-Infrastruktur

Grundbegriffe

Zutritts-, Zugangs-, Zugriffskontrolle

- ***Zutrittskontrolle:*** Schutz des physischen Systems (Bsp. Serverraum)
- ***Zugangskontrolle:*** Schutz des logischen Systems (Bsp. Betriebssystem)
- ***Zugriffskontrolle:*** Daten-bezogen; Schutz der Operationen (Bsp. Dateisystem)

Teil II
Kryptographie (SW 02-04)

2 Symmetrische Kryptographie

Sie verstehen was Steganographie ist

Steganographie Verstecken von Information, z.B. in Bildern oder Audiofiles.

Sie verstehen was Private-Key-Kryptographie ist, welche Arten von Sicherheit es gibt und welche Angriffsarten auf Verschlüsselung existieren

Zeichencodierung Kodierung (=Encoding) heisst, einen Wert mit Symbolen eines Zeichensatzes darzustellen. Beispiel:

Dezimalsystem	100
Binärsystem	1100100
Hexadezimalsystem ('hex')	64
ASCII	hello
Base64	aGVsbG8=

Achtung: Kodierung $\neq$ Verschlüsselung

Symmetrische Verschlüsselung Bei symmetrischen Verschlüsselungsverfahren gibt es im Gegensatz zu den asymmetrischen Verfahren, **nur einen einzigen Schlüssel**. Dieser Schlüssel ist für die Verschlüsselung, als auch für die Entschlüsselung zuständig.

Secret Key Verschlüsselung Secret Key ('Symmetrische') Verschlüsselung wird zwischen zwei Parteien verwendet, welche einen **gemeinsamen Schlüssel** besitzen. Ausserdem wird sie oft verwendet, wenn der gleiche Benutzer ein Dokument verschlüsseln und zu einem späteren Zeitpunkt wieder entschlüsseln muss.

TODO BILD

Private Key: Ein Kennwort, das benutzt wird, um einen Klartext zu verschlüsseln und so einen Geheimtext zu erhalten.

TODO BILDER
Jeder kann den öffentlichen Schlüssel zum Verschlüsseln verwenden. Nur der Besitzer des privaten Schlüssels kann entschlüsseln.

Sie können „klassische" symmetrische Verschlüsselungverfahren wie Ceasar cipher, Vigenère cipher, one-time pad anwenden und verstehen die Vor- und Nachteile bzw. Schwachstellen dieser Verfahren

Cesar cipher Caesar-Verschlüsselung ist ein einfaches symmetrisches Verschlüsselungsverfahren, das auf der monographischen und monoalphabetischen Substitution basiert.
Vorteil: es ist **einfach**.
Nachteil: es ist **unsicher**, da es sehr schnell geknackt werden kann.
Schwachstelle: Die in der natürlichen Sprache ungleiche Verteilung der Buchstaben wird durch diese Art der Verschlüsselung nicht verborgen, so dass eine Häufigkeitsanalyse (Frequenzanalyse) das Wirken einer einfachen monoalphabetischen Substitution enthüllt.

TODO BILD: Schematische Darstellung einer Verschiebechiffre mit Verschiebung um 3 Buchstaben.

Das folgende Diagramm zeigt die Häufigkeitsverteilung der Buchstaben in einem längeren Text in deutscher Sprache:

TODO BILD

TODO Wie zu erwarten, ist der häufigste Buchstabe E, gefolgt von N und I, wie es im Deutschen üblicherweise der Fall ist. Wird der Text mit dem Schlüssel 10 (oder anders gesagt, mit dem Schlüsselbuchstaben J) chiffriert, erhält man einen Geheimtext, der folgende Häufigkeitsverteilung besitzt: (BILD)

Der häufigste Buchstabe ist hier O, gefolgt von X und S. Man erkennt auf den ersten Blick die Verschiebung des deutschen „Häufigkeitsgebirges“ um zehn Stellen nach hinten und besitzt damit den Schlüssel. Voraussetzung ist lediglich, dass man die Verteilung der Zeichen des Urtextes vorhersagen kann.

Besitzt man diese Information nicht oder möchte man auf die Häufigkeitsanalyse verzichten, kann man auch die Tatsache ausnutzen, dass bei der Cäsar-Chiffre nur eine sehr kleine Anzahl möglicher Schlüssel in Frage kommt. Da die Größe des Schlüsselraums nur 25 beträgt, was einer „Schlüssellänge“ von nicht einmal 5 bit entspricht, liegt nach Ausprobieren spätestens nach dem 25. Versuch der Klartext vor.

Cesar cipher: Vorgang
- Verschiebt jeden Buchstaben des Alphabets um eine bestimmte Anzahl Stellen
- Soll bereits von Julius Caesar verwendet worden sein
- Der Schlüssel wird entweder als Anzahl Stellen, um die verschoben wird, oder als Buchstaben, auf den ‘A’ verschoben wird angegeben
- Variante: ROT13 (Verschlüsselung = Entschlüsselung)
- Problem 1: Schlüssellänge (nur 26 verschiedene Schlüssel)
- Problem 2: Frequenzanalyse

TODO BILD aus Folie mit Cesar Verschiebung

Vigenère cipher
- Schlüssel: Wort der Länge L
- Jeder Buchstabe im Text wird mit der Cesar cipher des entsprechenden Schlüsselwortes verschlüsselt
- Anzahl mögliche Schlüssel: 26^L
- Problem: Frequenzanalyse jeder L’ten Stelle

TODO BILD Vigenère cipher

One-time pad
- Jede Stelle wird mit einem anderen Schlüssel verschlüsselt
- Darf nur 1 Mal verwendet werden!
- Anzahl möglicher Schlüssel = Anzahl möglischer Nachrichten
- Ist sicher, d.h. Geheimtext verrät keinerlei (zusätzliche) Information über den Klartext
- Intuitiv: Für einen bestimmten Geheimtext sind **alle** Klartexte (dierser Länge) möglich

TODO BILD one-time pad

Sie wissen welche modernen Verschlüsselungsalgorithmen in der Praxis verwendet werden und was deren Eigenschaften sind

Informationstheoretische Sicherheit Das Ziel informationstheoretischer Sicherheit ist der Schutz von Daten vor unbefugtem Zugriff während der Übertragung. Im Unterschied zur Kryptographie basiert informationstheoretische Sicherheit nicht auf der Annahme, dass die Rechenleistung eines unberechtigten Empfängers nicht gross genug ist, um die Daten zu decodieren. Vielmehr garantiert informationstheoretische Sicherheit, dass ein unberechtigter Empfänger selbst bei beliebig grosser Rechenleistung nicht in der Lage ist, solcherart geschützte Nachrichten zu decodieren. Mit anderen Worten erhält ein Angreifer durch den Geheimtext keinerlei (zusätzliche) Information über den Klartext.Beispielsweise ist OTP informationstheoretisch sicher.
Formal: $P(M = m) = P(M = m|C = c)$ Erklärung der Variabeln??

Berechenmässige Sicherheit Der sicheren Übertragung und Aufbewahrung vertraulicher Daten kommt in unserer von Information dominierten Gesellschaft immer grössere Bedeutung zu. Die heute gebräuchlichen Verfahren zur Datenverschlüsselung bieten allerdings nur beschränkte, sogenannt berechenmässige Sicherheit. Das bedeutet, dass diese prinzipiell von einem Angreifer, der über genügend Rechenleistung (zum Beispiel einen, heute noch hypothetischen, Quantencomputer) verfügt, gebrochen werden können.

Kerckhoff’s Prinzip Der Angreifer kennt den Algorithmus und alle Details des Systems. Nur der Schlüssel ist geheim.

Angriffsarten Bei der Sicherheit von modernen Verschlüsselungssystemen wird zwischen den Angriffsmöglichkeiten des Angreifers unterschieden:
- **Ciphertext only attack:** Angreifer erhält nur den zu entschlüsselnden Geheimtext
- **Known plaintext attack:** Angreifer erhält zusätzlich andere Klartext-Geheimtext-Paare
- **Chosen plaintext attack:** Angreifer kann zusätzliche Klartexte wählen, zu denen er auch die Geheimtexte erhält

TODO ev. BILD zu Angriffsarten

Sie verstehen was eine Hashfunktion ist und welche Eigenschaften eine kryptographische Hashfunktion ausmachen, bzw. was es heisst, wenn eine Hashfunktion gebrochen ist

TODO

Sie kennen moderne Hashfunktionen und wissen welche Eigenschaften diese haben

TODO

Sie kennen Anwendungen von Hashfunktionen

TODO

Sie wissen was ein keyed Hash (HMAC) ist und wofür dieser verwendet werden kann

TODO

Sie kennen die „Best-practices“ zu Passwortsicherheit und wissen, gegen welche Angriffe diese schützen

TODO

3 Asymmetrische Kryptographie

Asymmetische Verschlüsselung In der asymmetrischen Kryptografie (Verschlüsselung) arbeitet man nicht mit einem einzigen Schlüssel, sondern mit einem **Schlüsselpaar**. Bestehend aus einem **öffentlichen** und einem **privaten Schlüssel**. Man bezeichnet diese Verfahren als asymmetrische Verfahren oder Public-Key-Verfahren.

Sie verstehen was Public-Key-Kryptographie ist, worauf deren Sicherheit basiert und wie sie zur Verschlüsselung, für Signaturen und zur Authentisierung verwendet werden kann

Public Key Verschlüsselung Basiert auf Funktionen, welche einfach zu berechnen sind, deren Umkehrfunktion aber (vermutlich) schwierig zu berechnen ist. Beispiel:

Multiplikation (einfach):	$97 \times 84 = 8051$
Faktorisieren (schwierig):	$8051 = ?$

TODO BILDER aus „The Science of Secrecy“

Sie kennen die gängigen asymmetrischen Verschlüsselungs- und Signaturalgorithmen und wissen, worauf deren Sicherheit basiert

TODO

Sie wissen wie Diffie-Hellmann-Schlüsselaustausch bzw. ElGamal-Verschlüsselung funktioniert

Diffie-Hellman (DH) Diffie-Hellman ist ein Schlüsselvereinbarungsprotokoll. Der vereinbarte gemeinsame geheime Schlüssel kann danach zur Verschlüsselung der Nachricht verwendet werden.

TODO BILD & ev. Beispiel Wiki

ElGamal-Verschlüsselung ElGamal verwendet DH um einen asymmetrischen Verschlüsselungsalgorithmus zu erstellen.

TODO BILD ElGamal

TODO ev. Beispielrechnung machen

Sie wissen was kryptographisch sichere Zufallszahlen sind und wo diese verwendet werden

TODO

Sie wissen was eine elektronische Signatur ausmacht

TODO

Sie wissen wie hybride Verschlüsselung bzw hybride Signaturen funktionieren

TODO

4 Zertifikate und SSL-TLS

Sie kennen die verschiedenen Arten von „Trust“

TODO

Sie wissen was eine Public-Key-Infrastruktur, eine Certificate Authority und ein Zertifikat ist, wofür und wie diese verwendet werden und wie Zertifikate ausgestellt und revoziert werden

TODO

Sie wissen was SSL/TLS ist, welche Funktionalität es erreicht und wie das Protokoll konzeptionelle abläuft

TODO

Teil III
Angriffe (SW 05-06)

5 Angriffe auf Webanwendungen

Bedrohungen auf Anwendungsebene Webanwendung, Session, Headers, CSRF

Sie wissen was eine Webanwendung ausmacht, wie HTTP funktioniert

Was unterscheidet eine Webanwendung aus Sicherheitssicht zu anderen Anwendungen?
- Kommuniziert über HTTP mit einem Server
  - zustandsloses Protokoll
- Läuft in einem Browser
  - Mehrere Webanwendungen können parallel im gleichen Browser laufen
  - Die Webanwendung *erbt* vom Browser implementierte Features bzw. muss diese richtig ansprechen

HTTP Der Browser kommuniziert mit dem Webserver über das **Hypertext Transfer Protokoll (HTTP)**. HTTP besteht aus *Requests* und *Reponses*.

HTTP-Request-Methoden Die häufigsten HTTP-Request-Methoden sind **GET** und **POST**. Es existieren aber auch **PUT, HEAD, DELETE, PATCH, OPTIONS**.

GET `https://www.hslu.ch/?p=5 HTTP/1.1`
`User-Agent: Mozilla/5.0`
- Message Body: kein
- Ruft Daten vom Server ab
- Sollte Serverzustand nicht verändern

POST `https://www.hslu.ch/ HTTP/1.1`
`User-Agent: Mozilla/5.0`
- Message Body: `id=123&pwd=password`
- Darf Serverzustand verändern
- Wird nicht gecachet

Häufigste Reponse-Codes
- 200 OK
- 204 No Content
- 301 Moved Permanently
- 302 Found (Vorher: „Moved temporarely“)
- 304 Not Modified
- 400 Bad Request
- 403 Forbidden
- 404 Not Found
- 500 Internal Server Error

HTTP Zustand HTTP ist ein zustandsloses Protokoll, d.h. es hat kein ‘Gedächtnis’, bzw. Erinnerung.

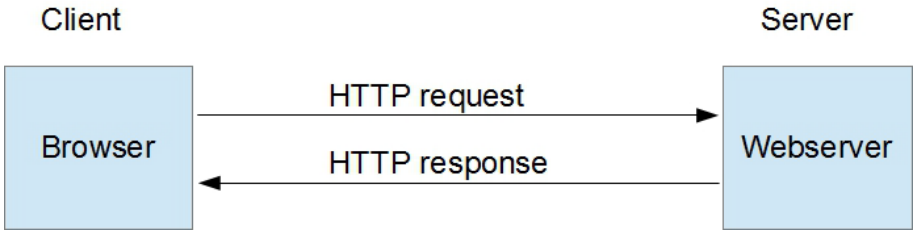

Abbildung 2: HTTP zustandslos

Die einzige Möglichkeit einen Zustand an den Client zu übergeben ist, diesen per weiteren Requests mitzuschicken. Die Zustände werde mit einem Cookie oder einem „Hidden field“ erfasst.

Cookies Cookies sind kurze Textdaten, welche vom Server als Header an den Browser übermittelt werden und von diesem ebenso als Header bei requests wieder mitgesendet werden. Cookies werden vom Browser verwaltet. Die meistgenutzte Möglichkeit ist es, ein Cookie zu setzen. Jedoch dürfen auch Cookies nicht client-seitig angepasst werden können!

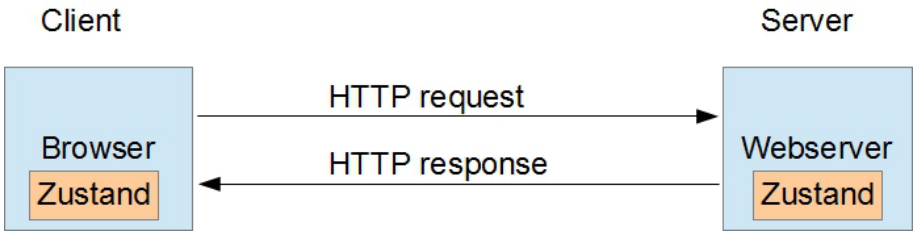

Abbildung 3: HTTP Zustand per Request (hidden field)

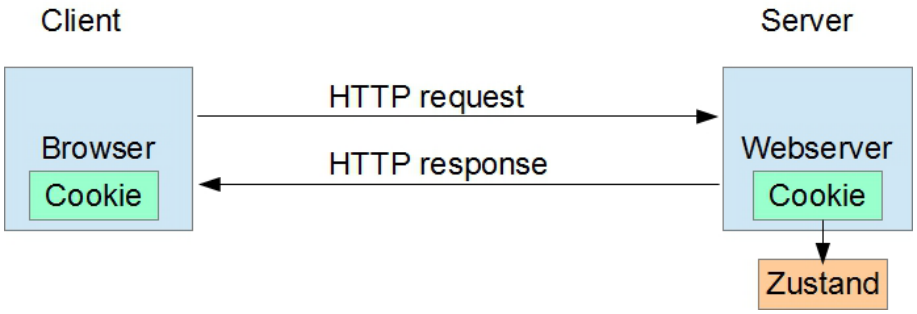

Abbildung 4: Einsatz eines Cookies

Cookie Eigenschaften Die Eigenschaften von Cookies sind:
- **Persistent** (mit Ablaufdatum) oder **Session-Cookie** (ohne Ablaufdatum)
- **Secure** (wird nur über HTTPS übertragen)
- **HTTP Only** (darf nur von HTTP gelesen werden)
- **Same Site** (wird nicht bei Cross-Domain-Aufrufen mitgesendet, z.B. 'embedded' Link, Image)

Sie wissen was eine Session ist und welche Eigenschaften einer Session bei welchen Angriffen wichtig sind bzw wie sie gegen gewisse Angriffe Schutz bieten

Session Eine Session ist der Zeitraum, in dem ein Client eine stehende Verbindung mit einem Server hat; vom Login bis zum Logout. Der Server vergibt dem Client eine eindeutige Session-ID. Die Sitzungsdaten (z.B. Warenkorb) werden im Server gespeichert. Bei jedem Request gibt der Client seine Session-ID mit, damit der Server beim Response die zugehörigen Daten dieser ID übermitteln kann. Es gibt auch Sessions ohne stehende Verbindung (ohne Login). Dies wird zu Statistikzwecken verwendet, beispielsweise um die Bewegung des Besuchers auf der Website zu verfolgen. Oder aber auch um einen Warenkorb ohne Login verwenden zu können.

Schwaches Session-Management Was ist das?
- der Sessionwert ist vorhersagbar
- der Sessionwert kann vom Client gesetzt werden
- die Cookie-Attribute 'Secure', 'HttpOnly' oder 'Same Site' sind nicht gesetzt
- Cookie-Domain oder -Pfad sind nicht so eingeschränkt wie möglich
- die Session wird bei einem Logout nicht invalidiert
- die Session hat kein server-seitiges Timeout (Inaktivitäts- und absolutes Timeout)

Schwaches Session-Management Was kann man dagegen tun?
- lange und kryptographisch zufällige Sessionwerte wählen
- nur vom Server gewählte Sessionwerte akzeptieren
- Cookies als 'Secure','HttpOnly' oder 'Same Site' mit so eingeschränkter Domain und Pfad wie möglich setzten
- Session **server-seitig** bei einem Logout oder Timeout invalidieren

Same Origin Policy Mehrere Webanwendungen können im gleichen Browser parallel laufen. Die Same-Origin-Policy verhindert, dass eine parallel laufende Webanwendungen uneingeschränkt

- auf die Daten einer anderen Anwendung zugreifen
- die Cookies einer anderen Anwendung lesen oder mitschicken
- Requests auf die andere Anwendung absetzen

kann.
Same Origin Policies im Browser gibt es z.B. für Cookies, DOM access (Zugang zu document.cookie), HTML5Storage, XMLHttpRequests.

Same Origin Policy: Cookies Cookies haben eine **domain** und **path**.
- **Setzen des Cookies:** Nur Domain-Suffix des URL-Hostname dürfen gesetzt werden. (Aber keine Top-Level Domains!)
  Path kann beliebig gesetzt werden.
- **Senden des Cookies:** Cookies werden dnur dann mitgeschickt, wenn die Cookie-Domain ein Domain-Suffix der URL-Domain und der Cookie-Path ein Prefix des URL-Path ist.

Session Fixation Was ist das?
Der Sessionwert wird nach einem Login oder Loginschritt nicht geändert. Ein angreifer mit Zugang zu einer unauthentisierten Session kann warten bis ein Benutzer sich einloggt und ist damit selbst eingeloggt.

Session Fixation Was kann man dagegen tun?
Sessionwert nach jedem Authentisierungsschritt ändern.

Sie kennen sicherheitsrelevante Header

Sicherheitsrelevante Response-Header
1. **HSTS:** `Strict-Transport-Security: max-age=31536000; includeSubDomains`
   Seite wird nur via HTTPS aufgerufen. `max-age` muss hoch gesetzt werden!
2. **Frame-Options:** `X-Frame-Options: deny`
   Verbietet das Einbinden der Seite in einem Frame oder erlaub es nur für bestimmte Domains
3. **XSS-Protection:** `X-XSS-Protection: 1; mode=block`
   Filtert und säubert oder blockeirt die Anzeige der Seide, wenn ein XSS-Angriff endeckt wird
4. **Content-Type-Options:** `X-Content-Type-Options: nosniff`
   Verhindert, dass der Content als einen anderen MIME-Type interpretiert wird als angegeben
5. **CSP:** `Content-Security-Policy: script-src 'self'`
   Definiert, welche Resourcen (z.B. Bilder, Scripts, Fonts, etc.) von wo eingebunden werden können
6. **CORS** `Access-Control-Allow-Origin: http://foo.example`
   Cross-Origin Resource Sharing (CORS) ist ein Mechanismus, der Webbrowsern oder auch anderen Webclients Cross-Origin-Requests ermöglicht. Zugriffe dieser Art sind normalerweise durch die Same-Origin-Policy (SOP) untersagt. CORS ist ein Kompromiss zugunsten grösserer Flexibilität im Internet unter Berücksichtigung möglichst hoher Sicherheitsmassnahmen.
7. **Caching-Options** TODO: hat jemand Infos?
8. **HPKP (deprecated!):** `Public-Key-Pins:`
   `pin-sha256=d6qzRu9zOECb90Uez27xWltNsj0e1Md7GkYYkVoZWmM=;`
   `pin-sha256=Ë9CZ9INDbd+2eRQozYqqbQ2yXLVKB9+xcprMF+44U1g=;`
   `report-uri=http://example.com/pkp-report;`
   `max-age=10000; includeSubDomains`
   HTTP Public Key Pinning: Nur das Serverzertifikat mit dem korrekten Fingerprint wird akzeptiert. Wurde wieder abgekündigt und die meisten Browser unterstützen es nicht mehr.

Sie verstehen wie ein Cross-Site-Request-Forgery-Angriff abläuft und wie man sich dagegen schützen kann

CSRF - Cross-Site Request Forgery Was ist das?
Der Angreifer bringt einen Benutzer dazu, einen Request aus seinem Browser abzusetzen und dadurch eine Aktion auf dem Server auszulösen. Ist der Benutzer zu dem Zeitpunkt eingeloggt, wird das Cookie automatisch mitgeschickt.

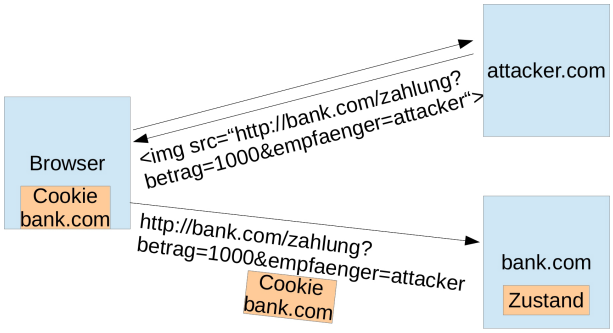

Abbildung 5: Cross-Site Request Forgery

6 Angriffe auf Protokollebene

Sie kennen die Grundbegriffe der Anwendungssicherheit

TODO

Sie kennen Beispiele von Angriffen auf verschiedenen Ebenen des Protokollstacks und wissen was diese bewirken

TODO

Sie verstehen wie ein Cross-Site-Scripting / SQL-injection / Social-Engineering-Angriff abläuft und wie man sich dagegen schützen kann

TODO

Teil IV
Management (SW 07-09)

7 Standards & Frameworks, ISMS

Sie wissen, was ein ISMS ist und wie man damit umgeht

TODO

Sie kennen die wichtigsten Standards der Informationssicherheit

TODO

Sie finden sich in den Standards ISO 27001 und 27002 zurecht

TODO

Sie verstehen die Grundzüge der BSI-Standards (BSI=Bundesamt für Sicherheit in der Informationstechnik, Deutschland)

TODO

Sie kennen die Struktur und Grundziele des NIST CyberSecurityFrameworks

TODO

8 Risiko-Management und IT-Grundschutz

Das Risikoanalyse-Verfahren verstehen

TODO

Die Unterschiede zum Grundschutzverfahren kennen

TODO

Eine einfache Risikoanalyse durchführen können

TODO

Sie verstehen die Idee, die Ziele und die Konzepte des IT-Grundschutz-Vorgehens

TODO

Sie kennen den Aufbau der IT-Grundschutz-Kataloge und deren Anwendungsweise

TODO

Sie können die Teilschritte zum Aufbau eines Sicherheitskonzeptes nach IT-Grundschutz durchführen, kombinierte Risikoanalyse

TODO

9 Awarness

Sie verstehen die Wichtigkeit der «Awareness »

TODO

Sie kennen verschiedene Prozesse und Vorgehensweisen für die Initiierung, Durchführung und Erfolgsprüfung einer Awareness-Kampagne und können diese anwenden

TODO

Sie kennen die relevanten Erfolgsfaktorender Mitarbeiter-Sensibilisierung und -Schulung und können diese in einer Kampagne umsetzen

TODO

Teil V
Access Control (SW 10)

10 Access Control

Sie kennen verschiedene Arten der Authentisierung, wissen wie diese technisch ablaufen und was deren Vor- und Nachteile sind

TODO

Sie wissen wie verschiedene Authentisierungstoken technisch funktionieren, was deren Vor- und Nachteile sind und wie sie beim Login oder bei der Transaktionsbestätigung im e-Banking eingesetzt werden

TODO

Sie wissen was Authentisierung, Autorisierung ist, warum diese wichtig sind und wie Angriffe darauf ablaufen

TODO

Teil VI
Multi-Party-Computation (SW 11)

11 Cryptographic Protocols

Sie kennen einfache Beispiele von verteilten sicheren Berechnungen und verstehen wie die entsprechenden Protokolle ablaufen

TODO

12 Secret Sharing

Sie kennen Arten von Sicherheit von verteilten sicheren Berechnungen und wie diese angegriffen werden können

TODO

Sie wissen welche Eigenschaften elektronisches Geld ausmachen und kennen die technischen Grundlagen von Bitcoin

TODO

13 Zero Knowledge Proof

Sie wissen was Zero-Knowledge-Proofs sind und wie diese ablaufen

TODO

Teil VII
Quantum (SW 12)

14 Quantum Computing and Quantum Cryptography

Sie wissen was ein Quantencomputer ist und was ihn von einem „klassischen“ Computer unterscheidet

TODO

Sie verstehen welchen Einfluss die Existenz eines Quantencomputers auf die Kryptographie hat

TODO

Sie verstehen wie Quantenschlüsselaustausch funktionert

TODO

Teil VIII
WAF, Federations (SW 13)

15 Firewalls

Sie wissen was die Aufgaben einer Firewall sind

TODO

Sie verstehen die Funktionsweise einer WAF und wie sie eine Webanwendung vor Angriffen schützen kann

TODO

16 Federations

Sie verstehen wie Authentisierung mit Identity Federation abläuft, was die Voraussetzungen dafür sind und was die Vor- und Nachteile von Federations sind

TODO

Teil IX
Talks (SW 14)

17 Malware

Sie verstehen, welche Arten von Malware es gibt, welche Massnahmen gegen Malware sinnvoll sind und wie diese wirken

TODO

18 WAF

Sie verstehen wo Machine-Learning in einer WAF eingesetzt werden kann und was einene Machine-Learning-Ansatz vom „herkömmlichen“ Einsatz einer WAF unterscheidet

TODO

Sie kennen Beispiele von Angriffen, welche mittels Machine-Learning auf einer WAF erkannt werden konnten

TODO