

PHISHING UND SOCIAL ENGINEERING

Simon Lang

31. Mai 2015

Version 1.0.0

STUDIENGANG	Informatik 5 Ba 2012
SEMINAR	Sicherheitsanwendungen/PKI
DOZENT	Peter Stadlin
SCHULE	ZHAW - School of Engineering

Kurzfassung

Schlagwörter: Phishing, Social Engineering, Public Key Infrastructure, Fachhochschule, ZHAW School of Engineering

Inhaltsverzeichnis

1	Einleitung	1
1.1	Ziele	1
1.2	Begründung	1
2	Beschreibung der Aufgabe	2
2.1	Aufgabenstellung	2
2.1.1	Ausgangslage	2
2.1.2	Ziele der Arbeit	2
2.1.3	Aufgabenstellung	2
2.1.4	Erwartete Resultate	2
3	Einführung	3
3.1	Über den Autor	3
3.2	Aufbau	3
3.3	Aufbau des Internets	3
3.4	Standards	4
3.5	Interne vs. Externe Entwicklung	5
4	Requirements Engineering	6
4.1	Endgeräte	6
4.1.1	Responsive- vs Adaptive Web Design	6
4.1.2	Bandbreite	8
5	Phishing	9
6	Schlussfolgerung	10
6.1	Persönliches	10
	Quellenverzeichnis	11

Abbildungsverzeichnis

3.1 Aufbau des Internet	4
4.1 Responsive- vs Adaptive Web Design ¹	7
4.2 Responsive Web Design ²	7

-
- ¹ *Responsive vs Adaptive Design for UI*. URL: <http://blog.zymr.com/responsive-vs-adaptive-design-for-ui> (besucht am 31.05.2015).
- ² *The Difference Between Adaptive Design And Responsive Design / Search Engine People*. URL: <http://www.searchenginepeople.com/blog/the-difference-between-adaptive-design-and-responsive-design.html> (besucht am 31.05.2015).

Tabellenverzeichnis

Akronyme

Bezeichnung	Beschreibung
AWD	Adaptive Web Design
CA	Certification Agency
CSS	Cascading Style Sheets
HTTPS	HyperText Transfer Protocol Secure
JS	Java Script
RWD	Responsive Web Design
W3C	World Wide Web Consortium
WWW	World Wide Web
ZHAW	Zürcher Hochschule für Angewandte Wissenschaften

Glossar

HTML

HTML (engl. Hypertext Markup Language) ist eine textbasierte Auszeichnungssprache zur Strukturierung digitaler Dokumente wie Texte mit Hyperlinks, Bildern und anderen Inhalten. HTML-Dokumente sind die Grundlage des World Wide Web und werden von Webbrowsern dargestellt.

KAPITEL 1

Einleitung

1.1 Ziele

Jede Software die entwickelt wird ist unterschiedlich, und doch haben sie einiges gemeinsam. Diese Arbeit widmet sich der Softwareentwicklung für Webseiten und versucht darzustellen, was in diesem Bereich im speziellen zu beachten ist.

1.2 Begründung

Das Internet ist das weltweit grösste Netzwerk. Die Anzahl der Teilnehmer ist unmöglich zu bestimmen, da Endgeräte sich einloggen und auch wieder ausloggen. Laut IWS hatten im März 2007 etwa 16,9 Prozent der Weltbevölkerung Zugang zum Internet¹. In der Schweiz verfügten im Jahr 2012 85 Prozent der Bevölkerung über einen privaten Internetzugang. Insgesamt nutzen im Herbst 2013 81% der Bevölkerung regelmässig (täglich oder mehrmals pro Woche) das Internet. Fast 40% der Bevölkerung nutzten 2012 einen Breitbandanschluss, mit einer Übertragungsrate von mehr als 256 Kbit/s².

Dadurch wird auch entsprechend viel Software für das weltweit grösste Netzwerk produziert. Darüber handelt diese Schreiben.

¹ *World Internet Users Statistics and 2014 World Population Stats*. URL: [http : / / www . internetworldstats.com/stats.htm](http://www.internetworldstats.com/stats.htm) (besucht am 30.05.2015).

² *Internet – Wikipedia*. URL: <https://de.wikipedia.org/wiki/Internet#Nutzerzahlen> (besucht am 30.05.2015).

KAPITEL 2

Beschreibung der Aufgabe

2.1 Aufgabenstellung

2.1.1 Ausgangslage

Im Jahre 1969 entstand das Arpanet. Nach einem langsamen Start vergrößerte es sich rasant zu dem heute bekannten Internet. Die Tendenz ist immer noch rasant wachsend. Beschleunigt wird der Wachstum heutzutage durch die unzähligen mobilen Geräte, die Zugriff auf das Internet haben. Durch den rasanten Wechsel der damit verbundenen Technologien muss sich auch die Softwareentwicklung stets anpassen.

2.1.2 Ziele der Arbeit

Ziel der Arbeit ist es, die Schwierigkeiten und Probleme des Software Engineerings für die Webseitenentwicklung zu analysieren. Es sollen Konzepte gezeigt werden, wie Software für die verschiedenen Endgeräten mit ihren unzähligen Browsern entwickelt werden. Dazu wird eine grobe Übersicht über die Software für Webseiten gegeben.

2.1.3 Aufgabenstellung

Es soll ein Dokument zum Thema DSSE für die Webseitenentwicklung erstellt werden. Das Papier soll die Schwierigkeiten von Software in dieser Branche aufzeigen und einen groben Überblick über das Thema geben.

2.1.4 Erwartete Resultate

Folgende Ergebnisse werden am Schluss dieser Seminararbeit erwartet:

- Dokumentation
- Handout
- Präsentation

KAPITEL 3

Einführung

3.1 Über den Autor

Mein Name ist Simon Lang. Als gelernter Informatiker arbeite ich seit 2006 in der Webentwicklungsbranche. Seit 2012 studiere ich Informatik an der [Zürcher Hochschule für Angewandte Wissenschaften \(ZHAW\)](#). Durch mehrjährige Erfahrung in der Webentwicklung habe ich mich im Seminar zur Vorlesung *Software Engineering* für die Vertiefung im Web entschieden.

3.2 Aufbau

Die Arbeit befasst sich mit den wesentlichen Schritten der Softwareentwicklung, welche im SWEBOK¹ beschrieben sind.

- Requirements Engineering
- Software Design
- Software Construction
- Software Testing
- Software Maintenance / Software Configuration Management

Als Wissen wird vorausgesetzt, was die grundlegenden Arbeitsschritte in den einzelnen Kabiteln des SWEBOK sind. Die Arbeit geht nicht direkt über das SWEBOK, sondern befasst sich mit den speziellen Ausprägung für die Softwareentwicklung im Internet.

3.3 Aufbau des Internets

Das Internet ist eine Client/Server Architektur. Die Clients stellen Anfragen an einen Server, welcher eine Antwort zurückliefert. Der Client kann dabei ein Benutzer an seinem Computer sein, oder eine Maschine. In der Reisebranche ist dies zum Beispiel der Fall, wenn der Benutzer etwas bucht. Er bestätigt seinen Einkauf und der Server bucht darauf

¹ *index* • *IEEE Computer Society*. URL: <http://www.computer.org/web/swebok> (besucht am 30.05.2015).

die Reise. Der Server verbindet sich dabei auf ein drittes System, zum Beispiel jenes des Reiseveranstalters.

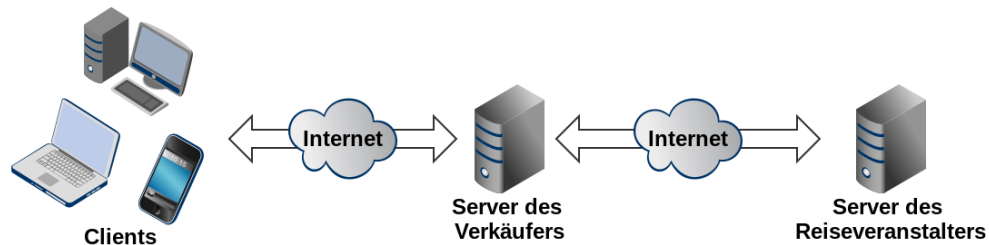


Abbildung 3.1: Aufbau des Internet

Wenn eine Webseite angezeigt werden soll, fragt der Client den Server an, und dieser liefert ein **HTML** Dokument aus. Dieses kann weitere Dokumente von weiteren Servern abfragen, wie zum Beispiel Bilder. Das **HTML** Dokument wird von einer Programmiersprache auf dem Server generiert. Das ausgelieferte Dokument kann danach von einer Client-Seitigen Sprache weiter modifiziert werden. Als Programmiersprache auf dem Client wird meistens **Java Script (JS)** eingesetzt. Die **HTML** Datei sollte nur den Inhalt und die Struktur der Webseite vorgeben. Das Aussehen wird über **Cascading Style Sheets (CSS)** definiert.

3.4 Standards

Es gibt unzählige Standards für das **World Wide Web (WWW)**. Die wichtigsten werden vom **World Wide Web Consortium (W3C)**¹ herausgegeben. Die Standards sind folgendermassen strukturiert:

- Web Design and Applications
- Web of Devices
- Web Architecture
- Semantic Web
- XML Technology
- Web of Services
- Browsers and Authoring Tools

Vorgegeben wird die Sprache **HTML** und auch wie diese Dokumente aufgebaut werden sollen. Auch wie die Browser die Dateien darzustellen haben ist Teil eines Standards des **W3C**.

Seit einigen Jahren wurden die Standards für Mobiltelefone und Tablets erweitert. Programmierer für das Internet sollten die gängigsten Standards kennen und sich auch daran halten, so dass andere Entwickler sich einfacher in den bestehenden Code einarbeiten können.

¹ *World Wide Web Consortium (W3C)*. URL: <http://www.w3.org/> (besucht am 30.05.2015).

3.5 Interne vs. Externe Entwicklung

Webentwickler arbeiten entweder an internen oder externen Projekten. Bei ersteren ist der Arbeitgeber der Auftraggeber, wo hingegen bei letzteren ein externer Kunde über den Umfang der Software bestimmt. Für die Entwicklung macht dies ein grosser Unterschied, da die internen Projekte meistens über Jahre hinweg gepflegt werden. Wird die Software für ein Kunden erstellt gibt es zuerst oft eine Projektausschreibung, wo mehrere Softwarehersteller sich bewerben können. Nach der Umsetzung und einer Garantiefrist der Auftrag abgeschlossen. In den Projektausschreibung wird oft ein zu tiefer Preis angeboten, was mit einer Minderung der Qualität ausgeglichen wird.

KAPITEL 4

Requirements Engineering

Dieses Kapitel zeigt die speziellen Eigenschaften des Requirements Engineering im Bereich der Webentwicklung.

Früh in der Entwicklung einer Software muss man die Rahmenbedingungen festlegen. Zuerst wird gezeigt, für welche Geräte und Browser man sich spezialisieren und generalisieren kann.

Danach werden die wichtigsten nicht funktionalen Eigenschaften einer Webseite aufgezeigt und zum Schluss noch weitere wichtige Aspekte des Requirement Engineerings.

4.1 Endgeräte

Es gibt verschiedene Endgeräte, welche die Webseite darstellen müssen.

- PC
- Mobile
- Tablet
- E-Reader
- Spielkonsolen

Als erster Punkt des Requirements Engineering sind die Geräte aufgeführt, da davon vieles abhängt. Zum Beispiel die Grösse des Bildschirms, die Grösse des Eingabegerätes (Maus, Finger), die Bandbreite und noch weitere Punkte.

Für die verschiedenen Bildschirmgrössen gibt es zwei verschiedene Ansätze, die im Unterkapitel [4.1.1 Responsive- vs Adaptive Web Design](#) beschrieben werden.

Dem Problem der Bandbreite nimmt sich das Kapitel [4.1.2 Bandbreite](#) an.

4.1.1 Responsive- vs Adaptive Web Design

¹ Beim [Responsive Web Design \(RWD\)](#) wird eine Seite generiert, die sich der Bildschirmgrösse anpasst, wo hingegen beim [Adaptive Web Design \(AWD\)](#) für verschiedene Bildschirm-

¹ *Responsive vs. Adaptive Design: What's the Best Choice for Designers?* - UXPin. URL: <http://blog.uxpin.com/6439/responsive-vs-adaptive-design-whats-best-choice-designers/> (besucht am 31.05.2015).

größen jeweils ein anderes Layout ausgeliefert wird.



Abbildung 4.1: Responsive- vs Adaptive Web Design^a

^a *Responsive vs Adaptive Design for UI*. URL: <http://blog.zymr.com/responsive-vs-adaptive-design-for-ui> (besucht am 31. 05. 2015).

Ein RWD liefert der Server für jedes Endgerät das selbe HTML aus. Die Elemente ordnen sich jedoch auf den verschiedenen Bildschirmgrößen anders an. Die folgende Grafik illustriert dieses vorgehen.



Abbildung 4.2: Responsive Web Design^a

^a *The Difference Between Adaptive Design And Responsive Design | Search Engine People*. URL: <http://www.searchenginepeople.com/blog/the-difference-between-adaptive-design-and-responsive-design.html> (besucht am 31. 05. 2015).

Der Vorteil an dieser Variante ist es, dass keine Überprüfung der Bildschirmgröße nötig ist und auf dem Bildschirm immer eine angepasste Ansicht ermöglicht wird. Auch wenn man die größe des Browserfensters anpasst erhält man immer eine passende Ansicht. Die Programmierung wird dadurch vereinfacht, dass nur eine HTML Seite generiert werden muss. Jedoch wird das Layout komplizierter und es müssen mehr Daten an das Engerät ausgeliefert werden.

Beim AWD werden eigene HTML Seiten für die verschiedenen Auflösungen gepflegt. Um den selben Umfang wie das RWD zu ermöglichen, müssen die folgenden sechs Bildschirm-

breiten gepflegt werden:

- 320
- 480
- 760
- 960
- 1200
- 1600

Generell macht es Sinn ein [RWD](#) zu pflegen, da der Pflegeaufwand generell geringer ausfällt. Es gibt jedoch auch Gründe für ein [AWD](#). Zum Beispiel wenn eine bestehende Seite für mobile Geräte angepasst werden muss ist der Aufwand oft geringer, wenn man eine separate Ansicht dafür umsetzt. Die Ladezeiten für ein [AWD](#) sind meistens auch besser, was folgende Tabelle aufzeigt:

Metrik	AWD	RWD
Antwortzeit	568 ms	1'202 ms
Zeit bis das Dokument vollständig geladen ist	1'536ms	4'086 ms
Bytes Downloaded	2'474'326 kB	4'229'363 kB
Objekte Downloaded	20	61

4.1.2 Bandbreite

xxx

KAPITEL 5

Phishing

KAPITEL 6

Schlussfolgerung

Social Engineering ist eine Angriffsform, die weniger technischer- dafür psychologischer Natur ist. Der Mensch rückt ins Zentrum des Angriffes, nicht die Maschine. Grundlagen für einen Angriff sind schnell erlernt. Doch um erfolgreich zu sein muss man die vorgestellten Techniken lernen und verinnerlichen, sowie selbstverständlich sehr viel üben. Es wird auch Mut vorausgesetzt, denn als Angreifer tritt man aus dem Schatten in das Licht.

Das Social Engineering ist dabei sehr viel sicherer als zunächst angenommen wird. Viele Attacken bleiben unerkannt, da die Opfer diese gar nicht bemerken. Denn das Sicherheitsbewusstsein für eine solche Attacke ist noch unausgereift.

Phishing wirft einen Köder in einen grossen See voller möglichen Opfer und hofft, dass wenige anbeissen. Die Angriffe können von sehr primitiv bis zu sehr ausgeklügelt reichen. Meistens sind sie jedoch für ein geschultes Auge leicht erkennbar. Aber es wird immer ein Fisch geben welcher den Köder schluckt.

6.1 Persönliches

Zur Einarbeitung in das Social Engineering benötigte ich sehr viel Zeit. Das Thema beginnt sehr trocken und hat wenig technische Aspekte. Je tiefer ich jedoch in die Materie eindrang, desto mehr packte mich das Interesse. Ich konnte sehr viel während den Recherchen lernen und einige Techniken kann man auch im Alltag oder im Geschäftsleben gut einsetzen. Zum Beispiel kann das Elizitieren bei Lohn- oder Vertragsverhandlungen zum eigenen Nutzen verwendet werden.

Als Hauptinformationsquelle für das Social Engineering habe ich das Buch *Die Kunst des Human Hacking* von Christopher Hadnagy verwendet. Es ist spannend geschrieben mit vielen Beispielen und ich kann es als Lecktüre durchaus empfehlen.

Phishing war als Thema für mich wesentlich interessanter, da dieses mehr technisches enthält. Ich fand es spannend, dass ich beim schreiben über Phishing sehr viel parallelen zum Social Engineering ziehen konnte.

Abschliessend lässt sich zusammenfassen, dass ich sehr viel Zeit in diese Arbeit investiert habe, es aber auch grossen Spass gemacht hat Recherchen zu betreiben.

Quellenverzeichnis

- [1] *index • IEEE Computer Society*. URL: <http://www.computer.org/web/swebok> (besucht am 30.05.2015) (siehe S. 3).
- [2] *Internet – Wikipedia*. URL: <https://de.wikipedia.org/wiki/Internet#Nutzerzahlen> (besucht am 30.05.2015) (siehe S. 1).
- [3] *Responsive vs Adaptive Design for UI*. URL: <http://blog.zymr.com/responsive-vs-adaptive-design-for-ui> (besucht am 31.05.2015) (siehe S. 7).
- [4] *Responsive vs. Adaptive Design: What's the Best Choice for Designers? - UXPin*. URL: <http://blog.uxpin.com/6439/responsive-vs-adaptive-design-whats-best-choice-designers/> (besucht am 31.05.2015) (siehe S. 6).
- [5] *The Difference Between Adaptive Design And Responsive Design | Search Engine People*. URL: <http://www.searchenginepeople.com/blog/the-difference-between-adaptive-design-and-responsive-design.html> (besucht am 31.05.2015) (siehe S. 7).
- [6] *World Internet Users Statistics and 2014 World Population Stats*. URL: <http://www.internetworldstats.com/stats.htm> (besucht am 30.05.2015) (siehe S. 1).
- [7] *World Wide Web Consortium (W3C)*. URL: <http://www.w3.org/> (besucht am 30.05.2015) (siehe S. 4).