Skript

Wir machen das Internet *sicher*

März 2015

Fassung vom 15. Juni 2015

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Projekt

Kryptographie – Wir machen das Internet sicher

Sichere Kommunikation mit internetbasierten Angeboten

André Hilbig et. al.

Versionsinformationen:

Hash:	b60da90
Branch:	(None)
Stand:	2015-06-15 16:35:48 +0200
Zuletzt bearbeitet von:	André Hilbig (mail@andrehilbig.de)

Worum es geht?

Schülerinnen und Schüler nutzen tagtäglich Informatiksysteme zur Kommunikation. Die Ziele, die die Kommunikation dabei verfolgt sind vielfältig. Vom Zugehörigkeitsgefühl zu bestimmten Gruppen über dem Einholen von Informationen und der »Selbstdarstellung« bis hin zur direkten *Eins-zu-Eins*-Kommunikation mit Freunden. Genauso vielfältig wie der wichtige Nutzen sind jedoch auch die Risiken. Über das »Abfischen« von privaten und sensiblen Daten durch Dritte, wie Geheimdienste, Werbeindustrie, Internetkonzernen oder kriminellen Personen, bis hin zur böswilligen Veränderung der Kommunikation selbst, wie etwa bei Cybermobbing.

Um den vernünftigen Umgang mit internetbasierter Kommunikation zu befördern, ist die Aufklärung über Risiken und die Auffindung zur Minimierung selbiger notwendig. Ohne ein Mindestmaß an Verständnis über die sozialen Zusammenhänge sowie die technischen Grundlagen ist ein sicherer Umgang nicht möglich. Die hier dokumentierte Projektwoche soll Schülerinnen und Schüler befähigen, Angebote im Internet bezüglich des Nutzens und der Sicherheit einzuschätzen und etwaige Werkzeuge und Mechanismen zu benutzen, um die Sicherheit zu erhöhen.

Projekt – Kompetenzen

1. Die Schülerinnen und Schüler erklären die Funktionsweise von netzwerkbasierter Datenübertragung indem sie die Nutzung und Bereitstellung von Daten in Netzwerken (und dem Internet) anhand von Planspielen und konkreten Angeboten untersuchen,
2. definieren die zentralen Sicherheitsziele, erkennen deren Notwendigkeit innerhalb konkreter, alltäglicher Situationen und zeigen entsprechende verantwortungsbewusste Handlungsoptionen auf,
3. nutzen unter Verwendung geeigneter, alltagsnaher Werkzeuge die bereitgestellten Dienste entfernter Informatiksysteme verantwortlich, sicher und selbstbestimmt,
4. gestalten ihr soziales Miteinanders durch die Verwendung von internetbasierten Angeboten zur Kommunikation indem sie sowohl die sozialen Voraussetzungen als auch die technischen Grundlagen für sich selbst als auch beteiligte Mitmenschen benennen und durch kritisches abwägen zu einer sinnvollen Wahl der Werkzeuge bzw. Angebote gelangen.

⇒ Sichere, sinnvolle Kommunikation mit internetbasierten Angeboten für sich selbst und andere ermöglichen.

Inhalte dieses Projekts

1 Planung

1.1 Grobe inhaltliche Planung

Es handelt sich um drei Tage. Am letzten Tag ist wahrscheinlich eine Art Präsentation vorgesehen. Folgende Themengebiete erscheinen mir den Kompetenzen dienlich und insgesamt interessant:

Netzwerke und Internet(s) Wie funktioniert Kommunikation in Netzwerken? Und was ist eigentlich dieses Internet? Hier könnten einfache Topologien und Protokolle besprochen werden, etwa mit dem Planspiel Netzwerkübertragung und Paketierung von Hilbig und Salamon.

Angebote Nachdem einfache Protokolle und die generelle Übermittelung von Daten klar geworden sind, sollte auch kurz auf Dienste und Angebote im Internet eingegangen werde. Eventuell kann dies auch später erfolgen. Generell müssen soziale Netzwerkdienste, Chats und Instant-Messaging (*kurz:* IM) in sozialer sowie technischer Funktion erklärt werden. Hier könnte auch auf die Problematiken der Klartextübertragung in Bezug auf Topologien eingegangen werden.

Kryptographie und Kryptologie Wie könnte ich mich gegen die Klartextübertragung und das Abhören absichern? Einfache kryptographische Grundprinzipien müssen erklärt werden. Es bietet sich an hierfür das Spioncamp (vgl. Müller 2012) zu nutzen. Eventuell werden auch Abfangszenarien durchgespielt, z. B. Passwordfishing, Abgreifen von Daten aus RFID (Personalausweis) etc. Wichtig ist, dass klar wird, woran ich heute eine sichere Verschlüsselung (Sicherheitsziele) erkennen kann.

Anwendung Die Welt der Schülerinnen und Schüler steckt voller Angebote zur Kommunikation. Wir wollen diese Welt untersuchen und mit dem kryptographischen Wissen absichern. Wenn eine Absicherung gegebener Angebote nicht möglich ist, wird nach Alternativen gesucht. Ziel wäre tatsächlich jede Kommunikationsmethode der Schülerinnen und Schüler abzusichern.

1.2 Möglichkeiten zur Verschlüsselung aktueller Angebote

Die Anforderungen der Schülerinnen und Schüler an ein Werkzeug zur Kommunikation sind vielfältig. Hier sind einige mögliche Angebote bzw. Szenarien mit entsprechenden Möglichkeiten zur Verschlüsselung aufgeführt. Wichtig sind folgende Punkte zur Auswahl eines Werkzeugs zur Verschlüsselung (neben angemessener Sicherheit):

- Multi-Platform: Es müssen sowohl Win, Mac und Linux auf Desktopseite als auch mind. android mobil (optional sicherlich auch iOS wichtig) unterstützt werden.
- Sicherheitsmechanismus muss prüfbar sein: OpenSource
- Kostenlos verfügbar

Angebot	**Möglichkeiten zur Verschlüsselung**
E-Mail	PGP bzw. gpg
IM	otr-plugins
SMS	?
Mobile-IM	TextSecure
Bilder- und Videoaustausch	?
Dateiaustausch	Bittorrent-sync, PGP, encFS

Tabelle 1: Möglichkeiten gegebene Angebote zur Kommunikation abzusichern

1.3 Grobe zeitliche Planung

Zeit	Thema	Hinweise/Beschreibung
		Vorbesprechung
40 min	Wir kommunizieren – das ist wichtig – aber richtig	– Was ist Kommunikation? → Begriffe sammeln – Loriot-Sketch: Kommunikation kann schief laufen/problematisch sein. Verständnisprobleme, Empathie, Streit, Sprache, Schwierigkeiten – Problematiken: Übung 2, Übung 3
10 min	Was werden wir machen?	Kurze Vorstellung und evtl. eine Übung für Gruppenvertrauen?
		Tag 1
Teil 1 *1.5 Stunden*	Kennenlernen Werkzeuge erleichtern und ermöglichen uns die Kommunikation	Übung 1 – Gibt es Werkzeuge/Methoden/Geräte, die für die Kommunikation benötigt werden? – Unterschiede zwischen Informatiksystemen und »analogen« Methoden als Werkzeug im Gespräch ermitteln. – Welche Werkzeuge benutzt ihr? (Übung 4) → medial präsentierbar festhalten!
Teil 2 *2.5 Stunden*	Wie könnte das mit der *Whats App* eigentlich funktionieren?	– Aufgreifen eines Beispiels mit IM aus der vorgelaufenen Übung – Grobe Besprechung von Datenübermittlung, Internet usw. (evtl. Brainstorming) – Es scheinen also Nachrichten über Netzwerke ausgetauscht werden: Planspiele Netzwerkübertragung bzgl. Topologien und Paketierung durchspielen ⇒ Topologien, Paketierung und Protokolle ableiten – Motivation der Sicherheitsziele: über Erweiterungsmöglichkeit der Planspiele oder Planspiel Datenschutz in kurzer Fassung? ⇒ Formulierung von Sicherheitszielen (inkl. sozialer Sicherheit?), evtl. mit Hinweis auf Sicherheitsarchitektur (Anderson 2008, 4f; Hilbig 2014, 22f)

Fortsetzung auf der nächsten Seite…

Zeit	Thema	Hinweise/Beschreibung
Teil 3 *2 Stunden*	Was ist eigentlich dieses *Facebook*?	Hier folgt Stephan…
		Tag 2
Teil 1 *3 Stunden*	Wir gründen ein Spioncamp	– Bearbeiten geeigneter Stationen des Spioncamps + Knacken aus Materialsammlung? ⇒ Code vs. Chiffre ⇒ Verfahren allgemein: Substitution (monoalphabetisch: Caesar – polyalphabetisch: Vigenère), Transposition (Skytale), Schlüsselaustausch (Diffie-Hellman) ⇒ Symmetrisch, asymmetrisch, hybrid – Schlüssel! ⇒ Einschätzung der Verfahren hinsichtlich Sicherheit (Hinweis auf Kryptologie) – Wichtig sind vor allem die richtigen Keywords aktueller Methoden, um selbstständig nach Verfahren/Werkzeugen suchen zu können
Teil 2 *2 Stunde*	Präsentation vorbereiten	Erstellen von Präsentationen zum Spioncamp
Teil 3 *1 Stunde*	Wir wollen Sicherheit – nur wie?	– Schülerinnen und Schüler finden Möglichkeiten ihre Kommunikationswerkzeuge abzusichern – Vorschlag: Gruppenteilige Arbeit, einteilen nach Publikationskategorie (vgl. Hilbig 2014, S. 36)? – Wir geben Angebote vor oder alle erfragten werden benutzt? – Produkt: Anleitungen für die anderen, Präsentationen, Organisation einer Kryptoparty?
		Tag 3
Teil 1 *2 Stunde*	Wir wollen Sicherheit – nur wie?	Fortsetzung vom Tag zuvor…
Teil 2	Präsentationen erstellen, anschauen, probieren	Präsentationen für den Nachmittag aufbauen und vorbereiten (Mittagessen?)
Abschluss	Reflexion, Fragen	

Tabelle 2: Erster Entwurf für eine mögliche zeitliche Planung

2 Konkrete Ausgestaltung

2.1 Planspiel Routing

Mit dem Planspiel soll sowohl die Topologie von Netzwerken als auch die Notwendigkeit von Verschlüsselung deutlich werden.

Ziele

Die Schülerinnen und Schüler können …

- erklären in welchen Strukturen das Routing von Daten in Netzwerken stattfindet,
- die Problematiken von Netzwerktopologien für die Privatheit der eigenen Daten erläutern und
- entwickeln mögliche Ideen zur Verbesserung der Sicherheit.

Durchführung

Beschreibung und Material erstellen – Wie auswerten und möglicherweise präsentieren?

2.2 Spioncamp

Das Spioncamp der DdI an der Uni Wuppertal (Müller 2012) soll verwendet werden, um den Schülerinnen und Schülern die Methoden zur Verschlüsselung von Texten näher zu bringen.

Ziele

Die Schülerinnen und Schüler können …

- den Unterschied zwischen **Codierung** und **Verschlüsselung** erläutern,
- grenzen die **Verschlüsselungsverfahren** Subsitution und Transposition voneinander ab,
- **entdecken konkrete Verfahren** zur mono- und polyalphabetischen Verschlüsselung und
- erläutern die Funktion und Bedeutung eines **Schlüssels** für die Verschlüsselung.

Aufbau und Stationen

Das Spioncamp soll als freies Stationenlernen eingesetzt werden. Zunächst erhalten die Schülerinnen und Schüler eine kurze Einleitung und Erklärung zur Verwendung und zum Ablauf. Danach können die Schülerinnen und Schüler frei zwischen den Stationen wählen. Sie entscheiden über die Reihenfolge und Präferenz der Stationen. Es gibt Pflicht- und Kürstationen.

Codierung »Die Codierungen dienen zur Abgrenzung des Begriffs Kryptographie. Codierungen sind öffentlich und benötigen keinen Schlüssel. Falls nur eine der drei Codierung bearbeitet werden soll, können sie zu einer Station zusammengefasst werden« (Müller 2012).
An dieser Station **muss** eine der Kodierungen bearbeitet werden, es **können** alle bearbeitet werden:

- Braille,
- Morse oder
- Winkeralphabet.

Steganographie »Steganographie bezeichnet lediglich das Verstecken von Information. Dies allein stellt keine Verschlüsselung dar« (Müller 2012). Diese Station ist **nicht verpfichtend**.

Substitution (monoalphabetisch) Buchstaben bleiben **wo** sie sind, aber nicht **was** sie sind. Jedem Buchstaben wird *immer genau* ein anderer Buchstabe zugeordnet.

Substitution (polyalphabetisch) Buchstaben bleiben **wo** sie sind, aber nicht **was** sie sind. Allerdings ist **was** sie sind immer verschieden.

Transposition Die Buchstaben bleiben **was** sie sind, allerdings nicht **wo** sie sind.
An dieser Station **muss** eines der Verfahren bearbeitet werden, es **können** alle bearbeitet werden:

- Syktale,
- Schablone oder
- Pflügen.

Schlüsseltausch Der geheime Schlüssel stellt das Passwort dar, mit dem der verschlüsselte Text wieder entschlüsselt werden kann. Dies kann z. B. die Verschiebung einer Substitution sein. Der Schlüssel muss immer geheim bleiben, aber zugleich ausgetauscht werden, damit der Empfänger die Nachricht entschlüsseln kann. Auf dem Weg könnte jedoch bereits der Schlüssel abgefangen werden, so dass die gesamte Verschlüsselung wirkungslos wird.
An dieser Station ist die Reihenfolge wichtig – alles ist obligatorisch:

1. Modulo und
2. Diffie-Hellmann.

Die Schülerinnen und Schüler erhalten ein Protokoll auf dem sie ihre Beobachtungen festhalten und die Stationen abhaken. Desweiteren sind hier einige zentrale Fragestellungen notiert, die die Schülerinnen und Schüler am Ende beantworten können sollen.

Erweiterte Sicherung

Am dritten Tag sollen die zentralen Inhalte der Stationen (vgl. Abschnitt 2.2, S. 5) am Nachmittag im Rahmen einer »Museumsausstellung« für Unbeteiligte verdeutlicht werden. Dafür sollten die Schülerinnen und Schüler ein Plakat erstellen, dass die Stationen zusammenfasst.

Hierfür bietet es sich an, dass die Schülerinnen und Schüler sich aufteilen und jeweils einzelne Aspekte bearbeiten. Diese können dann am Ende auf dem großen Plakat aufgeklebt werden:

- Was ist eine Kodierung?
- Was ist eine Verschlüsslung?
- Was ist eine monoalphabetische Verschlüsselung?
- Was ist eine polyalphabetische Verschlüsselung?
- Was bedeutet die Verschlüsselung durch Transposition?
- Was ist ein (geheimer) Schlüssel und warum ist es wichtig einen Schlüssel *sicher* auszutauschen?

Protokollbögen erstellen
Schriftlicher Arbeitsauftrag zum Plakat?

3 Reflexion

Literatur

Anderson, Ross J. (2008). *Security Engineering. A Guide to Building Dependable Distributed Systems*. 2. Aufl. Wiley. ISBN: 978-0-470-06852-6.

Hilbig, André (2014). »Entwicklung informatischer Kompetenzen zur Verhinderung von Mobbing«. Master-Thesis. Wuppertal: Fachgebiet Didaktik der Informatik – Bergische Universität. URL: http://www.ham.nw.schule.de/pub/bscw.cgi/4912964 (besucht am 08. 09. 2014).

Müller, Dorothee, Hrsg. (2012). *Spioncamp*. URL: http://ddi.uni-wuppertal.de/material/spioncamp.html (besucht am 31. 03. 2015).

Übungen zu diesem Projekt

Übung 1 Wer bist du, was machst du?

Ablauf:

- Alle werden durcheinander zu Pärchen gemischt.
- Stellt euch dem anderen vor, was macht ihr, was findet ihr toll, welche Hobbys usw? Nach 5min wird gewechselt.
- Schreibe nun für deine Partnerin oder deinen Partner ein Namensschild. Beschreibe dabei in einem kurzen Satz, was ihn oder sie besonders macht.

Übung 2 Bis hier hin und keinen Schritt weiter!

Ablauf:

- Es werden zwei Gruppen gebildet, die sich in zwei Linien mit ausreichend Platz gegenüber stellen.
- Auf ein Zeichen hin, fangen die Schülerinnen und Schüler der einen Linie an, individuell auf den Gegenüber zu zugehen. Zunächst soll der oder die jeweils Laufende selbst erspüren, wie weit er gehen darf. Danach werden die Rollen getauscht. Es werden keine verbalen oder nonverbalen Zeichen gegeben. Nur Blickkontakt ist erlaubt.
- Als zweiten Schritt soll der oder die jeweils Stehende der oder dem Laufenden deutlich machen, wo er stehen bleiben soll. Allerdings darf er dafür keinerlei sprachliche oder körperliche Zeichen geben.

Reflexion:

- Als erstes sollte deutlich werden, dass jeder seine eigene, individuelle Grenze hat → Privatsphäre ist nicht allgemein
- Offensichtlich haben wir auch ein Gespür für den persönlichen Raum des anderen.
- Außerdem können wir anderen mit winzigen, kaum erkennbaren Zeichen klar machen, wo sich diese Grenze befindet.
- Wie verändert sich die Position bei den jeweiligen Pärchen? Wie geht es dir damit? Fällt es dir schwer den anderen zu spüren, ihm ein Zeichen zu geben?
- Wie wichtig ist dir diese Grenze?

Erweiterung: Kann diese Grenze außer Kraft gesetzt werden? Wie kannst du die Grenze bei einem Facebook-Posting deutlich machen?

Es wäre möglich die Übung (evtl. nur mit einzelnen) zu wiederholen und dabei eine Sichtbarriere zwischen den Gruppen (Augen verbinden?) aufzubauen. Spannend ist die Frage, ob sich am Gefühl der Teilnehmenden und der Position etwas ändert.

Übung 3 Hey, du bist toll, so wie du bist!

Ablauf:

- Die Schülerinnen und Schüler werden in Pärchen eingeteilt – nach Möglichkeit sollten sie sich untereinander nicht näher kennen.
- Formuliere für die oder den andere[n] mindestens drei Stichpunkte, warum oder was an ihm besonders toll ist. Was macht ihn einzigartig und besonders?
- Die Kärtchen werden nicht vorgetragen und bleiben »privat«.

Reflexion:

- Wie war es für dich, für sie (ihn) etwas aufmunterndes und positives zu schreiben? Schwierig?
- Wie geht es dir mit deinem Kärtchen?

Übung 4 Sharing für Dummies – I like it

Aussagen:

1. Ich bin in Timo (Sabine) verliebt.
2. Der Informatikunterricht bei Herrn Hilbig ist total langweilig.
3. Heute ist mir … passiert, das war total peinlich!
4. Heute ist mir … passiert, das war echt cool!
5. Meine Telefonnummer lautet …
6. Ich habe heute Lust ins Kino zu gehen, wer noch?
7. Ich sehe heute so aus: [*Bild*]
8. Ich wohne in der …straße, Nummer …, in …

Angebote:

Angebote ggfs. an SuS anpassen

A Anruf
B Blog
C Chatroom
E E-Mail
I IM
N Soz. Netzwerk
S SMS
W Webseite

Arbeitsauftrag:

- Versuch dich mit den obigen Nachrichten/Aussagen zu identifizieren. Tu also so, als würdest du genau das jetzt gerade sagen wollen.
- Ordne die Aussagen dann in einer Tabelle einem Empfänger zu. An wen würdest du die jeweilige Nachricht senden – nahstehende Freunde, Bekannte, Internetfreunde, beliebig/unbeschränkt?
- Entscheide dich außerdem für eines der aufgeführten Angebote, um die Nachricht zu übermitteln (trage in die entsprechende Zelle einfach das Kürzel des Angebots ein).
- Es ist auch möglich, bestimmte Nachrichten für sich zu behalten. Dann einfach nichts eintragen!

	Mit bestem Freund – bester Freundin	Mit einem Bekanntem – einer Bekannten	Mit einem Internetfreund – einer Internetfreundin	beliebig mit jedem – jeder
1	A			
2				W
3		IM		
		…		

Tabelle 3: Beispielhafte Tabelle für die Übung 4

Hinweise zur Auswertung/Reflexion:

- Die Schülerinnen und Schüler sollen zunächst für sich die Tabelle erstellen und ausfüllen.
- Danach wird durch farblich kodierte Papierschnipsel die Tabelle auf einem größeren Plakat anonym nachgebildert.
- Typischerweise sollte eine Clusterung entstehen. Diese kann unterschiedliche Dimensionen haben. Auf der einen Seite scheinen bestimmte Aussagen eher mit bestimmten Personenkreisen geteilt zu werden. Hier gibt es also eine Art *Privatsphäre*, die intuitiv (und persönlich) entsteht. Auf der anderen Seite werden je nach erwünschtem Personenkreis (un)bewusst bestimmte Angebote ausgewählt.
- Es könnte sinnvoll sein, eine Art Conceptmap zu erstellen, in der die Angebote anhand ihrer zuvor ermittelten Privatsphäre (Publikationsrichtung) eingeordnet werden.