

Gottfried Wilhelm Leibniz Universität Hannover
Institut für Verteilte Systeme
Distributed Computing & Security Group

Seminar (Schlüsselkompetenz-Modul) **„Sicherheit und Privatsphäre in der Gesellschaft“**

Dozent: Prof. Dr. Matthew Smith in Kooperation mit apl. Prof. Dr. Stender-Vorwachs
(Rechtswissenschaften) und Dr. Matthias Rieger (Sozialwissenschaften)

Termin: donnerstags, 10 - 12 Uhr, Raum B028 Gebäude 1210

Themenvergabe: 20. Oktober 2011

Erster Vortragstermin: 03. November 2011

In diesem interdisziplinären Seminar werden gesellschaftlich relevante Themen der IT-Sicherheit in Zusammenarbeit mit den Sozial- und Rechtswissenschaften der Leibniz Universität Hannover bearbeitet. Themen aus dem Bereich Sicherheit und Privatsphäre werden dabei jeweils durch Studierende der drei verschiedenen Fachrichtungen aus der jeweiligen Sichtweise betrachtet. Das Seminar richtet sich an Studierende, die Themen der IT-Sicherheit interdisziplinär erarbeiten und gemeinsam diskutieren wollen. Der Schwerpunkt liegt auf der gemeinsamen Arbeit sowie dem Erarbeiten eines Themas des eigenen Studienfachs.

Ablauf

An jedem Seminartermin soll eines der zu vergebenen Themen vorgestellt und diskutiert werden. Je ein Studierender jeder Fachrichtung stellt dazu das Thema mit seinem jeweiligen Fachschwerpunkt vor. Die Inhalte sind so zu vermitteln, dass sie allen Teilnehmenden verständlich, jedoch in notwendiger Tiefe, dargestellt werden. Jeder Studierende hält einen Vortrag und leitet die folgende Diskussion (in Summe 30 Minuten). Die Veranstaltung sieht eine Abstimmung der Studierenden der verschiedenen Fachrichtungen vor. Die genaue Ausgestaltung und Schwerpunktsetzung eines Themas obliegt den Studierenden.

Aus der PO09

(2.4 Kompetenzbereich Nebenfach (Master)) In diesem Pflicht-Kompetenzbereich müssen 12-18 Leistungspunkte erworben werden. Dazu muss genau eines der folgenden Master-Nebenfachmodule gewählt werden, das zu bestehen ist. Außerdem kann ein Schlüsselkompetenz-Modul aus dem einschlägigen Angebot der Universität gewählt werden, zu dem mindestens 2 Leistungspunkte als Studienleistung erworben werden können.

Themen

Überwachung von Tauschbörsen zur Durchsetzung von Urheberrechten

Um das unautorisierte Vervielfältigen von urheberrechtsgeschützten Daten mit Hilfe von Internettauschbörsen bestrafen zu können, werden gezielt Technologien eingesetzt, die eine Überwachung der Datenströme in Internettauschbörsen anstreben. Es soll diskutiert werden inwiefern Technologien zu diesem Zweck geeignet und welche rechtlichen Implikationen aus Überwachungsergebnissen ableitbar sind.

Digital Rights Management

DRM ist ein Verfahren, um die Verwendung und Weitergabe digitaler Medien kontrollieren zu können. Zu den Medien gehören neben Musik auch Filme, Dokumente und Bücher. Eine Vielzahl solcher Systeme wurde von verschiedensten Firmen entwickelt und eingesetzt. Interessante Fragestellungen in diesem Bereich könnten unter anderem sein:

- Welche DRM Technologien /Kopierschutzmechanismen werden heutzutage eingesetzt?
- Wie sicher sind die Rechte mit diesen Verfahren durchsetzbar?
- DRM ist bei bestimmten Medien auf dem Rückzug. Wie steht es um die Zukunft von DRM?

Im Rahmen dieses Themas soll zudem die Frage erörtert werden, ob das unautorisierte Vervielfältigen von elektronischen Daten mit einem Diebstahl von physischen Gütern gleichsetzbar ist. Außerdem sollte diskutiert werden warum das unautorisierte Vervielfältigen von elektronischen Daten von Teilen der Bevölkerung als Bagatelle eingestuft wird.

Privatsphäre im Zeitalter des Internet

Wenige Internetnutzer sind sich des potentiellen Angriffes auf ihre persönlichen Daten im Internet bewusst. Im Vergleich zur „herkömmlichen“ Realität sind Daten nach der Bekanntgabe im Internet nur schwerlich zu kontrollieren. Weder technisch noch rechtlich sind hier umfassende Möglichkeiten gegeben, die oft auch von der Kooperation des Unternehmens abhängt (z.B. das Löschen eines Facebookprofils und das Vernichten der zugehörigen Daten). Es ergeben sich in diesem Bereich verschiedenste Fragestellungen die aus mehreren Blickwinkeln allgemein oder im speziellen betrachtet werden können. Hier einige exemplarische Beispiele:

- Warum braucht eine Gesellschaft Privatsphäre?
- Wie viel Privatsphäre benötigt man im Internet tatsächlich bzw. funktioniert das Internet wie wir es heute kennen ohne die Vernachlässigung der Privatssphäre?
- Bestehen rechtliche Möglichkeiten zur effektiven Sicherung von Privatsphäre?
- Welche technischen Möglichkeiten werden derzeit zur Sicherung der Privatsphäre eingesetzt?
- Welche Rolle spielen Services wie Google oder Facebook dabei zu leichtsinnig mit privaten Daten umzugehen?
- Wem kann man trauen? Aktuelle Data Breaches im Rückblick, z.B. Sony PSN.

Welche Rolle spielt das Internet bei aktuellen Unruhen, z.B. in Nordafrika oder England?

Die aktuellen Unruhen in Nordafrika wurden teilweise durch Internettechnologien unterstützt. Menschen nutzten Twitter oder Facebook, um Nachricht in die Welt zu senden oder Demonstrationen zu organisieren. Es wurden Bilder und Videos von Auseinandersetzungen auf Flickr und Youtube veröffentlicht. Im Rahmen dieses Themas soll es darum gehen zu diskutieren welche technischen Möglichkeiten am intensivsten genutzt wurden und ob sie zwingende Voraussetzung für eine Mobilisierung der Bevölkerung in Ländern wie Ägypten, Libyen oder Syrien sind bzw. waren. Die neuen Techniken ermöglichten Meinungsäußerungen trotz Unterdrückung/Zensur.

Wikileaks: Robin Hood der Moderne oder eine Gefahr für westliche Demokratien?

WikiLeaks ist eine Website des Typs Enthüllungsplattform, auf der Dokumente anonym veröffentlicht werden, die durch Geheimhaltung als Verschlussache, Vertraulichkeit, Zensur oder auf sonstige Weise in ihrer Zugänglichkeit beschränkt sind. WikiLeaks setzt dabei ein grundsätzliches öffentliches Interesse an den Informationen voraus. Das Projekt gibt an, denen zur Seite stehen zu wollen, „die unethisches Verhalten in ihren eigenen Regierungen und Unternehmen enthüllen wollen“. Dazu wurde nach eigenen Angaben ein System „für die massenweise und nicht auf den Absender zurückzuführende Veröffentlichung von geheimen Informationen und Analysen“ geschaffen¹. Hierbei soll im technischen Sinne die Infrastruktur soweit möglich diskutiert werden. Im juristischen Kontext sind interessante Fragestellungen beispielsweise die Haftbarkeit von Wikileaks für veröffentlichte Daten. Im gesellschaftlichen Kontext ist eine Erörterung der Akzeptanz von Whistle-Blowing Services in der Bevölkerung interessant.

Alterseinstufung von Webseiten

Mit dem neuen Jugendmedienschutz-Staatsvertrag (JMStV) müssen Anbieter von Inhalten diese anhand ihrer Erziehungs- und Entwicklungsbeeinträchtigung für Kinder einstufen². Im Wesentlichen soll hier diskutiert werden, welche technischen Möglichkeiten zu einer Klassifikation von Inhalten zur Verfügung stehen und inwiefern diese juristische Verbindlichkeit besitzen können. Außerdem soll diskutiert werden inwiefern durch eine solche Klassifikation der freie Informationsaustausch von Informationen im Internet möglicherweise behindert wird. Technisch von Interesse ist außerdem die automatische Einstufung von Inhalten und deren Effizienz/Korrektheit.

Internetsperren: Potentiale und Gefahren

Das Gesetz zur Erschwerung des Zugangs zu kinderpornographischen Inhalten in Kommunikationsnetzen (Zugangserschwerungsgesetz, ZugErschwG) soll in Deutschland den Zugang zu Webseiten mit Darstellungen sexueller Handlungen von und an Kindern (Kinderpornografie) im World Wide Web erschweren. Eine Strafverfolgung allein wegen des Aufrufs einer gesperrten Webseite bzw. Domain ist nach §5 ZugErschwG untersagt³. Es soll diskutiert werden inwiefern technische Möglichkeiten existieren, die ein wirkungsvolles Sperren von Internetinhalten ermöglichen und welche Möglichkeiten es dann außerdem gibt diese Sperren zu umgehen. Aus juristischer Sicht interessant wäre eine Evaluation wie Sperrlisten organisiert sein müssten,

¹Quelle: <http://de.wikipedia.org/wiki/WikiLeaks>

²Quelle: <http://ak-zensur.de/jmstv/>

³Quelle: <http://de.wikipedia.org/wiki/Zugangserschwerungsgesetz>

damit eine willkürliche und juristisch fragwürdige Auswahl von Inhalten vermieden werden kann. Außerdem ist interessant inwiefern bei dieser Technologie das Potential zu Missbrauch von Seiten des Staates bzw. privatwirtschaftlicher Instanzen besteht.

Vorratsdatenspeicherung: Wie viel Überwachung seitens des Staates ist notwendig?

Vorratsdatenspeicherung bezeichnet die Verpflichtung der Anbieter von Telekommunikationsdiensten zur Registrierung von elektronischen Kommunikationsvorgängen, ohne dass ein Anfangsverdacht oder eine konkrete Gefahr besteht (Speicherung bestimmter Daten auf Vorrat). Erklärter Zweck der Vorratsdatenspeicherung ist die verbesserte Möglichkeit der Verhütung und Verfolgung von schweren Straftaten (Terrorismus). Die Vorratsdatenspeicherung ist eine Vorstufe der Telekommunikationsüberwachung. Die auf Vorrat zu speichernden Daten erlauben weitgehende Analysen persönlicher sozialer Netzwerke. Mit Hilfe der auf Vorrat zu speichernden Daten lässt sich, ohne dass auf Kommunikationsinhalte zugegriffen wird, das Kommunikationsverhalten jedes Teilnehmers analysieren. In dem Maße, in dem die Kommunikation über elektronische Medien zunimmt, wird die Bedeutung solcher Analysen für die Erstellung von Persönlichkeitsprofilen wachsen. Das deutsche Bundesverfassungsgericht erklärte die deutschen Vorschriften zur Vorratsdatenspeicherung mit einem Urteil vom 2. März 2010 für verfassungswidrig und nichtig. Das Urteil verpflichtete deutsche Telekommunikationsanbieter zur sofortigen Löschung der bis dahin gesammelten Daten. Zur Begründung gab das Gericht an, dass das Gesetz zur anlasslosen Speicherung umfangreicher Daten sämtlicher Nutzer elektronischer Kommunikationsdienste keine konkreten Maßnahmen zur Datensicherheit vorsehe und zudem die Hürden für staatliche Zugriffe auf die Daten zu niedrig seien. Eine Vorratsdatenspeicherung verstoße allerdings nicht generell gegen das Grundgesetz⁴.

Der Bundestrojaner: Ein effektives Mittel zur Terroristenbekämpfung?

Als Online-Durchsuchung wird der verdeckte staatliche Zugriff auf fremde informationstechnische Systeme über Kommunikationsnetze bezeichnet. Der Begriff umfasst dabei sowohl den einmaligen Zugriff (Online-Durchsicht) wie auch die, sich über einen längeren Zeitraum erstreckende Online-Überwachung. Als bisher in Deutschland gesetzlich nicht ausdrücklich geregelte Methode staatlicher Informationsgewinnung soll die Online-Durchsuchung im Rahmen der Strafverfolgung, zur Gefahrenabwehr oder zur nachrichtendienstlichen Informationsbeschaffung eingesetzt werden. Ziel der kriminalpolizeilichen Online-Durchsuchung soll sein, in Einzelfällen und nach einem richterlichen Beschluss die privaten Computer von mutmaßlichen Schwerstkriminellen zu durchsuchen, um Hinweise auf mögliche kriminelle Netze zu erlangen. Am 27. Februar 2008 entschied das Bundesverfassungsgericht, dass die Regelungen zur Online-Durchsuchung in Nordrhein-Westfalen verfassungswidrig und Online-Durchsuchungen prinzipiell nur unter strengen Auflagen zulässig sind.⁵

CyberWar: Droht uns der digitale Weltkrieg?

Welche neuen Gefahren drohen der Gesellschaft durch den sogenannten CyberWar? CyberWar ist ein Oberbegriff für das Eindringen in Computersysteme, die Veränderung von Inhalten (z.B. zu Propagandazwecken), diverse Formen des Social Engineering, Störung und Unterdrückung von Internetdiensten, Sabotage und Einschleusen kompromittierter Hardware.

⁴Quelle: <http://de.wikipedia.org/wiki/Vorratsdatenspeicherung>

⁵Quelle: <http://de.wikipedia.org/wiki/Online-Durchsuchung>

Wie real sind diese Gefahren und welche Bedeutung kann ihnen zugeschrieben werden? Gibt es bereits Kriege im digitalen Raum?

TOR und anonyme Kommunikation: Potentiale und Gefahren

Tor ist ein Netzwerk zur Anonymisierung der Verbindungsdaten. Es wird für TCP-Verbindungen eingesetzt und kann beispielsweise für Web-Browsing, Instant Messaging, IRC, SSH, E-Mail, P2P und andere benutzt werden. Tor schützt vor der Analyse des Datenverkehrs seiner Nutzer⁶. Aus technischer Sicht ist eine Analyse der zugrundeliegenden Sicherheitsinfrastruktur interessant. Aus juristischer Sicht kann evaluiert werden inwiefern der Betrieb eines Exit-Nodes (der Schnittstelle zwischen TOR und dem unverschlüsselten Internet) zu einer Störerhaftung des Betreibenden führen kann. Außerdem stellt sich die Frage, inwiefern Anonymität gesellschaftlich notwendig ist.

ePerso – Sinnvolles Werkzeug zur Identifizierung im Internet oder Risiko?

Neben den neuen Möglichkeiten, die der ePerso bietet bringt er ebenso neue Probleme mit sich. Ist die Identität einer Person im Internet gesichert? Welche Probleme können sich ergeben? Welche Vorteile bietet die neue Technologie?

- http://www.bmi.bund.de/DE/Themen/Sicherheit/PaesseAusweise/ePersonalausweis/ePersonalausweis_node.html
- <http://www.heise.de/security/meldung/Phishing-Demo-zum-ePerso-Update-1170481.html>

ANONYMOUS – Kriminelle Vereinigung oder Robin Hood der Moderne

Anonymous ist ein weltweit operierendes Kollektiv nicht näher bekannter Personen. Anfangs als Spaßbewegung aus dem Imageboard 4chan hervorgegangen, tritt das Kollektiv seit 2008 vermehrt durch verschiedene Protestaktionen für die Redefreiheit und die Freiheit des Internets in Erscheinung. Seine Mitglieder agierten anfangs nur im Internet, später breiteten sich die Aktivitäten auch außerhalb der virtuellen Kommunikationssphäre des Internets aus⁷. In diesem Kontext ist aus technischem Sinne interessant welche Angriffstechniken verwandt wurden und inwiefern diese zu Erfolg führten bzw. wie potentielle Gegenmaßnahmen aussehen können. Aus sozialwissenschaftlicher Perspektive ist eine Untersuchung des Verhaltens von ANONYMOUS im Hinblick auf die „Hacker-Ethik“ und die hohe Akzeptanz der Gruppe in der Gesellschaft interessant. Auch juristisch kann man untersuchen inwiefern gerade so genannten DDoS-Angriffe, die üblicherweise aus vielen verschiedenen Ländern initiiert werden, rechtlich zu handhaben sind. Interessant ist auch die Frage inwiefern ein Hacker-Angriffs von Zivilisten als kriegerischer Akt eines Staates bewertet werden kann (siehe z.B. <http://www.spiegel.de/netzwelt/web/0,1518,767292,00.html>).

Bei Interesse oder weiteren Fragen wenden Sie sich bitte an:

Distributed Computing & Security Group (lehre@dcsec.uni~)

⁶Quelle: http://de.wikipedia.org/wiki/Tor_%28Netzwerk%29

⁷Quelle: http://de.wikipedia.org/wiki/Anonymous_%28Kollektiv%29, <http://www.spiegel.de/netzwelt/web/0,1518,733520,00.html>