

Informationssicherheit – SoSe 2023

Organisatorisches & Motivation

Prof. Dr. Holger Schmidt
holger.schmidt@fh-dortmund.de

Fachhochschule Dortmund
Fachbereich Informatik
Professur für IT-Sicherheit, Informatik

IT-Sicherheit, Informatik

- ▶ Prof. Dr. Holger Schmidt
- ▶ **Informationssicherheit** (46813)
 - ▶ Informatik (Bachelor, 4. Sem., Pflicht)
 - ▶ Informatik Dual (Bachelor, 2. Sem., Pflicht)
- ▶ **Datenschutz und Datensicherheit** (46813)
entspricht inhaltlich der Veranstaltung Informationssicherheit
 - ▶ Wirtschaftsinformatik (Bachelor, 6. Sem., Wahlpflicht)
- ▶ **Informationssicherheit für die Medizin** (46815)
basiert inhaltlich auf der Veranstaltung Informationssicherheit,
ergänzt um einen Medizinkontext
 - ▶ Medizinische Informatik (Bachelor, 4. Sem., Pflicht)
 - ▶ Medizinische Informatik Dual (Bachelor, 4. Sem., Pflicht)

► Fortgeschrittene Informationssicherheit (46900)

- ▶ Informatik (Bachelor, 4.-6. Sem., Wahlpflicht)
- ▶ Informatik Dual (Bachelor, 5.-9.. Sem., Wahlpflicht)
- ▶ Medizinische Informatik (Bachelor, 5.-7. Sem., Wahlpflicht)
- ▶ Medizinische Informatik Dual (Bachelor, 7.-9. Sem., Wahlpflicht)

► Ausgewählte Aspekte der Informationssicherheit (46857)

- ▶ Informatik (Master, 1.-3. Sem., Wahlpflicht)
- ▶ Medizinische Informatik (Master, 1.-3. Sem., Wahlpflicht)
- ▶ Wirtschaftsinformatik (Master, 1.-3. Sem., Wahlpflicht)

► Projekt- und Abschlussarbeiten

Organisatorisches

Konzept und Termine

Materialien ILIAS (<https://www.ilias.fh-dortmund.de/>)

Vorlesung 2 SWS Vorlesung in Präsenz

Dienstags, 12-13:30 Uhr; Beginn: 28.03.2023; Raum A.E.01

Vorlesungsfolien und **handschriftliche Notizen**

Übung 2 SWS Übung in Präsenz

Termine siehe Studienportal
(<https://portal.fh-dortmund.de/>)

Wöchentliche **Bearbeitung von Übungsblättern** als
Hausaufgaben (Aufwand ca. 1-4h!)

Präsentation der Hausaufgaben durch Studierende

Medizinische Informatik Zusatztermin Montags, 08.05.2023,
10:15-13:35 Uhr; Raum A.E.02

Prüfung 90-minütige Klausur

- ▶ **Votiersystem für Bonuspunkte** gemäß §27 RahmenPO bzw. der jeweils gültigen PO der Studiengänge
- ▶ Als Paar **mindestens 60%** aller Übungsaufgaben (# 35 insgesamt) zum Präsentieren votiert
- ▶ Votierung zu Beginn jeder Übung durch Ankreuzen auf Votierliste, d. h. wer votieren möchte muss anwesend sein (um dann ggf. zu präsentieren)
- ▶ Welches Paar welche Übungsaufgabe präsentiert wird in jeweiliger Übung **zufällig bestimmt**. Nichtanwesenheit führt zu Bewertung der Präsentation als nicht erfolgreich.

- ▶ Präsentation so, dass eine **(nahezu) korrekte Lösung** gezeigt wird, die auch erklärt werden kann. Andernfalls wird die Präsentation als nicht erfolgreich bewertet.
- ▶ Nicht erfolgreiches Präsentieren kann einmalig ausgeglichen werden.
- ▶ Nach Votierung von **mindestens 60%** aller Übungsaufgaben und **mindestens zweimaliger erfolgreicher** Präsentation werden **10 Bonuspunkte** für die Klausur vergeben.
- ▶ Die Bonuspunkte verfallen mit Beginn der neuen Vorlesung im übernächsten Semester.

- ▶ *IT-Sicherheit – Konzepte - Verfahren - Protokolle* von Eckert (2023)
- ▶ *Kryptografie – Verfahren - Protokolle - Infrastrukturen* von Schmeh (2016)

Ergänzend:

- ▶ *Security Engineering: A Guide to Building Dependable Distributed Systems* von Anderson (2020)
- ▶ ISO/IEC 27000, 2018

Die Literatur ist typischerweise in der Hochschulbibliothek (auch als eBooks) verfügbar.

Hacking Hinweise

Earl Boebert: „In my view, a defender who doesn't know how to attack is no defender at all.“

- ▶ Die in der Veranstaltung behandelten Schwachstellen und Angriffe dienen ausschließlich der Ausbildung im Rahmen des Studiums.
- ▶ Entsprechend dürfen auf keinen Fall Schwachstellen ausgenutzt und Angriffe durchgeführt werden, denn dies hat in der Regel **strafrechtliche Konsequenzen** im Sinne hoher Geld- und Haftstrafen.
- ▶ Sogenanntes „**Pentesting**“ (**Ethical Hacking**) darf (wenn überhaupt) nur unter Laborbedingungen durchgeführt werden, d. h. ohne dabei einen laufenden IT-Betrieb zu stören und nur unter Verwendung vollständig lokaler, nicht vernetzter sowie eigener Infrastruktur.
- ▶ Im Zweifel **erkundigen Sie sich vorab** bei Prof. Dr. Holger Schmidt.

Prüfungshinweise

- ▶ Sämtliche in der Vorlesung und Übung behandelten Inhalte sind relevant für die Klausur (siehe auch Lernziele).¹
- ▶ Die Klausuraufgaben orientieren sich typischerweise an den Übungsaufgaben und natürlich an den in der Vorlesung vorgestellten Materialien.
- ▶ Übungsaufgaben, die hinsichtlich des Aufgabentyps und Schwierigkeitsgrades auch Klausuraufgaben sein könnten, sind als solche mit einem „K“ markiert. Dabei ist auch die zur Lösung veranschlagte Zeit angegeben (als grober Richtwert, relativ z. B. zur Qualifikation).
- ▶ Übungsaufgaben ohne entsprechende Markierung sind nicht per se als Klausuraufgaben ausgeschlossen.
- ▶ Klausureinsicht gemäß §13 RahmenPO

¹Ausnahmen: nicht für die Klausur relevant sind die mit OWASP WebGoat durchgeführten Übungsaufgaben 2.2 und 2.3 sowie die Vorlesungseinheit 10 „Sichere Software Entwicklung“.

Nutzungsbedingungen

Nutzungsbedingungen

- ▶ Das gesamte Lehr- und Lernmaterial (Vorlesungsfolien, Vorlesungsnotizen, Übungsblätter, Screencasts, etc.) wird ausschließlich begleitend zur diessemestrigen Lehrveranstaltung zur Verfügung gestellt.
- ▶ Der Zugriff auf diese Materialien ist durch ein Passwort geschützt und wird somit nur den Veranstaltungsteilnehmern ermöglicht.
- ▶ Eine Weiterverbreitung dieser Materialien, insbesondere auch über das Internet, ist ausdrücklich untersagt bzw. bedarf einer vorherigen expliziten Erlaubnis von Prof. Dr. Holger Schmidt.

Themen & Lernziele

Themen & Relevanz

- ▶ Terminologie
- ▶ Standards & Recht
- ▶ Faktor Mensch & Organisatorische Sicherheitsmaßnahmen
- ▶ Technische Sicherheitsmaßnahmen
 - ▶ Kryptographische Verfahren
 - ▶ Authentifikation
 - ▶ Zugriffskontrolle
- ▶ Entwicklung sicherer Software

OWASP Top 10¹

- A01** Broken Access Control
- A02** Cryptographic Failures
- A03** Injection
- A04** Insecure Design
- A07** Identification and Authentication Failures
- A08** Software and Data Integrity Failures

¹<https://owasp.org/Top10/>, aufgerufen am 28. Juni 2023

Die Studierenden sind in der Lage,

- ▶ grundlegende **Terminologie** der Informationssicherheit zu definieren, zu differenzieren und zu erklären.
- ▶ die zentrale Bedeutung von **Standardisierung** in der Informationssicherheit zu verstehen und methodisch abzubilden.
- ▶ selbständig Informationen über **Schwachstellen und Bedrohungen** zu sichten, zu analysieren und darauf aufbauend fundierte Entscheidungen zu treffen.
- ▶ **organisatorische und technische Sicherheitsmaßnahmen** zu erklären und anzuwenden.

The diagram is a word cloud centered around the concept of information security. The most prominent word is 'Sicherheit' (Security), which is rendered in a large, bold, dark blue font. Surrounding it are several other large, dark blue words: 'Faktor Mensch' (Factor Human), 'Sicherheitsstandards' (Security standards), 'Entwicklung sicherer Software' (Development of secure software), 'Verfügbarkeit' (Availability), 'Vertraulichkeit' (Confidentiality), 'Integrität' (Integrity), 'Schwachstellen' (Weak points), and 'Bedrohungen' (Threats). Interspersed among these large words are numerous smaller, lighter blue words representing specific technologies, protocols, and management practices. These include: 'Security Awareness', 'Digitale Signaturen', 'Sicherheitsprotokolle', 'Physikalische Sicherheit', 'Informationsflußkontrolle', 'Privacy-Enhancing Technologien', 'Intrusion und Malware Detection', 'Zugriffskontrolle', 'Fallbeispiele', 'Kryptografie', 'PKI', 'Authentifikation', 'Zertifikate', 'Betriebssystemsicherheit', 'Sicherheitsmanagement', 'Biometrische Systeme', 'Netzwerksicherheit', and 'Trusted Computing'. The overall layout is organic and radiating from the central 'Sicherheit' word.

(White Hat) Hacker



Motivation



Quelle des Logos:

<http://heartbleed.com/>,
aufgerufen am 28. Juni 2023

Heartbleed

Bruce Schneier²:

„Catastrophic“ is the right word. On the scale of 1 to 10, this is an 11.“

- ▶ Schwachstelle (CVE-2014-0160) in **OpenSSL**
- ▶ Offenlegung geheimer Schlüssel und dadurch nachträgliche Entschlüsselung aufgezeichneter SSL/TLS verschlüsselter Verbindungen
- ▶ Sehr große Verbreitung von OpenSSL im Web, Kommunikation, Embedded Systems u. v. m.
- ▶ **Heartbleed** bestand 27 Monate: veröffentlicht am 14.03.2012 mit OpenSSL 1.0.1 und behoben am 07.04.2014 mit OpenSSL 1.0.1g



Quelle des Logos:
<http://heartbleed.com/>,
aufgerufen am 28. Juni 2023

²<https://www.schneier.com/blog/archives/2014/04/heartbleed.html>, aufgerufen am 28. Juni 2023

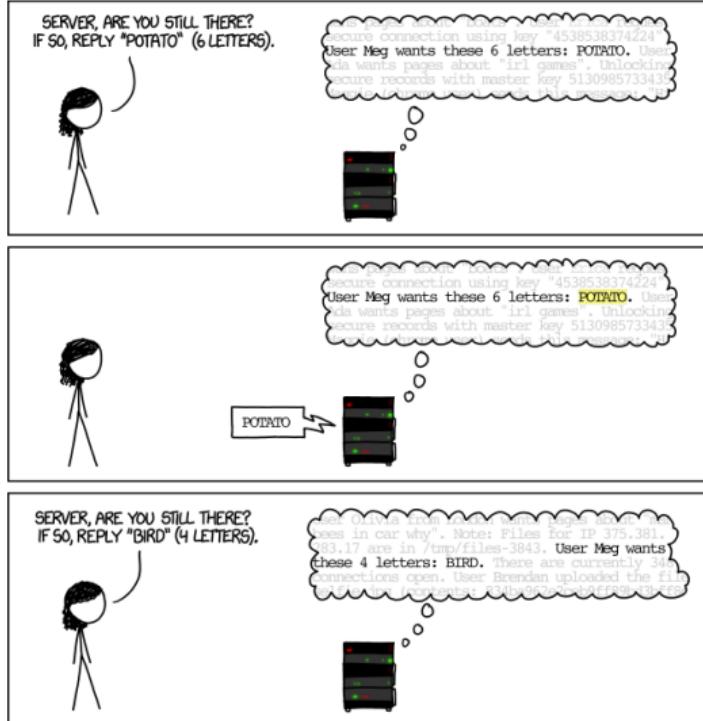
- ▶ **Secure Socket Layer** (SSL) bzw. die mit Version 3.0 eingeführte Bezeichnung **Transport Layer Security** (TLS)
- ▶ SSL/TLS nutzt ein symmetrisches Kryptosystem, d. h. beide Teilnehmer (Server und Client) verwenden den gleichen Schlüssel.
- ▶ Die Schlüssel werden individuell bei der Erstellung einer Session zwischen Client und Server generiert.
- ▶ SSL/TLS wird typischerweise bei HTTPS eingesetzt.
- ▶ OpenSSL ist eine der verbreitetsten Implementierungen von SSL/TLS.

Namensgebung

- ▶ **Heartbleed** stammt vom Namen der betroffenen **Heartbeat**-Komponente RFC 6520³ (Requests for Comments) von OpenSSL ab.
- ▶ Heartbeat simuliert einen Herzschlag durch regelmäßigen Austausch von Datenpaketen (Payload) zwischen Server und Client.
- ▶ Heartbeat dient als Mechanismus zur Aufrechterhaltung einer SSL/TLS Verbindung und als Bestätigung der **Verfügbarkeit** beider Seiten.

³<https://tools.ietf.org/html/rfc6520>, aufgerufen am 28. Juni 2023

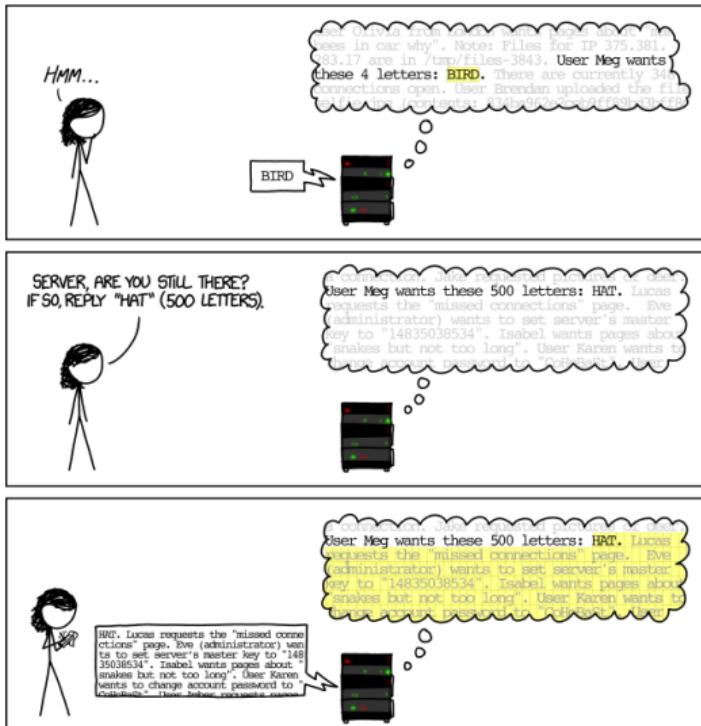
xkcd Webcomic – Teil 1



„Heartbleed Explanation“, <https://xkcd.com/1354/>, aufgerufen am 28. Juni 2023,
lizenziert unter CC BY-NC 2.5.⁴

⁴<https://creativecommons.org/licenses/by-nc/2.5/>

xkcd Webcomic – Teil 2



„Heartbleed Explanation“, <https://xkcd.com/1354/>, aufgerufen am 28. Juni 2023,
lizenziert unter CC BY-NC 2.5.⁵

⁵<https://creativecommons.org/licenses/by-nc/2.5/>

- ▶ OpenSSL ist größtenteils in der Programmiersprache C verfasst.
- ▶ Ursächlich für Heartbleed ist ein **Programmierfehler**:
 - ▶ Prüfung einer EingabevARIABLE versäumt, in der die Länge der zurückzuliefernden Daten mitgeteilt wird
 - ▶ Dadurch ist ein lesender Zugriff über die Grenzen der zurückzuliefernden Daten hinaus möglich (**buffer over-read**).

Auswirkungen:

- Offenlegung von kritischen Daten, z. B. Benutzernamen mit Passwörtern und privater Schlüssel des Serverzertifikats

Fehlerbehebung:

- Ignorieren von Heartbeat-Nachrichten, die nach mehr Daten fragen als für den Payload nötig

Analyse:

- Fehler in Komponente zur Gewährleistung der Verbindungsverfügbarkeit bedroht Maßnahmen die Vertraulichkeitsziele implementieren
- Banale Fehler (unvollständige Implementierung)
- Performanz über Sicherheit (OpenSSL umgeht vorhandene C-Sicherheitsmechanismen)
- Keine Rollentrennung (Spezifikation, Programmierung und Validierung durch eine Person)

- ▶ Fehler in Funktion `tls1_process_heartbeat(SSL *s)`⁶
- ▶ Eine **HeartbeatMessage** wird via **SSL3_RECORD** Struct übermittelt.
- ▶ **SSL3_RECORD** enthält u. a. die Variablen **length** als Beschreibung der Anzahl übermittelter Bytes und **data** als Zeiger auf den Anfang der **HeartbeatMessage**.
- ▶ Die Variable **payload_length** der **HeartbeatMessage** beschreibt die Anzahl der Bytes des zurückzusendenden Payloads.
- ▶ Der Sender der **HeartbeatMessage** bestimmt die Größe des Payloads und kann diese wegen fehlender Überprüfung gezielt missbrauchen.
- ▶ **SSL3_RECORD length** und **HeartbeatMessage payload_length** müssten verglichen und auf Abweichungen hin überprüft werden.
- ▶ Angreifer kann von **SSL3_RECORD length** abweichende Payloads anfordern und erhält diese auch.

⁶https://git.openssl.org/gitweb/?p=openssl.git;a=blob;f=ssl/t1_lib.c;h=c5c805cce286d12d81c5fdccfe9173d61a68ee82;hb=4817504d069b4c5082161b02a22116ad75f822b1, aufgerufen am 28. Juni 2023

- ▶ Die Entwickler von OpenSSL haben einen Patch (Version 1.0.1g)⁷ veröffentlicht („Patch and pray“).
- ▶ Alternativ kann bzw. konnte jeder Zeit OpenSSL ohne die betroffene Heartbeat-Komponente kompiliert werden (-DOPENSSL_NO_HEARTBEATS)
- ▶ Besser: Designprinzip **Perfect Forward Secrecy**

⁷https://git.openssl.org/gitweb/?p=openssl.git;a=blobdiff;f=ssl/t1_lib.c;h=bcb99b819dadaebdf2c8f88d92ee9024c45f9df3;hp=a2e2475d136f33fa26958fd192b8ace158c4899d;hb=731f431497f463f3a2a97236fe0187b11c44aead;hpb=4e6c12f3088d3ee5747ec9e16d03fc671b8f40be, aufgerufen am 28. Juni 2023

Nach 3 Jahren ... OpenSSL blutet noch



Quelle: <https://twitter.com/achillean/status/823275177802862592/photo/1>,

aufgerufen am 28. Juni 2023

Zusammenfassung

Zusammenfassung

- ▶ Organisatorische Rahmenbedingungen festgelegt
- ▶ Themen und Lernziele übergreifend definiert
- ▶ Motivierendes Beispiel kennengelernt

Weiterführende Literatur

Weiterführende Literatur

- ▶ <http://heartbleed.com/>, aufgerufen am 28. Juni 2023
- ▶ <https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-0160>,
aufgerufen am 28. Juni 2023
- ▶ <https://tools.ietf.org/html/rfc6520>, aufgerufen am 28. Juni 2023
- ▶ https://www.theregister.co.uk/2014/04/09/heartbleed_explained/,
aufgerufen am 28. Juni 2023
- ▶ <https://nakedsecurity.sophos.com/2014/04/08/anatomy-of-a-data-leak-bug-openssl-heartbleed/>, aufgerufen am 28. Juni 2023
- ▶ <https://git.openssl.org/>, aufgerufen am 28. Juni 2023

-  Anderson, R. (2020). *Security Engineering: A Guide to Building Dependable Distributed Systems* (3. Aufl.). John Wiley & Sons Inc.
<https://www.cl.cam.ac.uk/~rja14/book.html> (siehe S. 9).
-  Eckert, C. (2023). *IT-Sicherheit: Konzepte - Verfahren - Protokolle* (11. Aufl.). De Gruyter Oldenbourg. (Siehe S. 9).
-  ISO/IEC 27000. (2018). ISO/IEC 27000: Information technology – Security techniques – Information security management systems – Overview and vocabulary. (Siehe S. 9).
-  Schmeh, K. (2016). *Kryptografie – Verfahren - Protokolle - Infrastrukturen* (6. Aufl.). dpunkt.verlag. (Siehe S. 9).