Die Entwicklung eines digitalen Praktikums der Cybersicherheit im Bereich „Smart Home“

Victor Jüttner[1,2] und Erik Buchmann[2,3]

Abstract: Die Cybersicherheit ist ein Querschnittsthema, das alle Bereiche der Informatik berührt. Entsprechend wichtig ist es, Studierenden praktische Erfahrungen zu aktuellen Themen in diesem Gebiet zu vermitteln. Dies wird schwierig, wenn die Studierendenzahlen größer werden. Wünschenswert ist darum ein Praktikum der Cybersicherheit, das einen aktuellen Themenquerschnitt für Studierende niederschwellig abbildet, einen digitalen Zugang zu Experimenten bietet, und ohne viel Lehrpersonal oder Tutoren auskommt. Dieser Praxisbeitrag beschreibt unsere Erfahrungen aus einem Praktikum der Cybersicherheit, das eine Experimentierplattform für so ein digitales Praktikum entwickelt hat.

1 Einführung

Aufgrund seiner Komplexität existieren für die Cybersicherheit nur wenige praktische digitale Lehrangebote, z. B. der OWASP Juice Shop[4], Hack the Box[5] oder GRFICSv2[6]. Diese sind eher hochschwellig nutzbar, setzen eine intensive Betreuung und erhebliche Fachkenntnisse voraus, und zielen auf inhaltlich „tiefe“ Kenntnisse.

Für die Vermittlung von „breit“ angelegten, praktischen Grundlagen der Cybersicherheit [SF14] an größere Studierendengruppen sind jedoch andere Anforderungen zu setzen, insbesondere wenn nur Kenntnisse aus einem Informatik- oder Informatik-nahen Bachelorabschluss vorausgesetzt werden können. Hier ist ein Praktikum der Cybersicherheit gefragt, dass ein aktuelles Einsatzszenario in der Breite abdeckt, anstelle sich beispielsweise auf Penetrationstests zu fokussieren. Das Praktikum sollte niederschwellig angelegt sein, d. h., einen digitalen oder hybriden Zugang zu einer Experimentierplattform und weiteren Materialien wie Lehrvideos oder Hintergrundmaterialien bieten. Insbesondere sollte es auch möglich sein, auf diese Weise größere Zahlen von Studierenden zu betreuen.

In diesem Praxisbeitrag geht es um ein Präsenz-Praktikum, das eine Smart Home-Experimentierplattform für ein digitales Praktikum der Cybersicherheit entwickelt hat. Smart Home-Geräte sind z. B. über das Smartphone schaltbare Steckdosen, Türsensoren oder

[1] Dept. of Computer Science, Leipzig University, Germany. juettner@informatik.uni-leipzig.de
[2] Center for Scalable Data Analytics and Artificial Intelligence (ScaDS.AI) Dresden/Leipzig, Germany.
[3] Dept. of Computer Science, Leipzig University, Germany. buchmann@informatik.uni-leipzig.de
[4] https://pwning.owasp-juice.shop
[5] https://www.hackthebox.com/universities
[6] https://github.com/Fortiphyd/GRFICSv2

doi: 10.18420/delfi2023-23

Lampen. Wir haben die Aufgabe gestellt, eine intuitive Experimentierplattform mit typischen Smart Home-Geräten aufzubauen, die digital fernsteuerbar ist. Diese Plattform unterstützt Experimente im Bereich Cybersicherheit, die von der Integration und sicheren Konfiguration der Geräte über deren Absicherung bis hin zur Angriffserkennung reichen.

2 Abgrenzung und Verwandte Arbeiten

Die **Cybersicherheit** betrachtet defensive Methoden zur Absicherung von IT-Komponenten gegen Angreifer [Cr14], die auch vollautomatisch mit Viren oder Bot-Netzen Schäden verursachen können. Dabei ist wichtig, dass Cybersicherheit als ein Querschnittsthema vermittelt wird. Das heißt, es geht um Planung, Entwicklung, Einsatz und Erfolgskontrolle von Maßnahmen in einem komplexen IT-Ökosystem, und zwar über Abteilungs-, Prozess-, Netzwerk- und Rechnergrenzen hinweg [SF14].

Das **Smart Home** ist ein Konzept, um Alltagsgeräte wie Lampen, Waschmaschinen oder Garagentoröffner mit IT-Komponenten auszustatten und zu vernetzen, sodass sie beispielsweise mittels Sprachassistenten oder dem Smartphone kontrolliert werden können. Komplexere Funktionalität wie das Erkennen von Sprachbefehlen oder die Analyse von Sensordaten wird dabei an einen Cloud-Dienstleister ausgelagert. Für das Vermitteln von Themen der Cybersicherheit sind Smart Home-Szenarien [Ro10] besonders vielversprechend, weil sie eine hinreichend komplexe Infrastruktur aus Smartphones, Endgeräten, Internet- Gateway und Cloud-Dienstleistern benötigen, mit denen die Studierenden als „Digital Natives“ aber bereits vertraut sind. Mit dem Internet-Gateway gibt es einen zentralen Punkt, über den alle Geräte und Angreifer kommunizieren müssen. Die Auswertung von am Gateway aufgezeichneten Netzwerkpaketen mittels Machine Learning und künstlicher Intelligenz ist ein aktuelles Forschungsthema [Ch18]. Existierende Experimentierumgebungen sind jedoch nicht frei zugänglich [Da22], simulieren eine künstliches Smart Home [Ku22] oder generieren künstliche Testdaten aus einer realen Umgebung [Da22].

E-Learning-Ansätze für Cybersicherheit simulieren eine komplexe, vernetzte Umgebung, in der Studierende Techniken zur Angriffserkennung und/oder Absicherung üben können. Ein typisches Beispiel ist der absichtlich unsichere OWASP Juice Shop. Das ist ein Onlineshop, bei dem Betriebssystem, Datenbank-Backend, Webserver und Web-Frontend Schwachstellen enthalten. Der Juice Shop kann als digitales Lehrangebot zur Verfügung gestellt werden, um Penetrationstests zu üben. Ein anderes Beispiel ist Hack the Box (HtB). Dabei handelt es sich um eine Online-Schulungsumgebung, um spielerisch offensive und defensive Sicherheitsfähigkeiten zu erlernen. HtB bietet verschiedene virtuelle Umgebungen wie „Hacking Labs“, „Capture the Flag“ oder „Hacking Battlegrounds“ in denen Studierende in Teams oder allein praktisch lernen können. Ein drittes Beispiel ist das Graphical Realism Framework for Industrial Control Simulation (GRFICSv2). Dieser Simulator für eine Anlagensteuerung besteht aus verschiedenen industriellen IoT-Geräten und einer Firewall. GRFICSv2 legt einen Fokus auf eine grafische Darstellung der Geräte, um einen intuitiveren Zugang zu vermitteln. Überwiegend adressieren solche Ansätze klassische Client-

Server-Systeme, müssen den Studierenden sorgfältig erklärt werden bzw. setzen viel bereits vorhandenes Fachwissen voraus, und zielen auf eng fokussierte Themen wie Penetrationstests oder Firewall-Konfigurationen.

3 Konzeption des Cybersicherheits-Praktikums

Die **inhaltliche Ausrichtung** unseres Präsenz-Praktikums bestand darin, eine Experimentierplattform für ein zukünftiges digitales Praktikum der Cybersicherheit im Smart Home aufzubauen und prototypisch zu testen. Zu diesem Zweck haben wir 20 Smart Home-Geräte angeboten. Die Experimentierplattform sollte angeschlossene Geräte über das Netzwerk fernsteuerbar machen, und sie mittels Sensoren und Kameras überwachen. Mit typischen Werkzeugen der Cybersicherheit, z. B. nmap oder Metasploit, sollten Angriffe auf die Geräte gestartet werden. Am Gateway sollte aller Datenverkehr von und zu den Geräten aufgezeichnet werden. Zuletzt sollten die aufgezeichneten Netzwerkpakete mit Hilfe der Sensoren mit Labeln „Nutzeraktion“, „Angriff“ und „Unbekannt“ annotiert und mit Machine-Learning-Verfahren ausgewertet werden. Diese Ausrichtung deckt ein breites Themenspektrum der Cybersicherheit ab.

Mit diesen Themen sollten vier **Qualifikationsziele** erreicht werden: Ein (I) fundamentales Verständnis von Angriffen auf aktuelle IT-Systeme, (II) selbständiges Identifizieren von Sicherheitslücken, (III) Planung und Umsetzung von Sicherheitstechniken, sowie (IV) selbständige und zielführende Arbeit im Team.

Formal war das Praktikum für 5 LP = 150 Arbeitsstunden ausgelegt, davon 15 · 2 Stunden in Präsenz. Es richtete sich an Studierende des M. Sc. Data Science und M. Sc. Informatik. Als Teilnahmevoraussetzungen wurden vertiefte Kenntnisse im Bereich Programmierung, Netzwerkprotokolle und Rechnernetze sowie Kenntnisse in Machine Learning und Cybersicherheit genannt. Eine zeitgleiche Belegung des Moduls „Grundlagen der IT-Sicherheit“ wurde empfohlen. Die **Prüfungsleistung** sollte als Gruppenleistung erbracht werden. Jede Gruppe sollte ein 20-minütiges Videotutorial und eine schriftliche Dokumentation erstellen, wobei das Video zu 75%, die Dokumentation zu 25% in die Note einging. Den Teilnehmern wurde vorab erläutert, dass das Tutorial nach den Kriterien „sinnvoller Aufbau“, „verständlicher Inhalt“, „geeignete Mediennutzung“ und „technische Durchführung“ (Zeitvorgaben, Lautstärke, etc.) bewertet wird, die Dokumentation nach „fachlicher Tiefe“ und „übersichtlicher Darstellung“. Video und Dokumentation waren als Basis für ein zukünftiges digitales oder zumindest hybrides Praktikum der Cybersicherheit gedacht. Die **zeitliche Planung** des Praktikums hat 15 Wochen Bearbeitungszeit vorgesehen, mit einer **qualitative Lehrevaluation** nach dem ersten Drittel. Wir haben 8 Meilensteine vorgegeben, die die Selbstorganisation der Gruppen, den Aufbau der Geräte, die Inbetriebnahme der Sensorik zur Überwachung der Geräte, die Datenaufzeichnung, die Aufbereitung der Daten sowie die prototypische Angriffserkennung und die Prüfungsleistung umfassen. Das Praktikum enthielt einen hohen Forschungsanteil. Es war vorab nicht absehbar, inwiefern die Aufgabenstellung in der gegebenen Zeit vollständig lösbar war. Deshalb haben wir anstelle detaillierter inhaltlicher

und organisatorischer Vorgaben eine **intensive Betreuung** vorgesehen: Ein Professor, ein Postdoc und eine studentische Hilfskraft für den Betrieb der technischen Infrastruktur haben 12 Praktikumsteilnehmer betreut.

4 Durchführung des Cybersicherheits-Praktikums

In einer **Beschaffungsphase** haben wir für die Experimentierplattform 20 typische Smart Home-Geräte, zwei stationäre Rechner als Internet-Gateway und Angreifer, zwei Tablets mit Android-Betriebssystem für die Steuerung, zwei Webcams sowie WLAN-fähige Mikrocontroller mit NodeMCU-Betriebssystem und Sensoren bestellt. Unsere Universität hat das Praktikum mit Mitteln aus einer Initiative für digitale Lehre unterstützt.

In der **Auftaktveranstaltung** wurden Aufgabenstellung und Zielsetzung des Praktikums, Meilensteine, Geräte, sowie Prüfungsleistung und Bewertungskriterien vorgestellt. Die 12 Teilnehmer haben sich in 4 Gruppen aufgeteilt. Eine Gruppe wollte sich auf das Gateway, eine andere auf Angriffe und zwei weitere auf die Smart Home-Geräte konzentrieren.

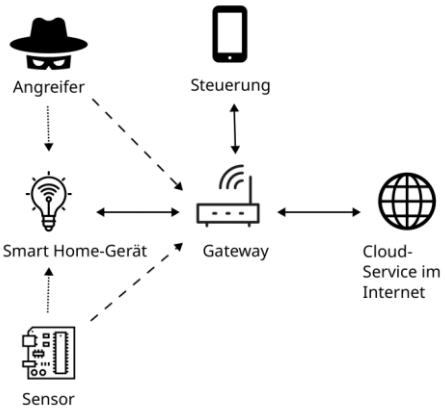

Abb. 1: Schematischer Aufbau

Abb. 2: Schematischer Aufbau

Im **weiteren Ablauf** hat die erste Gruppe das Gateway als Schnittstelle zwischen Geräten und Internet realisiert. Sie hat Aufzeichnung von Netzwerkpaketen implementiert, Schnittstellen für die Annotation der Pakete mit Labeln entwickelt und Filter für das Reduzieren der Datenmenge nach Attributen (IP-Adresse und Port, Protokoll, Zeitstempel, ...) programmiert. Die Infrastruktur ist in Abbildung 1 dargestellt. Die zweite Gruppe hat Smart Home-typische Angriffe recherchiert und automatisiert. Zu den Angriffen zählen Vorbereitungshandlungen (Geräteerkennung, Portscans), generische Angriffe (Denial-of-Service) und spezifischen Angriffe (Exploits aus dem Metasploit-Framework). Für das Label „Angriff" wurde bei jedem Angriff automatisch ein spezielles START/STOP-Datenpaket an das

Gateway versandt.

Die anderen beiden Gruppen haben festgestellt, dass Geräte schwer aufzuzeichnen sind, wenn sie nicht mittels WLAN oder Zigbee, sondern mittels Z-Wave-Protokoll kommunizieren. Dasselbe gilt für Geräte, deren Zustand nicht über Sensoren für Helligkeit, Bewegung oder Schalterposition prüfbar ist. Intelligente Lautsprecher, Türschlösser, Wasserstandsmelder o. Ä. wurden darum nicht verwendet. In die Plattform integriert wurden zwei Lampen, zwei Steckdosen, zwei Relais, ein Öffnungsmelder und ein Garagentoröffner. Die Studierenden haben dabei für den Öffnungsmelder eine kleine hölzerne Tür gebaut,

für den Garagentoröffner ein ferngesteuertes Garagentor aus Modellbau-Teilen. Für das Label „Nutzeraktion“ haben die Sensoren spezielle ACTIVITY-Datenpakete an das Gateway geschickt. Abbildung 2 zeigt einen Ausschnitt der Plattform. Die qualitativen Lehrevaluation ergab, dass die Studierenden nach der Inbetriebnahme der Geräte die Meilensteine und den Zweck des Praktikums aus den Augen verloren hatten, und Schwierigkeiten mit der Selbstorganisation hatten. Darum haben wir zusätzlich Vortragstermine anberaumt, bei denen jede Gruppe den Stand der Arbeiten, aktuelle Probleme und Wünsche an andere Gruppen in 10 Minuten vorzutragen hatte. Am Ende haben alle Gruppen den Machbarkeitsnachweis für die Angriffserkennung mit Machine Learning erbracht und die Videos und Ausarbeitungen fristgerecht abgeliefert.

5 Auswertung

Wir verfolgten zwei Ziele: Beiträge für ein zukünftiges digitales Praktikum der Cybersicherheit (vgl. Abschnitte 1, 2) sowie den Lehrerfolg dieses Praktikums (vgl. Abschnitt 3).

Lehrerfolg dieses Praktikums Wir sahen 4 Qualifikationsziele vor, die mit den Prüfungsleistungen „Videotutorial“ und „Dokumentation“ nachzuweisen waren. Die Bewertungskriterien haben wir vorab bekannt gegeben. Informell hatten wir in zahlreichen Gesprächen in den Gruppen den Lehrerfolg überwacht. Dabei beobachteten wir, dass sich das Wissen der Teilnehmer hinsichtlich der Qualifikationsziele I-III (Angriffe, Schwachstellen, Gegenmaßnahmen) kontinuierlich gesteigert hat. Die Prüfungsleistungen haben dies bestätigt. Für das Qualifikationsziel IV (Teamarbeit) mussten wir intervenieren. Die qualitative Lehrevaluation nach dem ersten Drittel des Praktikums hat gezeigt, dass die Kommunikation zwischen den Gruppen nicht ausreichte, und das gemeinsame Praktikumsziel unklar war. Wir führen dies auf die Breite des Themas „Cybersicherheit“ zurück, und haben mit Vorträgen und einer von uns vorgenommenen Strukturierung der Präsenztermine gegengesteuert.

Beiträge für ein digitales Praktikum der Cybersicherheit Aus Zeitgründen wurde nur einen Teil der angebotenen Geräte in Betrieb genommen, und nur einzelne Ansätze umgesetzt, z. B. Portscan- und Passwort-Angriffe, und „Gradient Boosting“ als Machine Learning-Verfahren zur Angriffserkennung. Die Studierenden haben selbst den Wunsch geäußert, weitere Geräte in Betrieb zu nehmen, einen umfangreicheren Datensatz zu erstellen und mit zusätzlichen Verfahren zu evaluieren. Das Praktikum hat damit nachgewiesen, dass mit der

Plattform Themen der Cybersicherheit von der Inbetriebnahme der Geräte über Angriffe bis hin zur Analyse von Netzwerkdaten vermittelt, werden können. Die erstellten Videos und Dokumentationen bieten einen niederschwelligen Zugang zu Experimenten. Für ein zukünftiges digitales Praktikum der Cybersicherheit erfordern die Videos und Dokumente noch didaktische Aufbereitung. Damit die bislang überwiegend in Präsenz genutzte Plattform sicher betrieben werden kann, ist sie über einen VPN-Zugang ans Internet anzubinden, und über die noch nicht angeschlossenen Webcams zu überwachen.

6 Zusammenfassung

In diesem Praxisbeitrag haben wir ein Praktikum beschrieben, in dem wir mit einer überschaubaren Teilnehmerzahl Konzepte für ein zukünftiges digitales Praktikum der Cybersicherheit entwickeln und austesten wollten. Dabei haben wir folgende Erkenntnisse gewonnen: Thematisch sind unsere Erfahrungen durchweg positiv. Smart Homes sind für die Studierenden ein spannendes Thema, zu dem sie durch den täglichen Umgang mit Smartphones und intelligenten Geräten leicht Zugang finden. Das Thema ist sehr gut geeignet, um Anliegen der Cybersicherheit in der Breite zu vermitteln, vom sicheren Hardware-Einsatz bis zur Angriffserkennung durch künstliche Intelligenz. Organisatorisch war eine zu flexible Gestaltung des Praktikums problematisch. Unsere Teilnehmer haben den technischen Aufbau priorisiert, und wenig Zeit für Teamkommunikation, Wissenskonsolidierung, Datensammlung und Angriffserkennung aufgewendet. Dabei haben die Teilnehmer über den technischen Fragestellungen das Praktikumsziel aus den Augen verloren. Für ein digitales Format ist zu überlegen, wie Abgaben präziser definiert und Kommunikationsstrukturen vorgegeben werden können, ohne die Experimentiermöglichkeiten eines Praktikums einzuschränken. Eine Möglichkeit wären Prüfungsleistungen, bei deren Erwerb sich die Teilnehmer gegenseitig helfen können, aber nicht müssen.

Literaturverzeichnis

[CH18] Chernyshev, M. et al.: Internet of Things (IoT): Research, Simulators, and Testbeds. IEEE Internet of Things Journal 5/3, S. 1637–1647, 2018.

[Cr14] Craigen, D. et al.: Defining Cybersecurity. Technology Innovation Management Review 4/10, 2014.

[Da22] Dadkhah, S. et al.: Towards the Development of a Realistic Multidimensional IoT Profiling Dataset. In: Conference on Privacy, Security and Trust. 2022.

[Ku22] Kumar, P. et al.: Sad-IoT: Security Analysis of DDOS Attacks in IoT Networks. Wireless Personal Communications 122/1, S. 87–108, 2022.

[Ro10] Robles, R. J.; Kim, T. - h.; Cook, D.; Das, S.: A Review on Security in Smart Home Development. Journal of Advanced Science and Technology 15/, 2010.

[SF14] Singer, P. W.; Friedman, A.: Cybersecurity and Cyberwar: What Everyone Needs to Know. Oxford University Press, USA, 2014.