Modulhandbuch
Master Cyber Security

Fakultät Elektrotechnik, Medientechnik und Informatik

Prüfungsordnung 15.12.2017

Stand: Donnerstag 06.06.2019 08:59

CY-01 SECURITY LIFECYCLE MANAGEMENT

Modul Nr.	CY-01
Modulverantwortliche/r	Prof. Dr. Peter Fröhlich
Kursnummer und Kursname	CY-01 Security Lifecycle Management
Lehrende	Laurin Dörr Stefan Felixberger Prof. Dr. Peter Fröhlich Prof. Dr. Josef Scherer Prof. Dr. Terezia Toth
Semester	1
Dauer des Moduls	1 Semester
Häufigkeit des Moduls	jährlich
Art der Lehrveranstaltungen	Pflichtfach
Niveau	Postgraduate
SWS	4
ECTS	5
Workload	Präsenzzeit: 60 Stunden Selbststudium: 90 Stunden Gesamt: 150 Stunden
Prüfungsarten	schr. P. 90 Min.
Dauer der Modulprüfung	90 Min.
Unterrichts-/Lehrsprache	Deutsch

Qualifikationsziele des Moduls

Fachkompetenz

Die Studierenden sollen das Security Lifecycle Management für Industrie und Automotive kennen lernen. Sie sollen es als ein Konzept zur nahtlosen Integration sämtlicher Informationen, die im Verlauf des Security-Lebenszyklus einer Anlage, eines Produktes oder eines Automobils anfallen, verstehen. Das Konzept beruht auf abgestimmten Methoden, Prozessen und Organisationsstrukturen und setzt grundlegende Kennntisse von technischen Systemen voraus.

Dazu erwerben die Studierenden die folgenden Kompetenzen: Kenntnisse des Cybersecurity Framework, Grundlagen vernetzter Steuerungssysteme, Grundlagen Risikoanalyse für Industrieanlagen, Recht in der Informationstechnologie, Grundlagen des Business Continuity Management.

Methodenkompetenz

Die Studenten wenden den Security-Lebenszyklus am Beispiel einer Produktionsanlage oder eines Automobils an. Sie bewerten und überprüfen darauf abgestimmte Methoden, Prozessen und Organisationsstrukturen basierend auf technischen Standards, Gesetzen und Verordnungen.

Persönliche Kompetenzen

Neben der Vermittlung von Fakten- und Begriffswissen wird zusätzlich verfahrensorientiertes Wissen durch die direkte Anwendung in der Lehrveranstaltung vermittelt. Die Studenten können den Security-Lebenszyklus auf komplexe technische Systeme anwenden.

Verwendbarkeit in diesem und in anderen Studiengängen

Für diesen Studiengang: Pflichtfach im Master-Studiengang Cyber Security

Für andere Studiengänge: keine

Zugangs- bzw. empfohlene Voraussetzungen

formal: keine

inhaltlich: keine

Inhalt

- Cyber Security Framework (Prof. Dr.-Ing. Peter Fröhlich)
- Grundlagen vernetzter Steuerungssysteme (Prof. Dr.-Ing. Terezia Toth)
- Grundlagen der Risikoanalyse von technischen Systemen am Bsp. einer Industrieanlage (M.Sc. Laurin Dörr)
  - Risikoanalyse nach BSI
  - FMEA- Failure Mode and Effects Analysis
  - Planung einer Risikoanalyse
  - Workshop Risikoanalyse
- Grundlagen des Business Continiuity Management (Prof. Dr. Josef Scherer)
  - Einführung in das BCM
  - Lösungen: Integriertes „Kombi-Managementsystem on demand“
  - P/D/C/A: „Plan“: Ziele-Management
  - Prozessorientierte Organisation / Die Evolution des Prozessmanagements
  - Umrüstung“ der Organisation auf ein Integriertes „GRC-Kombi-Managementsystem on demand“

- Tue Gutes und rede darüber: Intern oder extern: Reifegradmessung / Audit / Zertifizierung

- Recht in der Informationsgesellschaft (Stefan Felixberger; Richter)
  - Grundlagen/Compliance
  - Strafrechtliche und zivilrechtliche Aspekte
  - Datenschutz
  - IT-Sicherheit aus rechtlicher Sicht
  - Telekommunikation/Telemedien: Grundprinzipien des Online-Rechts
  - Rechtskonforme Internetnutzung: „Kontrolle vs. Fernmeldegeheimnis“
  - Vorgaben für Websites und geschäftliche Mails
  - Outsourcing und Auftragsverarbeitung

Lehr- und Lernmethoden

Seminaristischer Unterricht, Praktikum, Infomarkt

Im Unterricht werden die Inhalte unter Einbeziehung der Studenten erarbeitet, mit Hilfe eines Lückenskripts dokumentiert, durch Beispiele illustriert und durch Verständnisfragen flankiert und eingeübt. Übungsaufgaben, Kontrollfragen, Hinweise und Musterlösungen dienen dem Studenten zur Nacharbeit und zur Aneignung der Inhalte. Durch anwendungsorientierte Beispiele und Aufgabe wird der Nutzen der Begriffe und Methoden Security Lifecycle Management

Im Workshops wird das in der Vorlesung Erlernte gefestigt. In den Workshops werden folgende Themen behandelt: Risikoanalyse von Industrieanlagen, CAN und Ethernet-Netzwerke in Steuerungssystemen

Im Infomarkt bereiten die Studenten ausgewählte Themen selbstständig vor und präsentieren die Ergebnisse an Hand einer Poster Session.

Besonderes

Vorträge von Gastdozenten

Empfohlene Literaturliste

Allgemein

- ISO 2700x
- Claudia Eckert: IT-Sicherheit: Konzepte - Verfahren – Protokolle; Oldenburg Verlag; ISBN 978-3-486-72138-6

- Kersten, Heinrich, Klett, Gerhard: Business Continuity und IT-Notfallmanagement; Springer-Verlag; ISBN 978-3-658-19118-4

Industrie

- IEC 62443
- https://www.bsi.bund.de/DE/Themen/Industrie_KRITIS/industriellesicherheit_node.html
- https://ics-cert.us-cert.gov/

Automotive

- SAE J3061
- EVITA Projekt
- NHTSA - Cybersecurity Best Practices for Modern Vehicles
- Works of ISO/TC 22 (Road vehicles)
- ISO/SAE 21434 - Road Vehicles -- Cybersecurity engineering

Cyber Security Framework

- Byres, Eric , Tofino Security and Cusimano, John, exida Consulting LLC: 7 Steps to ICS and SCADA Security – White Paper; Feb. 16, 2012; www.tofinosecurity.com
- http://isa99.isa.org/ISA99%20Wiki/WP_Overview.aspx

Recht in der Informationsgesellschaft

Datenschutzrecht

- Rüpke, Giselher; Lewinski, Kai von; Eckhardt, Jens (2018): Datenschutzrecht. Grundlagen und europarechtliche Neugestaltung. München: C.H. Beck (Studium und Praxis).

Kommnentar

- Gola, Peter; Eichler, Carolyn; Franck, Lorenz; Klug, Christoph; Lepperhoff, Niels (Hg.) (2018): Datenschutz-Grundverordnung. VO (EU) 2016/679 : Kommentar. Verlag C.H. Beck. 2. Auflage. München: C.H. Beck.
- Gola, Peter; Jaspers, Andreas; Müthlein, Thomas; Schwartmann, Rolf (2017): Datenschutz-Grundverordnung im Überblick. Erläuterungen, Schaubilder und Organisationshilfen für die Datenschutzpraxis. 2. Auflage. Frechen: DATAKONTEXT.

- Müthlein, Thomas; Gola, Peter (Hg.) (2017): Datenschutz-Grundverordnung (DS-GVO). Textausgabe Englisch - Deutsch = General Data Protection Regulation (GDPR). 2. Auflage. Frechen: DATAKONTEXT.

Online

- https://www.stiftungdatenschutz.org/dsgvo-info/
- https://www.bitkom.org/Themen/Datenschutz-Sicherheit/Datenschutz/EU-DSGVO/Datenschutzkonforme-Datenverarbeitung.html
- https://www.gdd.de/gdd-arbeitshilfen/praxishilfen-ds-gvo/praxishilfen-ds-gvo
- https://vds.de/fileadmin/vds_publikationen/vds_10010_web.pdf
- http://rsw.beck.de/rsw/upload/ZD/ZD_01-2018_-_Beitrag_Veil_1.pdf
- https://fg-secmgt.gi.de/fileadmin/FG/SECMGT/2017/3_Sachs_gi_informatik_dsgvo_sec.pdf

Aktuelle Tätigkeitsberichte der Datenschutz-Aufsichtsbehörden BW/Bayern

- https://www.baden-wuerttemberg.datenschutz.de/tatigkeitsbericht/
- https://www.lda.bayern.de/media/baylda_report_08.pdf

Beschäftigtendatenschutz:

- https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2018/03/Ratgeber-ANDS-2.-Auflage.pdf

Vernetze Steuerungssysteme

- IEEE 802.x: http://standards.ieee.org/about/get/802/. Online verfügbar unter http://standards.ieee.org/about/get/802/.
- Bender, K. (1992): Profibus. Der Feldbus für die Automation. 2. Aufl. München: Hanser.
- Bormann, Alexander; Hilgenkamp, Ingo (2006): Industrielle Netze. Ethernet-Kommunikation für Automatisierungsanwendungen. Heidelberg: Hüthig (Praxis). Online verfügbar unter http://deposit.dnb.de/cgi-bin/dokserv?id=2695541&prov=M&dok_var=1&dok_ext=htm.
- Büsing, Alexander; Meyer, Holger (2002): INTERBUS-Praxisbuch. Projektierung, Programmierung, Anwendung, Diagnose. Heidelberg: Hüthig (Praxis).
- Busse, Robert (1996): Feldbussysteme im Vergleich. Mit 4 Tabellen. München, Bad Kissingen, Berlin, Düsseldorf, Heidelberg: Pflaum (Netztechnik).
- Etschberger, Konrad (2009): Controller-Area-Network. Grundlagen, Protokolle, Bausteine, Anwendungen. 4. Aufl. München: Hanser, Carl.

- Popp, Manfred (2005): Das PROFINET IO-Buch. Grundlagen und Tipps für Anwender. Heidelberg: Hüthig (Praxis).
- Reißenweber, Bernd (2011): Feldbussysteme zur industriellen Kommunikation. 3. Aufl. München: Deutscher Industrieverlag (Automatisierungstechnik 2016).
- Sauter, Martin (2015): Grundkurs mobile Kommunikationssysteme. LTE-Advanced, UMTS, HSPA, GSM, GPRS, Wireless LAN und Bluetooth. 6., überarb. und erw. Aufl. Wiesbaden: Springer Vieweg. Online verfügbar unter http://dx.doi.org/10.1007/978-3-658-08342-7.
- Schnell, Gerhard; Wiedemann, Bernhard (Hg.) (2012): Bussysteme in der Automatisierungs- und Prozesstechnik.
- Grundlagen, Systeme und Anwendungen der industriellen Kommunikation. 8., aktualisierte und erw. Aufl. Wiesbaden: Springer Vieweg (Praxis).
- Tanenbaum, Andrew S.; Wetherall, D. (2011): Computer networks. 5th ed. Boston, Momtreal: Pearson Prentice Hall.

CY-02 SECURITY ENGINEERING I

Modul Nr.	CY-02
Modulverantwortliche/r	Prof. Dr. Martin Schramm
Kursnummer und Kursname	CY-02 Security Engineering I
Lehrende	Martin Aman Sabrina Jahn Karl Leidl Jürgen Mottok Prof. Dr. Martin Schramm Dr. Thomas Störtkuhl
Semester	1
Dauer des Moduls	1 Semester
Häufigkeit des Moduls	jährlich
Art der Lehrveranstaltungen	Pflichtfach
Niveau	Postgraduate
SWS	4
ECTS	5
Workload	Präsenzzeit: 60 Stunden Selbststudium: 90 Stunden Gesamt: 150 Stunden
Prüfungsarten	schr. P. 90 Min.
Dauer der Modulprüfung	90 Min.
Unterrichts-/Lehrsprache	Deutsch

Qualifikationsziele des Moduls

Fachkompetenz

Die Studierenden sollen das Security Engineering als ganzheitlichen Ansatz begreifen. Es werden Werkzeuge, Prozesse und Methoden für Entwurf, Implementierung und Test von verlässlichen IT-Systemen in Industrie, IOT und Automotive behandelt.

Dazu erwerben die Studierenden die folgenden Kompetenzen in Security Engineering:

Mathematische Grundlagen der modernen Kryptographie, Grundlegende kryptographische Algorithmen und Protokolle, Sicherheitsmodelle, -architekturen und -strategien (ISO 27000), Betriebssysteme, Sichere Programmiertechniken, Sichere Konfiguration von Netzwerken.

Methodenkompetenz

Die Studierenden begreifen das Security Engineering als ganzheitlichen Ansatz. Die vermittelten Werkzeuge, Prozesse und Methoden können auf den Entwurf,

Implementierung und Test von verlässlichen IT-Systemen in Industrie, IOT und Automotive angewendet und bewertet werden.

Persönliche Kompetenzen

Neben der Vermittlung von Fakten- und Begriffswissen wird zusätzlich verfahrensorientiertes Wissen durch die direkte Anwendung in der Lehrveranstaltung vermittelt. Die Studenten können das Security Engineering auf komplexe technische Systeme anwenden.

Verwendbarkeit in diesem und in anderen Studiengängen

Für diesen Studiengang: Pflichtfach im Master-Studiengang Cyber Security

Für andere Studiengänge: keine

Zugangs- bzw. empfohlene Voraussetzungen

formal: keine

inhaltlich: keine

Inhalt

- Mathematische Grundlagen der modernen Kryptographie (Prof. Dr. Martin Schramm)
  - (Erweiterter) Euklidischer Algorithmus
  - Modulo Arithmetik – Restklassenmengen
  - Primzahlen
- Grundlegende kryptographische Algorithmen und Protokolle (Prof. Dr. Martin Schramm)
  - Symmetrische und asymmetrische Algorithmen
  - Integritätsalgorithmen
  - Digitale Signaturen und Public Key Infrastrukturen
- Betriebssysteme (M.Sc. Martin Aman)
  - Aufbau und Sicherheitsarchitektur
  - Security in Linux
  - Workshop

- Secure Software Engineering (Prof. Dr.-Ing. Jürgen Mottok)
  - Verlässliche Softwarearchitekturen / Codierregeln
  - Sicherheitsanforderungen für einen Anwendungsfall
  - Bedrohungsanalyse für den Anwendungsfall
  - Workshop
- Sicherheitsmodelle, -architekturen und -strategien (ISO 27000) (Dr. Thomas Störtkuhl)
  - Regulatorische Situation
  - Einführung i ISI/IEC 27001
  - Kontinuierlicher Verbesserungsprozess; Zertifizierungen
- Workshop: Sichere Konfiguration von Netzwerken (M.Sc. Karl Leidl)
  - Wichtige Tools
  - Unsicherer Netzwerkaufbau
  - Sichere Netzwerkkonfiguration

Lehr- und Lernmethoden

Seminaristischer Unterricht, Praktikum

Im Unterricht werden die Inhalte unter Einbeziehung der Studenten erarbeitet, mit Hilfe eines Lückenskripts dokumentiert, durch Beispiele illustriert und durch Verständnisfragen flankiert und eingeübt. Übungsaufgaben, Kontrollfragen, Hinweise und Musterlösungen dienen dem Studenten zur Nacharbeit und zur Aneignung der Inhalte. Durch anwendungsorientierte Beispiele und Aufgabe wird der Nutzen der Begriffe und Methoden Security Engineering vermittelt

Im Workshops wird das in der Vorlesung Erlernte gefestigt. In den Workshops werden folgende Themen behandelt: Sicherheitsanforderungen und Bedrohungsanalyse für einen konkreten Anwendungsfall, Sicherheit von Linux, Sicher Konfiguration von Netzwerken

Empfohlene Literaturliste

- Buchmann, Johannes (2016): Einführung in die Kryptographie. 6., überarbeitete Aufl. Berlin, Heidelberg: Springer (Springer-Lehrbuch).
- Wätjen, Dietmar (2018): Kryptographie. Grundlagen, Algorithmen, Protokolle. 3., aktualisierte und erweiterte Auflage. Wiesbaden: Springer Vieweg (Lehrbuch).

- ISO 2700x
- Bundesnetzargentur: IT Sicherheit im Energiesektor: https://www.bundesnetzagentur.de/DE/Sachgebiete/ElektrizitaetundGas/Unternehmen_Institutionen/Versorgungssicherheit/IT_Sicherheit/IT_Sicherheit.html
- IT-Sicherheitskatalog gemäß § 11 Absatz 1a Energiewirtschaftsgesetz: https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Energie/Unternehmen_Institutionen/Versorgungssicherheit/IT_Sicherheit/IT_Sicherheitskatalog_08-2015.pdf
- Claudia Eckert: IT-Sicherheit: Konzepte - Verfahren – Protokolle; Oldenburg Verlag; ISBN 978-3-486-72138-6

Sichere Konfiguration von Netzwerken

- Eckert, Claudia (2009): IT-Sicherheit. Konzepte - Verfahren - Protokolle. 6., überarb. und erw. Aufl. München: Oldenbourg.
- Schreiner, Rüdiger (2012): Computernetzwerke. Von den Grundlagen zur Funktion und Anwendung. 4., überarb. und erw. Aufl. München: Hanser.
- Tanenbaum, Andrew S.; Wetherall, David (2014): Computernetzwerke. 5., aktualisierte Aufl., 2. Dr. München: Pearson (Pearson Studium - IT).
- Weidman, Georgia; van Eeckhoutte, Peter (2014): Penetration testing. A hands-on introduction to hacking. San Francisco, California: No Starch Press.

Sichere Programmiertechniken

- Internet Security Glossary. Online verfügbar unter https://www.rfc-archive.org/getrfc.php?rfc=2828.
- Checklisten Handbuch IT-Grundschutz. Prüffragen zum IT-Grundschutz-Kompendium (2019). 3. aktualisierte Sonderausgabe, Stand: 1. Edition. Köln: Bundesanzeiger Verlag GmbH (Unternehmen und Wirtschaft).
- Bundesamt für Sicherheit in der Informationstechnik. Cyber-Sicherheits-Umfrage 2015- Cyber-Risiken, Meinungen und Maßnahmen, https://www.bsi.bund.de. Bonn. Online verfügbar unter https://www.bsi.bund.de.
- Bundesamt für Sicherheit in der Informationstechnik: IT-Grundschutz. G 5.42 Social Engineering. Bonn. Online verfügbar unter https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/g/g05/g05042.html.
- Bundesamt für Sicherheit in der Informationstechnik (2017): BSI: Die Lage der Informationssicherheit in Deutschland 2017. Bonn. Online verfügbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2017.pdf?__blob=publicationFile&v=4.

- Dilts, Robert B. (2010): Die Veränderung von Glaubenssystemen. NLP-Glaubensarbeit. 5. Aufl. Paderborn: Junfermann (Coaching fürs Leben).
- Eckert, Claudia: IT-Sicherheit. Konzepte - Verfahren - Protokolle: De Gruyter.
- Graves, Clare W. (2016): Levels of Existence. An Open System Theory of Values. In: Journal of Humanistic Psychology 10 (2), S. 131–155. DOI: 10.1177/002216787001000205.
- Hadnagy, Christopher (2011): Die Kunst des Human Hacking. Social engineering. 2. Auflage. Heidelberg: Mitp.
- Hadnagy, Christopher; Ekman, Paul; Dubau, Jürgen (2014): Social Engineering enttarnt. 1. Auflage. [Heidelberg]: Mitp.
- Hutchins, Eric M.; Cloppert, Michael J.; Rohan M. Amin, Rohan M.; Ph.D. (2011): Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains,. Online verfügbar unter https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf.
- Mitnick, Kevin D.; Simon, William L. (2011): Die Kunst der Täuschung. Risikofaktor Mensch. [Heidelberg]: Mitp.
- Mottok, Jürgen; Merk, Josef, Falter, Thomas (2016): Proceedings of 2016 IEEE Global Engineering Education Conference (EDUCON). Date and venue: 10-13 April 2016, Abu Dhabi, UAE. A multi dimensional view of the Graves value systems model on teaching and learning leading to a students-centered learning: Graves model revisited. [Piscataway, New Jersey]: IEEE.
- Paulus, Sachar (2011): Basiswissen Sichere Software. Aus- und Weiterbildung zum ISSECO Certified Professionell for Secure Software Engineering. 1. Auflage. Heidelberg: Dpunkt.verlag GmbH.
- Polizei Sachsen: „Achtung – geänderte Bankverbindung!“ – Betrug bei Rechnungsstellung per E-Mail. Online verfügbar unter https://www.polizei.sachsen.de/de/44606.htm.
- Rost, Johann; Glass, Robert L. (2011): The dark side of software engineering. The ethics and realities of subversion, lying, espionage, and other nefarious activities. Los Alamitos, CA, Hoboken, New Jersey: IEEE Computer Society; John Wiley & Sons, Inc.
- Schulz von Thun, Friedemann (2006): Miteinander reden. Orig.-ausg., Sonderausg. Reinbek bei Hamburg: Rowohlt Taschenbuch Verlag (Rororo Sachbuch, 62224).
- Steffens, Timo (2018): Auf der Spur der Hacker. Wie man die Täter hinter der Computer-Spionage enttarnt. Berlin, Germany, [Heidelberg]: Springer Vieweg.

- Watson, Gavin; Mason, Andrew; Ackroyd, Richard (2014): Social engineering penetration testing. Executing social engineering pen tests, assessments and defense. Waltham, MA: Syngress.

Industrielle Sicherheitsmodelle, -standards

- VDI/VDE 2182, Informationssicherheit in der industriellen Automatisierung, Allgemeines Vorgehensmodell, Blatt 1, (2011), Januar 2011. Online verfügbar unter https://www.vdi.eu/uploads/tx_vdirili/pdf/1728600.pdf.
- ISO/IEC 27005, Information technology — Security techniques — Information security risk management (2011).
- ISO/IEC 27002, Information technology — Security techniques — Code of practice for information security controls,. INTERNATIONAL STANDARD, ISO/IEC 27002 (Second edition, 2013).
- DIN ISO/IEC 27001, Information technology – Security techniques – Information security management systems – Requirements. (ISO/IEC 27001:2013 + Cor. 1:2014). English translation of DIN ISO/IEC 27001:2015-03 (2015), März 2015.
- Bundesamt für Sicherheit in der Informationstechnik (BSI-CS 005 Version 1.30 vom 2019): Industrial Control System Security, Top 10 Bedrohungen und Gegenmaßnahmen, BSI-CS 005 Version 1.30 vom 01.01.2019. Online verfügbar unter https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_005.pdf?__blob=publicationFile&v=9.
- Schäffter, M., Störtkuhl T., Public Key Infrastruktur, Aufbau und Implementierung in Banken und Sparkassen, Banken&Sparkassen, 2, 2001
- Beck, Ulrich (2016): Risikogesellschaft. Auf dem Weg in eine andere Moderne. 23. Auflage. Frankfurt am Main: Suhrkamp (Edition Suhrkamp, 1365 = N.F., 365).
- T. Störtkuhl, Manager mu?ssen Prozesse anstoßen, Computer Zeitung 37/2003
- Steiert, P., Wappler, S., Störtkuhl, T., Schaffung einer Infrastruktur für vertrauenswürdiges eBusiness, D-A-C-H, 2004
- Störtkuhl, T., Sicherheit für den Mittelstand, e-commerce Magazin 02/04
- Störtkuhl, T.IT-Sicherheit in Zeiten offener Netze, LANline Spezial V/2005
- Adlmanninger,U., Störtkuhl, T., Compliance in der Informationssicherheit, IT-Sicherheit, 6/2006
- Störtkuhl, T. et al., Ganzheitliches Management der Informationssicherheit, IT-Risiken in der Automatisierung, Wie man sie korrekt identifiziert, kontrolliert und minimiert,SecuMedia, 19. September 2008

o Störtkuhl, T., messtec drives Automation, 1-2/2018, http://www.md-automation.de/applikationen/standpunkte/it-risiken-der-automatisierung.

CY-03 SECURITY ENGINEERING II

Modul Nr.	CY-03
Modulverantwortliche/r	Prof. Dr. Martin Schramm
Kursnummer und Kursname	CY-03 Security Engineering II
Lehrende	Martin Aman Karl Leidl Ralf Reinhardt Prof. Dr. Martin Schramm Peter Semmelbauer
Semester	2
Dauer des Moduls	1 Semester
Häufigkeit des Moduls	jährlich
Art der Lehrveranstaltungen	Pflichtfach
Niveau	Postgraduate
SWS	4
ECTS	5
Workload	Präsenzzeit: 60 Stunden Selbststudium: 90 Stunden Gesamt: 150 Stunden
Prüfungsarten	PstA
Unterrichts-/Lehrsprache	Deutsch

Qualifikationsziele des Moduls

Fachkompetenz

Die Studierenden sollen das Security Engineering weiter vertiefen. Es werden Werkzeuge, Prozesse und Methoden für Entwurf, Implementierung und Test von verlässlichen IT-Systemen in Industrie, IOT und Automotive behandelt.

Die Studierenden erwerben die folgenden Kompetenzen in Security Engineering:

Weiterführende kryptographische Verfahren (Elliptische Kurven, Pairing-Based Cryptography, Identity-/Attribute-Based Cryptography, gitterbasierte Kryptographie, Post-Quantum Cryptography, Leichtgewichtige Kryptographie), Grundlegende Mechanismen für Manipulationsschutz und Zugriffsschutz, Grundlegende Vorgehensweisen für Schwachstellenanalyse, Bedrohungs- und Risikomodellierung, Definition und Entwurf von Sicherheitsstrategie und Sicherheitsmodell, Bestandteile von Defense-in-Depth Architekturen.

Methodenkompetenz

Die Studierenden begreifen das Security Engineering als ganzheitlichen Ansatz. Die vermittelten Werkzeuge, Prozesse und Methoden können auf den Entwurf, Implementierung und Test von verlässlichen IT-Systemen in Industrie, IOT und

Automotive angewendet und bewertet werden. Sie verstehen grundlegende Vorgehensweisen für die Schwachstellenanalyse, Bedrohungs- und Risikomodellierung, Definition und Entwurf von Sicherheitsstrategie und Sicherheitsmodell sowie die Bestandteile von Defense-in-Depth Architekturen.

Persönliche Kompetenzen

Neben der Vermittlung von Fakten- und Begriffswissen wird zusätzlich verfahrensorientiertes Wissen durch die direkte Anwendung in der Lehrveranstaltung vermittelt. Die Studenten können das Security Engineering auf komplexe technische Systeme wie Industrieanlagen und Automobile anwenden.

Verwendbarkeit in diesem und in anderen Studiengängen

Für diesen Studiengang: Pflichtfach im Master-Studiengang Cyber Security

Für andere Studiengänge: keine

Zugangs- bzw. empfohlene Voraussetzungen

formal: keine

inhaltlich: keine

Inhalt

- Weiterführende kryptographische Algorithmen und Protokolle (Prof. Dr. Martin Schramm)
  - Elliptische Kurven Kryptographie (ECC)
  - Post-Quantum Cryptography (PQC)
  - Leichtgewichtige Kryptographie
- Schwachstellenanalyse /Bewertung von Systemen (M.Sc. Martin Aman)
  - Kategorisierung von Schwachstellen, Schwachstellen-Datenbanken
  - Workshop
- Grundlagen des Hacking (M.Sc. Michale Heigl)
  - Analyse Schadsoftware
  - Penetration Testing Methodik
  - Exploitation

- Defense in Depth Architekturen (M.Sc. Peter Semmelbauer)
  - Defense in Depth (DiD)
  - Ebenen/ Umsetzungsmöglichkeiten
  - Architekturen/ Praxisbeispiele
- Offensive Web Application Security (Ralf Reinhardt)
  - OWASP als Organisation
  - OWASP Top 10
  - Offensive Security, Red Teaming, Ethical Hacking, Definitionen

Lehr- und Lernmethoden

Seminaristischer Unterricht, Praktikum

Im Unterricht werden die Inhalte unter Einbeziehung der Studenten erarbeitet, mit Hilfe eines Lückenskripts dokumentiert, durch Beispiele illustriert und durch Verständnisfragen flankiert und eingeübt. Übungsaufgaben, Kontrollfragen, Hinweise und Musterlösungen dienen dem Studenten zur Nacharbeit und zur Aneignung der Inhalte. Durch anwendungsorientierte Beispiele und Aufgabe wird der Nutzen der Begriffe und Methoden Security Engineering vermittelt

Im Workshops wird das in der Vorlesung Erlernte gefestigt. In den Workshops werden folgende Themen behandelt: Schwachstellenanalysen, OWASP TOP 10, Defense in Depth Architekturen

Empfohlene Literaturliste

- Werner: Elliptische Kurven in der Kryptographie, Springer Verlag
- Esslinger: The CrypTool Book: Learning and Experiencing Cryptography with CrypTool and SageMath, CrypTool Project
- Chatterjee, Sarkar: Identity-Based Encryption, Springer Verlag
- Rannenberg, Camenisch, Sabouri: Attribute-based Credentials for Trust: Identity in the Information Society, Springer Verlag
- Bernstein, Buchmann, Dahmen: Post-Quantum Cryptography, Springer Verlag
- Anderson: Security Engineering: A Guide to Building Dependable Distributed Systems, Wiley Verlag
- Bejtlich , R.: The Tao of Network Security Monitoring:Beyond Intrusion Detection . Addison-Wesley,2005.–ISBN 9780321246776

- Sanders , C.; Smith , J.: Applied NetworkSecurity Monitoring:Collection, Detection and Analysis . Elsevier Science &Technology Books,2013 (Syngress Media). – ISBN 9780124172081
- Bejtlich , R.: The Practice of Network Security Monitoring:UnderstandingIncident Detection and Response . No Starch Press,2013 (EBSCO ebook academic collection).– ISBN 9781593275099
- IT-Grundschutz-Baustein für Webanwendungen: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Download/Vorabversionen/Baustein_Webanwendungen.pdf
- OWASP Top 10 - 2013, allgemeine Informationen: https://www.owasp.org/index.php/Top_10_2013-Table_of_Contents

CY-05 SECURE OPERATIONS AND MAINTENANCE

Modul Nr.	CY-05
Modulverantwortliche/r	Prof. Dr. Andreas Grzemba
Kursnummer und Kursname	CY-05 Secure Operations and Maintenance
Lehrende	Prof. Dr. Andreas Grzemba Prof. Dr. Rolf Jung Prof. Dr. Nicolai Kuntze Karl Leidl Prof. Dr. Falk Pössnecker Prof. Dr. Martin Schramm
Semester	2
Dauer des Moduls	1 Semester
Häufigkeit des Moduls	jährlich
Art der Lehrveranstaltungen	Pflichtfach
Niveau	Postgraduate
SWS	4
ECTS	5
Workload	Präsenzzeit: 60 Stunden Selbststudium: 90 Stunden Gesamt: 150 Stunden
Prüfungsarten	schr. P. 90 Min.
Dauer der Modulprüfung	90 Min.
Unterrichts-/Lehrsprache	Deutsch

Qualifikationsziele des Moduls

Fachkompetenz

Die Studierenden sollen die wichtigen Methoden zum Betrieb und Wartung von Automationsanlagen und IOT kennen lernen. Es werden Werkzeuge, Prozesse und Methoden für angepasste Security Mechanismen für die Industrieautomation vorgestellt. Insbesondere **w**ird auf den Faktor Mensch und die Zugangskontrolle eingegangen. Zudem werden neue Entwicklungen aus der Forschung diskutiert.

Dazu erwerben die Studierenden die folgenden Kompetenzen:

Identitäts- und Zugangsmanagement; Sichere Fernwartung, Netzwerkdiagnose und Problembehandlung, Methoden und theoretische Grundlagen der Eignungsdiagnostik, Cyber Security Awareness, Ethik und der Faktor Mensch

Methodenkompetenz

Die Studierenden verstehen die wichtigen Methoden zum Betrieb und Wartung von Automationsanlagen und IOT und setzen sie zielgerichtet ein.

Persönliche Kompetenzen

Neben der Vermittlung von Fakten- und Begriffswissen wird zusätzlich verfahrensorientiertes Wissen durch die direkte Anwendung in der Lehrveranstaltung vermittelt. Insbesondere erwerben sie die Kompetenz, den Faktor Mensch im Kontext der Cyber Security zu bewerten.

Verwendbarkeit in diesem und in anderen Studiengängen

Für diesen Studiengang: Pflichtfach im Master-Studiengang Cyber Security

Für andere Studiengänge: keine

Zugangs- bzw. empfohlene Voraussetzungen

formal: keine

inhaltlich: keine

Inhalt

- Identitäts- und Zugangsmanagement –Systeme (Prof. Dr. Nicolai Kunze)
- Sichere Fernwartung (M.Sc. Martin Aman)
- Methoden und theoretische Grundlagen der Eignungsdiagnostik (Prof. Dr. Falk Pössnecker)
  - Methoden der Eignungsdiagnostik wie strukturiertes Interview, Assessment, Beobachtung, biographische Analyse,
  - Persönlichkeits- und Kompetenzmodelle,
  - Wahrnehmungsfehler
- Cyber Security Awareness, Ethik und der Faktor Mensch (Prof. Dr. Belle Wordward)
  - What is Ethics, Privicy
  - Intellectual Property, Crime
  - Evaluating and Controlling Technology
- Ausgewählte Themen in Cyber Security (Prof. Dr. Schramm/ Prof. Dr.-Ing Andreas Grzemba)
- Netzwerkdiagnose und Problembehandlung (M.Sc. Karl Leidl)

Lehr- und Lernmethoden

Seminaristischer Unterricht, Praktikum

Im Unterricht werden die Inhalte unter Einbeziehung der Studenten erarbeitet, mit Hilfe eines Lückenskripts dokumentiert, durch Beispiele illustriert und durch Verständnisfragen flankiert und eingeübt. Übungsaufgaben, Kontrollfragen, Hinweise und Musterlösungen dienen dem Studenten zur Nacharbeit und zur Aneignung der Inhalte. Durch anwendungsorientierte Beispiele und Aufgabe wird der Nutzen der Begriffe und Methoden für die Industrieautomation vermittelt

Im Workshops wird das in der Vorlesung Erlernte gefestigt. In den Workshops werden folgende Themen behandelt: Aufbau einer sichereren Fernwartung, Diagnose in Netzwerken

Empfohlene Literaturliste

- ISO 2700x
- Claudia Eckert: IT-Sicherheit: Konzepte - Verfahren – Protokolle; Oldenburg Verlag; ISBN 978-3-486-72138-6

Sichere Fernwartung

- Crist, Eric F.; Keijser, Jan Just (2015): Mastering OpenVPN: Packt Publishing.
- Du, Wenliang (2017): Computer security. A hands-on approach. [Lieu de publication non identifié]: CreateSpace.
- Knapp, Eric D.; Langill, Joel Thomas (2015): Industrial network security. Securing critical infrastructure networks for smart grid, SCADA, and other industrial control systems. Second edition. Amsterdam: Elsevier.
- Stallings, William (2017): Cryptography and network security. Principles and practice. Seventh edition, global edition. Boston: Pearson Education Limited.

Betriebssysteme:

- Stallings, William (2015): Operating systems. Internals and design principles. Eighth edition. Boston: Pearson.
- Tanenbaum, Andrew S. (2015): Modern operating systems. Fourth edition. Boston: Pearson.
- Schwachstellenanalyse:
- Forshaw, James (2018): Netzwerke hacken. Sicherheitslücken verstehen, analysieren und schützen. 1. Auflage. Heidelberg: dpunkt.

- Tanenbaum, Andrew S. (2015): Modern operating systems. Fourth edition. Boston: Pearson.

Netzwerkdiagnose und -problembehandlung

- Eckert, Claudia (2009): IT-Sicherheit. Konzepte - Verfahren - Protokolle. 6., überarb. und erw. Aufl. München: Oldenbourg.
- Schreiner, Rüdiger (2012): Computernetzwerke. Von den Grundlagen zur Funktion und Anwendung. 4., überarb. und erw. Aufl. München: Hanser.
- Tanenbaum, Andrew S.; Wetherall, David (2014): Computernetzwerke. 5., aktualisierte Aufl., 2. Dr. München: Pearson (Pearson Studium - IT).
- Weidman, Georgia; van Eeckhoutte, Peter (2014): Penetration testing. A hands-on introduction to hacking. San Francisco, California: No Starch Press.

Methoden und theoretische Grundlagen der Eignungsdiagnostik

- Daniel, Ewald; Lammert, Kathrein; Marx, Sabine U.; Weigang, Silke (2009): Einstellungstests. 45 sofort einsetzbare Aufgaben und Rollenspiele zur Personalauswahl. 2. Aufl. München: Haufe Verlag GmbH et Co. KG (Haufe-Praxisratgeber).
- Eck, Claus D.; Jöri, Hans; Vogt, Marlène (2016): Assessment-Center. Entwicklung und Anwendung - mit 57 AC-Aufgaben und Checklisten zum Downloaden und Bearbeiten im Internet ; mit 10 Tabellen. 3., überarb. und aktualisierte Aufl. Berlin [u.a.]: Springer.
- Erpenbeck, John (Hg.) (2007): Handbuch Kompetenzmessung. Erkennen, verstehen und bewerten von Kompetenzen in der betrieblichen, pädagogischen und psychologischen Praxis. 2., überarb. und erw. Aufl. Stuttgart: Schäffer-Poeschel.
- Fisseni, Hermann-Josef; Preusser, Ivonne (2007): Assessment-Center. Eine Einführung in Theorie und Praxis. Göttingen: Hogrefe.
- Hossiep, Rüdiger; Mühlhaus, Oliver (2015): Personalauswahl und -entwicklung mit Persönlichkeitstests. [mit Arbeitsmaterialien und Fallbeispielen]. 2., vollst. überarb. und erw. Aufl. Göttingen, Bern, Wien, Paris, Oxford, Prag, Toronto, Boston, Mass., Amsterdam, Kopenhagen, Stockholm, Florenz, Helsinki: Hogrefe (Praxis der Personalpsychologie, Bd. 9).
- Jetter, Wolfgang (2011): Effiziente Personalauswahl. Durch strukturierte Einstellungsgespräche die richtigen Mitarbeiter finden. 3rd ed. Stuttgart: Schäffer-Poeschel Verlag für Wirtschaft Steuern Recht.
- Kanning, Uwe Peter (2004): Standards der Personaldiagnostik. Berlin: Beuth.

- Kanning, Uwe Peter (2009): Diagnostik sozialer Kompetenzen. 2., aktualisierte Aufl. Göttingen, Bern, Wien: Hogrefe (Kompendien Psychologische Diagnostik, Bd. 4).
- Kersting, Martin (2008): Qualität in der Diagnostik und Personalauswahl - der DIN-Ansatz. Göttingen, Bern, Wien, Paris, Oxford, Prag, Toronto, Cambridge, Mass., Amsterdam, Kopenhagen: Hogrefe.
- Lienert, Gustav A.; Raatz, Ulrich (1998): Testaufbau und Testanalyse. 6. Aufl. Weinheim: Beltz Psychologie VerlagsUnion (Grundlagen Psychologie).
- Sarges, Werner (2000): Management-Diagnostik. 3., unveränd. Aufl. Göttingen, Bern, Toronto, Seattle: Hogrefe, Verl. für Psychologie. Online verfügbar unter Sarges, Werner (2000): Management-Diagnostik. 3., unveränd. Aufl. Göttingen, Bern, Toronto, Seattle: Hogrefe, Verl. für Psychologie. Online verfügbar unter http://www.sarges.
- Sarges, W. (2000): Psychologie in der Praxis. Anwendungs- und Berufsfelder einer modernen Wissenschaft. Personal: Auswahl, Beurteilung und Entwicklung. München: Deutscher Taschenb (DTV).
- Schmitt, Manfred; Gerstenberg, Friederike (2014): Psychologische Diagnostik kompakt. Mit Arbeitsmaterial zum Download. 1. Aufl., neue Ausg. Weinheim, Bergstr: Beltz, J.
- Schnell, Rainer; Hill, Paul Bernhard; Esser, Elke (2008): Methoden der empirischen Sozialforschung. 8., unveränd. Aufl. München: Oldenbourg (Lehrbuch).
- Schuler, Heinz (2014): Psychologische Personalauswahl. Eignungsdiagnostik für Personalentscheidungen und Berufsberatung. 4., vollständig überarbeitete und erweiterte Auflage. Göttingen, Niedersachs: Hogrefe Verlag (Wirtschaftspsychologie).
- Schuler, Heinz (2018): Das Einstellungsinterview. 2., überarbeitete Auflage. Göttingen: Hogrefe.
- Schuler, Heinz; Kanning, Uwe Peter (Hg.) (op. 2014): Lehrbuch der Personalpsychologie. 3., überarbeitete und erweiterte Aufl. Göttingen: Hogrefe.

CY-06 PROJECT

Modul Nr.	CY-06
Modulverantwortliche/r	Prof. Dr. Andreas Grzemba
Kursnummer und Kursname	CY-06 Project
Lehrende	Prof. Dr. Martin Schramm
Semester	3
Dauer des Moduls	1 Semester
Häufigkeit des Moduls	jährlich
Art der Lehrveranstaltungen	Pflichtfach
Niveau	Postgraduate
SWS	2
ECTS	20
Workload	Präsenzzeit: 0 Stunden Gesamt: 0 Stunden
Prüfungsarten	PrA, Präsentation 20 Min.
Dauer der Modulprüfung	20 Min.
Unterrichts-/Lehrsprache	Deutsch

Qualifikationsziele des Moduls

Fachkompetenz

Die Erstellung der Projektarbeit soll den Studierenden die Fähigkeit vermitteln, komplexe wissenschaftlich-technische Probleme aus dem Bereich Cyber Security weitgehend selbstständig oder in kleinen Gruppen unter Anleitung eines kompetenten Hochschulwissenschaftlers zu bearbeiten. Dazu müssen die Studierenden ihr Vorgehen zeitlich und inhaltlich planen und strukturieren und die Ergebnisse in entsprechender Form dokumentieren.

Methodenkompetenz

Die Studenten können für ein konkretes Projekt die geeigneten Methoden der Cyber Security auswählen und anwenden.

Persönliche Kompetenzen

Neben der Vermittlung von Fakten- und Begriffswissen wird zusätzlich verfahrensorientiertes Wissen durch die direkte Anwendung in der Lehrveranstaltung vermittelt. Insbesondere prüfen sie in Form einer Selbstreflexion den Erfolg der ausgewählten Methoden.

Verwendbarkeit in diesem und in anderen Studiengängen

Für diesen Studiengang: Pflichtfach im Master-Studiengang Cyber Security

Für andere Studiengänge: keine

Zugangs- bzw. empfohlene Voraussetzungen

formal: keine

inhaltlich: keine

Inhalt

- Das Thema des Projekts muss sich nicht direkt auf ein Modul aus dem Kurs beziehen, muss aber ein Thema aus dem Fachgebiet Cyber Security sein. Die Studenten können den betreuenden Professor ein Thema vorschlagen. In der Projektarbeit sollen immer praktische Untersuchungen mit theoretischen Anteilen verbunden werden. Mit den Betreuern bzw. Mitarbeitern der betreuenden Institute soll ein ständiger und intensiver Kontakt bestehen, um fachliche Inhalte zu vermitteln.
- Die schriftliche Projektarbeit wird zum Ende des Semesters dem Betreuer vorgelegt. Sie soll neben dem methodischen Vorgehen und den fachlichen Ergebnissen auch Bestandteile enthalten, wie sie in Berichten großer Projekte üblich sind (z.B. Einschätzungen der Marktsituation, Vergleich mit dem internationalen Stand von Wissenschaft und Technik). Die konkreten Vorgaben sind vom Thema abhängig und werden vom jeweiligen Betreuer gestellt.

CY-08 SECURITY INCIDENT MANAGEMENT

Modul Nr.	CY-08
Modulverantwortliche/r	Prof. Dr. Andreas Grzemba
Kursnummer und Kursname	CY-08 Security Incident Management
Lehrende	Prof. Dr. Andreas Grzemba
Semester	4
Dauer des Moduls	1 Semester
Häufigkeit des Moduls	jährlich
Art der Lehrveranstaltungen	Pflichtfach
Niveau	Postgraduate
SWS	4
ECTS	5
Workload	Präsenzzeit: 60 Stunden Selbststudium: 90 Stunden Gesamt: 150 Stunden
Prüfungsarten	schr. P. 90 Min.
Dauer der Modulprüfung	90 Min.
Unterrichts-/Lehrsprache	Deutsch

Qualifikationsziele des Moduls

Fachkompetenz

Die Studierenden erwerben die folgenden Fachkompetenzen:

Aktuelle Lage und Angreifermodelle, organisatorische Maßnahmen für ein SIEM, Business Continuity Management in der IT Sicherheit, Incident Response Methoden und Technologien, Forensik in embedded Netzwerken, Erkennung und Auswertung von Security Events.

Methodenkompetenz

Die Studierenden sollen wichtige Methoden, den gesamten organisatorischen und technischen Prozess der Reaktion auf erkannte oder vermutete Sicherheitsvorfälle bzw. Störungen in IT-Systemen und Industrieanlagen sowie in IOT und Automotive sowie hierzu vorbereitende Maßnahmen und Prozesse kennenlernen. Dies umfassen organisatorische, rechtliche sowie technische Aufgabenstellungen.

Persönliche Kompetenzen

Neben der Vermittlung von Fakten- und Begriffswissen wird zusätzlich verfahrensorientiertes Wissen durch die direkte Anwendung in der Lehrveranstaltung vermittelt. Insbesondere verstehen die Studierenden das Vorgehen von Angreifern.

Verwendbarkeit in diesem und in anderen Studiengängen

Für diesen Studiengang: Pflichtfach im Master-Studiengang Cyber Security

Für andere Studiengänge: keine

Zugangs- bzw. empfohlene Voraussetzungen

formal: keine

inhaltlich: keine

Inhalt

Inhalt

- Aktuelle Lage und Angreifermodelle (BSI)
  - Formale Angreifermodelle
  - Geläufige Modelle
- Organisatorische Maßnahmen für ein SIEM (Zeiss)
  - Architekturen und Prozesse
  - Tools
- Business Continuity Management in der IT Sicherheit (Prof. Dr. Helena Liebelt)
  - Prozesse
  - Rollen
  - Maßnahmen
- Social Engineering (Prof. Johannes Edler)
  - Historie und Grundmuster
  - Typische Formen
  - Abwehr
- Incident Response Methoden und Technologien (Kaspersky)
  - Incident Response Methodology
  - Erkennung und Untersuchung von Sicherheitsvorfällen (Post-Incident Activity)
  - Security Incident Response Team / Tools / Policies

- Planung und Durchführung von Response Strategien

- Forensik in embedded Netzwerken (M.Sc. Michael Heigl)
  - Datenerfassung (flüchtige, fragile, temporär zugreifbare Daten)
  - Anti-Forensik, Steganographie, File-Slack
  - Malware Forensics, Datenträgerforensik, Netzwerkforensik
  - Forensik-Tools
- Erkennung und Auswertung von Security Events (M.Sc. Amar Almaini)
  - Automatisierte Erkennung und Auswertung von bekannten Sicherheitslücken mittels Standards wie CVE, CWE
  - Event-Korrelation in SIEM-Systemen
  - Maschinelles Lernen und Informationssicherheit
  - Erkennung von Security Events in SDN

Lehr- und Lernmethoden

Seminaristischer Unterricht, Praktikum

Im Unterricht werden die Inhalte unter Einbeziehung der Studenten erarbeitet, mit Hilfe eines Lückenskripts dokumentiert, durch Beispiele illustriert und durch Verständnisfragen flankiert und eingeübt. Übungsaufgaben, Kontrollfragen, Hinweise und Musterlösungen dienen dem Studenten zur Nacharbeit und zur Aneignung der Inhalte. Durch anwendungsorientierte Beispiele und Aufgabe wird der Nutzen der Begriffe und Methoden für die Security Incident Management in der Industrieautomation vermittelt

Im Workshops wird das in der Vorlesung Erlernte gefestigt. In den Workshops werden folgende Themen behandelt: Incident Response Methoden, Forensik, BCM

Empfohlene Literaturliste

- ISO 2700x
- BSI Webseite: www.bsi.de
- Claudia Eckert: IT-Sicherheit: Konzepte - Verfahren – Protokolle; Oldenburg Verlag; ISBN 978-3-486-72138-6
- Kersten, Heinrich, Klett, Gerhard: Business Continuity und IT-Notfallmanagement; Springer-Verlag; ISBN 978-3-658-19118-4
- Christopher Hadnagy; Die Kunst des Human Hacking; mitp Professional

- Alexander Geschonneck: Computer Forensik – Computerstraftaten erkennen, ermitteln, aufklären; 5., aktualisierte und erweiterte Auflage, dpunkt.verlag
- Clint P. Garrison: Digital Forensics for Network, Internet and Cloud Computing, Syngress, 2010
- Michael Sikorski, Andrew Honig: Practical Malware Analysis – The Hands-On Guide to Dissecting Malicious Software; no starch press, 2012
- Jason T. Luttgens, Matthew Pepe, Kevin Mandia: Incident Response & Computer Forensics, 3rd Edition, McGraw-Hill Education, 2014
- Felix C. Freiling, Bastian Schwittay: A Common Process Model for Incident Response and Computer Forensics, Proceedings of the IMF, 2007
- Cameron Malin, Eoghan Casey, James Aquilina: A Practitioners Guide to Forensic Collection and Examination of Volatile Data, Syngress Elsevier, 2013
- Leighton R. Johnson III: Computer Incident Response and Forensics Team Management – Conducting a Successful Incident Response, Syngress Elsevier, 2014

CY-09 BEST PRACTISE IN INFORMATION SECURITY AUDITING

Modul Nr.	CY-09
Modulverantwortliche/r	Prof. Dr. Andreas Grzemba
Kursnummer und Kursname	CY-09 Best Practise in Information Security Auditing
Lehrende	Karl Leidl
Semester	4
Dauer des Moduls	1 Semester
Häufigkeit des Moduls	jährlich
Art der Lehrveranstaltungen	Pflichtfach
Niveau	Postgraduate
SWS	4
ECTS	5
Workload	Präsenzzeit: 0 Stunden Selbststudium: 150 Stunden Gesamt: 150 Stunden
Prüfungsarten	PstA
Unterrichts-/Lehrsprache	Deutsch

Qualifikationsziele des Moduls

Ziel ist das Erfassen potentieller Sicherheitslücken unterschiedlicher Systeme. Dazu gehört die Evaluierung von Systemen in Bezug auf IT-Sicherheit, z.B. das Erkennen von Schwachstellen in Applikationen und Betriebssystemen.

Die Studierenden sollen für mögliche Gefahren in der IT-Welt sensibilisiert werden, um das erlangte Wissen gezielt für geeignete Präventionsmaßnahmen einsetzen zu können. Dazu erwerben die Studierenden die folgenden Kompetenzen in Security Auditing:

Informationsbeschaffung, Schwachstellenanalyse, Exploitation- Ausnutzung von Schwachstellen, Post Exploitation - Schritte nach der Kompromittierung, Dokumentation (Anfertigen eines Audit-Reports)

Verwendbarkeit in diesem und in anderen Studiengängen

Für diesen Studiengang: Pflichtfach im Master-Studiengang Cyber Security

Für andere Studiengänge: keine

Zugangs- bzw. empfohlene Voraussetzungen

formal: keine

inhaltlich: keine

Inhalt

Vermitteln von fortgeschrittenen Kenntnissen über IT-Sicherheit und potentiellen Angriffsmöglichkeiten.

Dies umfasst unter anderem:

- Informationsbeschaffung, z.B.
  - Port Scanning
  - Service Enumeration
- Analyse von Schwachstellen von Komponenten und Netzwerken
  - Umgang mit Schwachstellendatenbanken (z.B. CVE)
- Ausnutzung von Schwachstellen, z.B.
  - Buffer Overflows in Programmen erkennen
  - Rücksprungadressen manipulieren
  - Shellcode einschleusen
- Post Exploitation - Schritte nach der Kompromittierung, z.B.
  - Rechteausweitung auf kompromittierten Systemen
- Dokumentation der Ergebnisse
  - Gliederung von Penetration-Test-Reports
  - Anfertigen eines Berichts der Testumgebung
- Durchführung eines vollständigen System-Audits, um die einzelnen erlernten Themen zu festigen

Lehr- und Lernmethoden

Online Modul, Praktikum

Im Online-Kurs können die Studierenden in einer Testumgebung durch praktische Übungen eigenständig Übungsaufgaben bearbeiten. Kontrollfragen, Hinweise und Musterlösungen dienen dem Studenten zur Nacharbeit und zur Aneignung der Inhalte. Durch anwendungsorientierte Beispiele und Aufgabe wird der Nutzen der Begriffe und Methoden Security Auditing vermittelt.

In den einzelnen Lernmodulen werden die individuellen Themen behandelt, die für die Durchführung eines Audits notwendig sind. In einem abschließenden vollständigen System-Audit wird das in der Vorlesung Erlernte gefestigt.

Empfohlene Literaturliste

- Jon Erickson: Hacking – The Art of Exploitation, 2nd Edition, no starch press.
- Georgia Weidman: Penetration Testing: A Hands-On Introduction to Hacking, 1. Auflage, No Starch Press.
- Claudia Eckert: IT-Sicherheit – Konzepte - Verfahren - Protokolle, 7. Auflage, Oldenbourg Verlag.

CY-10 THESIS

Modul Nr.	CY-10
Modulverantwortliche/r	Prof. Dr. Andreas Grzemba
Kursnummer und Kursname	CY-1001 Master´s Thesis CY-1002 Master´s Thesis Defense
Lehrende	Prof. Dr. Andreas Grzemba
Semester	5
Dauer des Moduls	1 Semester
Häufigkeit des Moduls	jährlich
Art der Lehrveranstaltungen	Pflichtfach
Niveau	Postgraduate
SWS	0
ECTS	20
Workload	Präsenzzeit: 0 Stunden Selbststudium: 600 Stunden Gesamt: 600 Stunden
Prüfungsarten	Präsentation 20 Min., Masterarbeit
Dauer der Modulprüfung	20 Min.
Unterrichts-/Lehrsprache	Deutsch

Qualifikationsziele des Moduls

Übergeordnetes Lernziel: Fähigkeit, ein umfangreiches Problem aus der Cyber Security selbstständig auf wissenschaftlicher Grundlage zu bearbeiten und zu lösen. Der Schwerpunkt soll auf der kreativen Entwicklung neuer Verfahren und Methoden liegen, wobei der umfassende Systemgedanke einen wesentlichen Anteil zu spielen hat.

Zugangs- bzw. empfohlene Voraussetzungen

formal: keine

inhaltlich: keine

Inhalt

- Das Thema der Masterarbeit wird von einem Professor der beteiligten Hochschulen gestellt, betreut und inhaltlich begleitet.
- Die Masterarbeit muss enthalten:
  - Darstellung des Standes der Wissenschaft und Technik des bearbeiteten Themas

- Beschreibung der Methodik und des Ablaufs des eigenen theoretischen und experimentellen Vorgehens
- Die Einbindung der eigenen Arbeiten in die Arbeit der betreuenden Institute/Fakultäten und eventueller Industriepartner
- Bericht über eigene Veröffentlichungen
- Die erreichten fachlichen Ergebnisse und deren Bewertung

CY-A04 SECURE PRODUCT DEVELOPMENT FOR AUTOMOTIVE SYSTEMS

Modul Nr.	CY-A04
Modulverantwortliche/r	Prof. Dr. Andreas Grzemba
Schwerpunkt	Automotive IT Security
Kursnummer und Kursname	CY-A0401 Automotive Security Standards and Laws CY-A0402 Security Architectures for Automotive Embedded Systems
Lehrende	Prof. Dr. Andreas Grzemba Michael Heigl Prof. Dr. Rolf Jung Prof. Dr. Martin Schramm Prof. Dr. Terezia Toth Kristina Wanieck
Semester	2
Dauer des Moduls	1 Semester
Häufigkeit des Moduls	jährlich
Art der Lehrveranstaltungen	Kern- / Wahlpflichtfach
Niveau	Postgraduate
SWS	5
ECTS	10
Workload	Präsenzzeit: 75 Stunden Selbststudium: 225 Stunden Gesamt: 300 Stunden
Prüfungsarten	schr. P. 90 Min.
Dauer der Modulprüfung	90 Min.
Unterrichts-/Lehrsprache	Deutsch

Qualifikationsziele des Moduls

Automotive Security Standards and Laws

Fachkompetenz

Die Studierenden sollen für den Schutz von Automobilen und automotiver Infrastruktur die grundlegenden Standards und gesetzlichen Bestimmungen vermittelt werden.

Dazu erwerben die Studierenden die folgenden Kompetenzen in Car IT Security Standards and Laws:

Gemeinsames Begriffsverständnis über Bedrohungen, Schwachstellen, Gegenmaßnahmen und verwandte Konzepte, Wichtigste Gefährdungen/Bedrohungen für Industrial Control Systems kennen und einordnen können; Systematik wichtiger

Publikationen (SAE J3061, NHTSA - Cybersecurity Best Practices for Modern Vehicles, Works of ISO/TC 22 (Road vehicles) ISO/SAE 21434 - Road Vehicles -- Cybersecurity engineering) verstehen und einordnen können; Maßnahmen für Car IT Security kennen und auf praktische Szenarien anwenden können, Anwendung der Standards auf die sichere Produkt- und Anlagenentwicklung.

Methodenkompetenz

Die Studenten verknüpfen die technischen Standards, Gesetze und Verordnungen mit dem Security-Lebenszyklus am Beispiel eines Automobils.

Persönlichen Kompetenzen

Neben der Vermittlung von Fakten- und Begriffswissen wird zusätzlich verfahrensorientiertes Wissen durch die direkte Anwendung in der Lehrveranstaltung vermittelt. Die Studenten können technischen Standards, Gesetze und Verordnungen bewerten und auf komplexe technische Systeme wie ein Automobil anwenden.

Security Architectures for Automotive Embedded Systems

Fachkompetenz

Die Studierenden sollen das das bisher erworbene Wissen vertiefen und auf Automotive Anwendungen transferieren. Es werden Werkzeuge, Prozesse und Methoden für angepasste Security Mechanismen für Car IT Security vorgestellt. Dieser Wissenstransferprozess wird mit Methoden von Open Innovation unterstützt.

Dazu erwerben die Studierenden die folgenden Kompetenzen:

Grundlagen Safety – Einfluss auf Security; Security Aspects von Car IT Systems, Sichere Implementierung kryptographischer Verfahren.

Methodenkompetenz

Die Studenten können Werkzeuge, Prozesse und Methoden für angepasste Security Mechanismen für Car IT bewerten.

Persönlichen Kompetenzen

Neben der Vermittlung von Fakten- und Begriffswissen wird zusätzlich verfahrensorientiertes Wissen durch die direkte Anwendung in der Lehrveranstaltung vermittelt. Die Studenten können wird mit Methoden von Open Innovation das erlernte Wissen auf neue technische Problem applizieren.

Verwendbarkeit in diesem und in anderen Studiengängen

Für diesen Studiengang: Pflichtfach im Master-Studiengang Cyber Security

Für andere Studiengänge: keine

Zugangs- bzw. empfohlene Voraussetzungen

formal: keine

inhaltlich: keine

Inhalt

Automotive Security Standards and Laws

- Industielle Sicherheits-Standards,-Regularien, - Richtlinien und –Gesetze (Dr.-Ing Andreas Grzemba)
  - Regulatorische Situation, IT-Sicherheitsgesetz
  - SAE J3061, NHTSA - Cybersecurity Best Practices for Modern Vehicles, Works of ISO/TC 22 (Road vehicles) ISO/SAE 21434 - Road Vehicles -- Cybersecurity engineering
  - Kontinuierlicher Verbesserungsprozess/ Zertifizierungen
- Sichere Produktentwicklungsprozesse (M.Sc. Michael Heigl)
  - Product Development Requirement
  - Technical Security Requirements
  - Design Priciples
- Car IT Security-Bedrohungen, Gefahren und Gegenmaßnahmen (Vector Informatik)
  - Gefährdungen und Bedrohungen
  - Maßnahmen für ICS Security
  - Definierte Schutzlevel erreichen

Security Architectures for Automotive Embedded Systems

- Grundlagen Car Safety – Einfluss auf Car IT Security (Prof. Dr. Rolf Jung)
  - Scenarios
  - Legal bases of Functional Safety
  - Risk and Functional analysis
  - Security and safety
- Automotive E/E-Architekturen (Prof. Dr. Andreas Grzemba)

- Architekturen modern Automobile
- Security Parameter moderner Car IT Systeme
- Workshop

- Cryptographic Engineering - Sichere Implementierung kryptographischer Verfahren (Prof. Dr. Martin Schramm)
  - Zufallszahlengeneratoren und Entropie
  - Montgomery Arithmetik
- Open Innovation und Kreativitätstechniken
  - Innovationsprozess
  - Bionik als Kreativitätstechnik

Lehr- und Lernmethoden

Automotive Security Standards and Laws

Seminaristischer Unterricht, Praktikum

Im Unterricht werden die Inhalte unter Einbeziehung der Studenten erarbeitet, mit Hilfe eines Lückenskripts dokumentiert, durch Beispiele illustriert und durch Verständnisfragen flankiert und eingeübt. Übungsaufgaben, Kontrollfragen, Hinweise und Musterlösungen dienen dem Studenten zur Nacharbeit und zur Aneignung der Inhalte. Durch anwendungsorientierte Beispiele und Aufgabe wird der Nutzen der Begriffe und Methoden der Car IT Security Standards and Laws vermittelt

Im Workshops werden das in der Vorlesung erlernte gefestigt. In den Workshops werden folgende Themen behandelt: Grundbedrohung, Schutzziele für Industrieanalgen und Forschungslabors, Angreifermodelle, Konzeption eines sichern Automobils

Security Architectures for Automotive Embedded Systems

Seminaristischer Unterricht, Praktikum,

Im Unterricht werden die Inhalte unter Einbeziehung der Studenten erarbeitet, mit Hilfe eines Lückenskripts dokumentiert, durch Beispiele illustriert und durch Verständnisfragen flankiert und eingeübt. Übungsaufgaben, Kontrollfragen, Hinweise und Musterlösungen dienen dem Studenten zur Nacharbeit und zur Aneignung der Inhalte. Durch anwendungsorientierte Beispiele und Aufgabe wird der Nutzen der Begriffe und Methoden für die Car IT Security vermittelt

Im Workshops werden das in der Vorlesung erlernte gefestigt. In den Workshops werden folgende Themen behandelt: Montgomery Arithmetik, Security Konzept für

eine Industriesteuerung, Open Innovation für die Entwicklung neuer Ideen und der Transfer auf Security Aspekten für E/E-Architekturen

Empfohlene Literaturliste

Automotive Security Standards and Laws

- NHTSA - Cybersecurity Best Practices for Modern Vehicles,
- ISO/SAE 21434 - Road Vehicles -- Cybersecurity engineering
- ISO 27000 Familie
- IT-Sicherheitsgesetz
- BSI Publikationen zu ICS Security: https://www.bsi.bund.de/DE/Themen/Industrie_KRITIS/industriellesicherheit_node.html
- Claudia Eckert: IT-Sicherheit: Konzepte - Verfahren – Protokolle; Oldenburg Verlag; ISBN 978-3-486-72138-6
- Cybersecurity Framework; https://www.nist.gov/cyberframework/framework

Security Architectures for Automotive Embedded Systems

- Josef Börcsök: Funktionale Sicherheit: Grundzüge sicherheitstechnischer Systeme
- Hans-Leo Ross: Funktionale Sicherheit im Automobil: ISO 26262, Systemengineering auf Basis eines Sicherheitslebenszyklus und bewährten Managementsystemen
- Lindemann, Udo: Methodische Entwicklung technischer Produkte; Springer Verlag; ISBN 978-3-642-01423-9

CY-A07 AUTOMOTIVE COMMUNICATION AND NETWORK SECURITY

Modul Nr.	CY-A07
Modulverantwortliche/r	Prof. Dr. Andreas Grzemba
Schwerpunkt	Automotive IT Security
Kursnummer und Kursname	CY-A0701 Security Aspects of Automotive Protocols CY-A0702 Automotive Network Security Laboratory Excercise
Lehrende	Prof. Dr. Andreas Grzemba
Semester	4
Dauer des Moduls	1 Semester
Häufigkeit des Moduls	jährlich
Art der Lehrveranstaltungen	Kern- / Wahlpflichtfach
Niveau	Postgraduate
SWS	5
ECTS	10
Workload	Präsenzzeit: 75 Stunden Selbststudium: 225 Stunden Gesamt: 300 Stunden
Prüfungsarten	PstA
Unterrichts-/Lehrsprache	Deutsch

Qualifikationsziele des Moduls

Security Aspects of Automotive Protocols

Fachkompetenz

Die die Studierenden erwerben folgenden Kompetenzen:

Fortgeschrittene Themen der Automatisierungstechnik, Einführung industrielle Netzwerke und historischer Hintergrund, Car IT Security, Moderne automotive Kommunikationsprotokolle, Implementierung von Sicherheitsmaßnahmen und Zugriffskontrolle in industriellen Netzwerken, Car IT Network and Design Architecture

Methodenkompetenz

Die Studierenden sollen die wichtigen Methoden für die gesamten organisatorischen und technischen Prozesse für die Absicherung der Car IT kennenlernen. Es werden angepasste Methoden für Reaktion auf erkannte oder vermutete Sicherheitsvorfälle bzw. Störungen in Car IT Systeme sowie in IOT sowie hierzu vorbereitende Maßnahmen und Prozesse vorgestellt.

Persönlichen Kompetenzen

Neben der Vermittlung von Fakten- und Begriffswissen wird zusätzlich verfahrensorientiertes Wissen durch die direkte Anwendung in der Lehrveranstaltung vermittelt. Die Studenten können komplexe technische Systeme analysieren und deren Schwachstellen erkennen.

Automotive Network Security Laboratory Excercise

Fachkompetenz

Die Studierenden lernen im Labor praktische Erfahrungen mit wichtigen InCar Protocols und ihrer Absicherung kennen.

Die Studierenden erwerben folgenden Kompetenzen: Security Monitoring von industriellen Netzwerken, Absicherung von M2M-Kommunikation, Cyber Security Evaluation InCar Netzwerke, Schaffung von Resilenz in InCar Communcation Infrastrukturen

Methodenkompetenz

Die Studierenden verstehen die Protokolle und können geeignete Absicherungsmaßnahmen auswählen.

Persönlichen Kompetenzen

Neben der Vermittlung von Fakten- und Begriffswissen wird zusätzlich verfahrensorientiertes Wissen durch die direkte Anwendung in der Lehrveranstaltung vermittelt. Die Studenten können komplexe technische Protokolle analysieren und deren Schwachstellen erkennen sowie geeignete Absicherungsmaßnahmen ergreifen.

Verwendbarkeit in diesem und in anderen Studiengängen

Für diesen Studiengang: Pflichtfach im Master-Studiengang Cyber Security

Für andere Studiengänge: keine

Zugangs- bzw. empfohlene Voraussetzungen

formal: keine

inhaltlich: keine

Inhalt

Security Aspects of Automotive Protocols

- Fortgeschrittene Themen für Autonomes Fahren (Prof. Thomas Limbrunner)
  - Konzepte von ADAS

- Cyber Physical Systems

- Einführung Automotive Netzwerke und historischer Hintergrund Car IT Security (Prof. Dr.-Ing Andreas Grzemba)
  - Grundlagen industrieller Netzwerke und der digitalen Kommunikation
  - Security-Mechanismen im OSI-Modell
- Moderne automotiver Kommunikationsprotokolle (Prof. Dr.-Ing. Andreas Grzemba)
  - Wichtige Protokolle wie Autmotive Ethernert, CAN, MQTT
  - Security-Anforderungen für die Kommunikationssysteme
- Implementierung von Sicherheitsmaßnahmen und Zugriffskontrolle in industriellen Netzwerken (Prof. Dr.-Ing. Nicolai Kunze)
  - Moderne Sicherheitsmethoden
  - Zero-Touch-Verfahren
- Automotive Network and Design Architecture (Dil.-Inf. Amar Almaini)
  - Grundlagen und Anwendung von SDN
  - SDN und Scurity

Automotive Network Security Laboratory Excercise

- Cyber Security Evaluation Car IT Netzwerke (BMW)
  - Security Evaluierung wichtiger Process Control Protokolle
- Absicherung von M2M-Kommunikation (Vector Informatik)
  - Besonderheiten der M2M-Kommunikation
  - Workshop
- Security Monitoring von InCar Netzwerken (Kasperky)
  - Network Intrusion Detection (NIDS) für InCar Control Protokolle
  - Workshop
- Schaffung von Resilienz in Car IT Infrastrukturen (M.Sc. Michael Heigl)
  - Resilienz-Maßnahmen
  - Workshop

Lehr- und Lernmethoden

Security Aspects of Automotive Protocols

Seminaristischer Unterricht, Praktikum

Im Unterricht werden die Inhalte unter Einbeziehung der Studenten erarbeitet, mit Hilfe eines Lückenskripts dokumentiert, durch Beispiele illustriert und durch Verständnisfragen flankiert und eingeübt. Übungsaufgaben, Kontrollfragen, Hinweise und Musterlösungen dienen dem Studenten zur Nacharbeit und zur Aneignung der Inhalte. Durch anwendungsorientierte Beispiele und Aufgabe wird der Nutzen der Begriffe und Methoden für die Security Requirements in der Car IT Security vermittelt

Im Workshops wird das in der Vorlesung Erlernte gefestigt. In den Workshops werden folgende Themen behandelt: automobile Kommunikationssysteme, Zugangsverfahren, CPS

Automotive Network Security Laboratory Excercise

Seminaristischer Unterricht, Praktikum

Im Unterricht werden die Inhalte unter Einbeziehung der Studenten erarbeitet, mit Hilfe eines Lückenskripts dokumentiert, durch Beispiele illustriert und durch Verständnisfragen flankiert und eingeübt. Übungsaufgaben, Kontrollfragen, Hinweise und Musterlösungen dienen dem Studenten zur Nacharbeit und zur Aneignung der Inhalte. Durch anwendungsorientierte Beispiele und Aufgabe wird der Nutzen der Begriffe und Methoden für InCar Protocols vermittelt.

In Workshops wird das in der Vorlesung Erlernte gefestigt. In den Workshops werden folgende Themen behandelt: M2M-Kommunikation, NIDS, Resilienz-Maßnahmen.

Empfohlene Literaturliste

Security Aspects of Automotive Protocols

- ISO/SAE 21434 - Road Vehicles -- Cybersecurity engineering
- BSI Webseite: www.bsi.de
- Siegmund, Gerd: SDN - Software-defined Networking; VDE-Verlag; ISBN 978-3-8007-4511-1
- Gaston C. Hillar: MQTT Essentials - A Lightweight IoT Protocol; Packt Publishing; ISBN: 978-1-78728-781-5
- Pascal Ackerman; Industrial Cybersecurity; Packt Publishing; ISBN: 978-1-78728-781-5
- Kirsten Matheus, Thomas Königseder: Automotive Ethernet; Cambridge Press, 2017

- Wolfhard Lawrenz, Nils Obermöller, CAN: Controller Area Network: Grundlagen, Design, Anwendungen, Testtechnik; VDE-Verlag

Automotive Network 5ecurity Laboratory Excercise

- ISO/SAE 21434 - Road Vehicles -- Cybersecurity engineering
- BSI Webseite: www.bsi.de
- Gaston C. Hillar: MQTT Essentials - A Lightweight IoT Protocol; Packt Publishing; ISBN: 978-1-78728-781-5
- Pascal Ackerman; Industrial Cybersecurity; Packt Publishing; ISBN: 978-1-78728-781-5
- Kirsten Matheus, Thomas Königseder: Automotive Ethernet; Cambridge Press, 2017
- Wolfhard Lawrenz, Nils Obermöller, CAN: Controller Area Network: Grundlagen, Design, Anwendungen, Testtechnik; VDE-Verlag

CY-I04 SECURE PRODUCT DEVELOPMENT FOR INDUSTRIAL APPLICATIONS

Modul Nr.	CY-I04
Modulverantwortliche/r	Prof. Dr. Andreas Grzemba
Schwerpunkt	Industrial IT Security
Kursnummer und Kursname	CY-I0401 Industrial Security Standards and Laws CY-I0402 Design of robust Industrial Control Systems
Lehrende	Laurin Dörr Prof. Dr. Rolf Jung Dr. Thomas Nowey Prof. Dr. Martin Schramm Dr. Thomas Störtkuhl Prof. Dr. Terezia Toth Kristina Wanieck
Semester	2
Dauer des Moduls	1 Semester
Häufigkeit des Moduls	jährlich
Art der Lehrveranstaltungen	Kern- / Wahlpflichtfach, Pflichtfach
Niveau	Postgraduate
SWS	5
ECTS	10
Workload	Präsenzzeit: 75 Stunden Selbststudium: 225 Stunden Gesamt: 300 Stunden
Prüfungsarten	schr. P. 90 Min.
Dauer der Modulprüfung	90 Min.
Unterrichts-/Lehrsprache	Deutsch

Qualifikationsziele des Moduls

Industrial Security Standards and Laws

Fachkompetenz

Die Studierenden sollen für den Schutz von Industrieanlagen die grundlegenden Standards und gesetzlichen Bestimmungen vermittelt werden.

Dazu erwerben die Studierenden die folgenden Kompetenzen in Industrial Security Standards and Laws:

Gemeinsames Begriffsverständnis über Bedrohungen, Schwachstellen, Gegenmaßnahmen und verwandte Konzepte, wichtigste Gefährdungen/Bedrohungen für Industrial Control Systems kennen und einordnen können; Systematik wichtiger

Publikationen (IEC 62443-3-Familie und BSI Publikationen zu ICS Security) verstehen und einordnen können; Maßnahmen für ICS Security kennen und auf praktische Szenarien anwenden können, Anwendung der Standards auf die sichere Produkt- und Anlagenentwicklung.

Methodenkompetenz

Die Studenten verknüpfen die technischen Standards, Gesetze und Verordnungen mit dem Security-Lebenszyklus am Beispiel einer Produktionsanlage oder eines Automobils.

Persönliche Kompetenzen

Neben der Vermittlung von Fakten- und Begriffswissen wird zusätzlich verfahrensorientiertes Wissen durch die direkte Anwendung in der Lehrveranstaltung vermittelt. Die Studenten können technischen Standards, Gesetze und Verordnungen bewerten und auf komplexe technische Systeme anwenden.

Design of robust Industrial Control Systems

Fachkompetenz

Die Studierenden sollen das das bisher erworbene Wissen vertiefen und auf industrielle Anwendungen transferieren. Es werden Werkzeuge, Prozesse und Methoden für angepasste Security Mechanismen für die Industrieautomation vorgestellt. Dieser Wissenstransferprozess wird mit Methoden von Open Innovation unterstützt.

Dazu erwerben die Studierenden die folgenden Kompetenzen:

Grundlagen Safety – Einfluss auf Security; Security Aspects von Industrial Control Systems, Sichere Implementierung kryptographischer Verfahren.

Methodenkompetenz

Die Studenten können Werkzeuge, Prozesse und Methoden für angepasste Security Mechanismen für die Industrieautomation bewerten.

Persönliche Kompetenzen

Neben der Vermittlung von Fakten- und Begriffswissen wird zusätzlich verfahrensorientiertes Wissen durch die direkte Anwendung in der Lehrveranstaltung vermittelt. Die Studenten können wird mit Methoden von Open Innovation das erlernte Wissen auf neue technische Problem applizieren.

Verwendbarkeit in diesem und in anderen Studiengängen

Für diesen Studiengang: Pflichtfach im Master-Studiengang Cyber Security

Für andere Studiengänge: keine

Zugangs- bzw. empfohlene Voraussetzungen

formal: keine

inhaltlich: keine

Inhalt

Industrial Security Standards and Laws

- Industielle Sicherheits-Standards,-Regularien, - Richtlinien und –Gesetze (Dr. Thomas Störtkuhl)
  - Regulatorische Situation, IT-Sicherheitsgesetz
  - IEC62443
  - Kontinuierlicher Verbesserungsprozess/ Zertifizierungen
- Sichere Produktentwicklungsprozesse (M.Sc. Lautin Dörr)
  - Product Development Requirement
  - Technical Security Requirements
  - Design Priciples
- ICS Security-Bedrohungen, Gefahren und Gegenmaßnahmen (Dr. Thomas Nowey)
  - Gefährdungen und Bedrohungen
  - Maßnahmen für ICS Security
  - Definierte Schutzlevel erreichen

Design of robust Industrial Contral Systems

- Grundlagen Safety – Einfluss auf Security (Prof. Dr. Rolf Jung)
  - Industrial scenarios
  - Legal bases of Functional Safety
  - Risk and Functional analysis
  - Security and safety
- Industrial Control Systems (Prof. Dr. Terezia Toth)
  - Architekturen modern Steuerungssysteme

- Security Parameter moderner Steuerungssysteme
- Workshop Simantic S7

- Cryptographic Engineering - Sichere Implementierung kryptographischer Verfahren (Prof. Dr. Martin Schramm)
  - Zufallszahlengeneratoren und Entropie
  - Montgomery Arithmetik
- Open Innovation und Kreativitätstechniken
  - Innovationsprozess
  - Bionik als Kreativitätstechnik

Lehr- und Lernmethoden

Seminaristischer Unterricht, Praktikum

Im Unterricht werden die Inhalte unter Einbeziehung der Studenten erarbeitet, mit Hilfe eines Lückenskripts dokumentiert, durch Beispiele illustriert und durch Verständnisfragen flankiert und eingeübt. Übungsaufgaben, Kontrollfragen, Hinweise und Musterlösungen dienen dem Studenten zur Nacharbeit und zur Aneignung der Inhalte. Durch anwendungsorientierte Beispiele und Aufgabe wird der Nutzen der Begriffe und Methoden der Industrial Security Standards and Laws vermittelt

Im Workshops wird das in der Vorlesung Erlernte gefestigt. In den Workshops werden folgende Themen behandelt:

Industrial Security Standards and Laws: Grundbedrohung, Schutzziele für Industrieanalgen und Forschungslabors, Angreifermodelle, Konzeption eines sichern Produkts

Design of robust Industrial Contral Systems: Montgomery Arithmetik, Security Konzept für eine Industriesteuerung, Open Innovation für die Entwicklung neuer Ideen und der Transfer auf Security Aspekten von Industrieanlagen

Empfohlene Literaturliste

Industrial Security Standards and Laws

- IEC 62443 Teil1-4
- ISO 27000 Familie
- IT-Sicherheitsgesetz

- BSI Publikationen zu ICS Security: https://www.bsi.bund.de/DE/Themen/Industrie_KRITIS/industriellesicherheit_node.html
- Claudia Eckert: IT-Sicherheit: Konzepte - Verfahren – Protokolle; Oldenburg Verlag; ISBN 978-3-486-72138-6
- Cybersecurity Framework; https://www.nist.gov/cyberframework/framework

Design of robust Industrial Contral Systems

- Josef Börcsök: Funktionale Sicherheit: Grundzüge sicherheitstechnischer Systeme
- Hans-Leo Ross: Funktionale Sicherheit im Automobil: ISO 26262, Systemengineering auf Basis eines Sicherheitslebenszyklus und bewährten Managementsystemen
- Lindemann, Udo: Methodische Entwicklung technischer Produkte; Springer Verlag; ISBN 978-3-642-01423-9

CY-I07 INDUSTRIAL COMMUNICATION AND NETWORK SECURITY

Modul Nr.	CY-I07
Modulverantwortliche/r	Prof. Dr. Andreas Grzemba
Schwerpunkt	Industrial IT Security
Kursnummer und Kursname	CY-I0701 Security Requirements for Indurstrial Plants CY-I0702 ICS Security Laboratory Excercises
Lehrende	Prof. Dr. Andreas Grzemba Prof. Dr. Martin Schramm
Semester	4
Dauer des Moduls	1 Semester
Häufigkeit des Moduls	jährlich
Art der Lehrveranstaltungen	Kern- / Wahlpflichtfach
Niveau	Postgraduate
SWS	5
ECTS	10
Workload	Präsenzzeit: 75 Stunden Selbststudium: 225 Stunden Gesamt: 300 Stunden
Prüfungsarten	PstA
Unterrichts-/Lehrsprache	Deutsch

Qualifikationsziele des Moduls

Security Requirements for Industrial Plants

Fachkompetenz

Dazu erwerben die Studierenden die folgenden Kompetenzen:

Fortgeschrittene Themen der Automatisierungstechnik, Einführung Industrielle Netzwerke und historischer Hintergrund ICS Security, Moderne industrielle Kommunikationsprotokolle, Implementierung von Sicherheitsmaßnahmen und Zugriffskontrolle in industriellen Netzwerken, Industrial Network and Design Architecture.

Methodenkompetenz

Die Studierenden sollen die wichtigen Methoden für die gesamten organisatorischen und technischen Prozesse für die Absicherung von Industrieanlagen kennenlernen. Es werden angepasste Methoden für eine Reaktion auf erkannte oder vermutete Sicherheitsvorfälle bzw. Störungen in Industrieanlagen sowie in IOT sowie hierzu vorbereitende Maßnahmen und Prozesse vorgestellt.

Persönliche Kompetenzen

Neben der Vermittlung von Fakten- und Begriffswissen wird zusätzlich verfahrensorientiertes Wissen durch die direkte Anwendung in der Lehrveranstaltung vermittelt. Die Studenten können komplexe technische Systeme analysieren und deren Schwachstellen erkennen.

ICS Security Laboratory Excercises

Fachkompetenz

Die Studierenden sollen im Labor praktische Erfahrungen mit wichtigen Prozess Control Protocols und ihrer Absicherung kennenlernen

Dazu erwerben die Studierenden die folgenden Kompetenzen:

Security Monitoring von industriellen Netzwerken, Absicherung von M2M-Kommunikation, Cyber Security Evaluation industrieller Netzwerke, Schaffung von Resilienz in kritischen Infrastrukturen

Methodenkompetenz

Die Studierenden verstehen die Protokolle und können geeignete Absicherungsmaßnahmen auswählen.

Persönliche Kompetenzen

Neben der Vermittlung von Fakten- und Begriffswissen wird zusätzlich verfahrensorientiertes Wissen durch die direkte Anwendung in der Lehrveranstaltung vermittelt. Die Studenten können komplexe technische Protokolle analysieren und deren Schwachstellen erkennen sowie geeignete Absicherungsmaßnahmen ergreifen.

Verwendbarkeit in diesem und in anderen Studiengängen

Für diesen Studiengang: Pflichtfach im Master-Studiengang Cyber Security

Für andere Studiengänge: keine

Zugangs- bzw. empfohlene Voraussetzungen

formal: keine

inhaltlich: keine

Inhalt

Security Requirements for Industrial Plants

- Fortgeschrittene Themen der Automatisierungstechnik (Prof. Dr.-Ing Ludwig Gansauge)
  - Konzepte von Industrie 4.0
  - Cyber Physical Systems
- Einführung Industrielle Netzwerke und historischer Hintergrund ICS Security (Prof. Dr.-Ing Andreas Grzemba)
  - Grundlagen industrieller Netzwerke und der digitalen Kommunikation
  - Security-Mechanismen im OSI-Modell
- Moderne industrielle Kommunikationsprotokolle (Prof. Dr.-Ing. Andreas Grzemba)
  - Wichtige Protokolle wie Profibus, CAN, MQTT und OPC-UA
  - Security-Anforderungen der Feldbusssysteme
- Implementierung von Sicherheitsmaßnahmen und Zugriffskontrolle in industriellen Netzwerken (Prof. Dr.-Ing. Nicolai Kunze)
  - Moderne Sicherheitsmethoden
  - Zero-Touch-Verfahren
- Industrial Network and Design Architecture (Dil.-Inf. Amar Almaini)
  - Grundlagen und Anwendung von SDN
  - SDN und Security

ICS Security Laboratory Excercises

- Cyber Security Evaluation industrieller Netzwerke (Genua)
  - Security Evaluierung wichtiger Process Control Protokolle
- Absicherung von M2M-Kommunikation (Kasperky)
  - Besonderheiten der M2M-Kommunikation
  - Workshop: Bluetooth
- Security Monitoring von industriellen Netzwerken (Kasperky)
  - Network Intrusion Detection (NIDS) für Process Control Protokolle
  - Workshop
- Schaffung von Resilienz in kritischen Infrastrukturen (M.Sc. Michael Heigl)

- Resilienz-Maßnahmen
- Workshop

Lehr- und Lernmethoden

Security Requirements for Industrial Plants

Seminaristischer Unterricht, Praktikum

Im Unterricht werden die Inhalte unter Einbeziehung der Studenten erarbeitet, mit Hilfe eines Lückenskripts dokumentiert, durch Beispiele illustriert und durch Verständnisfragen flankiert und eingeübt. Übungsaufgaben, Kontrollfragen, Hinweise und Musterlösungen dienen dem Studenten zur Nacharbeit und zur Aneignung der Inhalte. Durch anwendungsorientierte Beispiele und Aufgabe wird der Nutzen der Begriffe und Methoden für die Security Requirements in der Industrieautomation vermittelt

Im Workshops wird das in der Vorlesung Erlernte gefestigt. In den Workshops werden folgende Themen behandelt: Feldbussysteme, Zugangsverfahren, CPS

ICS Security Laboratory Excercises

Seminaristischer Unterricht, Praktikum

Im Unterricht werden die Inhalte unter Einbeziehung der Studenten erarbeitet, mit Hilfe eines Lückenskripts dokumentiert, durch Beispiele illustriert und durch Verständnisfragen flankiert und eingeübt. Übungsaufgaben, Kontrollfragen, Hinweise und Musterlösungen dienen dem Studenten zur Nacharbeit und zur Aneignung der Inhalte. Durch anwendungsorientierte Beispiele und Aufgabe wird der Nutzen der Begriffe und Methoden für Prozess Control Protocols in der Industrieautomation vermittelt

Im Workshops wird das in der Vorlesung Erlernte gefestigt. In den Workshops werden folgende Themen behandelt: M2M-Kommunikation, NIDS, Resilienz-Maßnahmen

Empfohlene Literaturliste

Security Requirements for Industrial Plants / ICS Security Laboratory Excercises

- IEC62443-Familie
- BSI Webseite: www.bsi.de
- Wolfgang Mahnke: OPC Unified Architecture; Springer-Verlag
- Gaston C. Hillar: MQTT Essentials - A Lightweight IoT Protocol; Packt Publishing; ISBN: 978-1-78728-781-5

o Pascal Ackerman; Industrial Cybersecurity; Packt Publishing; ISBN: 978-1-78728-781-5