



TOP 7.1 Fachbereiche

Jahresbericht 2021

GI-Fachbereich Sicherheit - Schutz und Zuverlässigkeit

Intention des Fachbereichs

Der GI-Fachbereich "Sicherheit - Schutz und Zuverlässigkeit" wurde im Februar 2002 gegründet und vernetzt zwei "Communities" miteinander: Während die „Safety-Community“ vor allem den Schutz der Umwelt vor IT-Systemen (beispielsweise Sicherheit des Menschen vor schwerwiegenden Systemfehlern in Flugzeugen, Kernreaktoren und Kraftwerken) sowie Fehlertoleranzmaßnahmen (z.B. Systemausfälle als Folge von Ermüdungserscheinungen, Softwarefehlern und Naturereignissen) im Blick hat, beschäftigt sich die „Security-Community“ hauptsächlich mit dem Schutz der IT-Systeme und ihrer Umgebung vor Bedrohungen von außen, insbesondere vor Gefahren, die von bösartigen Angriffen (durch Menschen) ausgehen.

Sicherheit ist ein Querschnittsthema. Für den Fachbereich gilt daher eine hohe Flexibilität hinsichtlich der Möglichkeiten zur Quervernetzung verschiedener Gruppen und Themen innerhalb und außerhalb der GI. Diese Quervernetzung wird sowohl in gemeinsamen Veranstaltungen als auch in der starken Berücksichtigung anderer Themen aus der Informatik deutlich. Sicherheit ist kein Selbstzweck, sondern wichtig zur Erfüllung gesellschaftlicher und wirtschaftlicher Bedürfnisse.

Der Fachbereich bietet ein Forum, in dem alle auf dem Gebiet der Sicherheit informationstechnischer Systeme arbeitenden Menschen ihr Fachthema, organisiert in Fachgruppen, wiederfinden. Neben der rein wissenschaftlichen Arbeit ermöglicht der Fachbereich einen fachlichen Austausch zwischen Wissenschaft und Praxis.

Zu den Zielen des Fachbereichs zählen:

- Unterstützung der wissenschaftlichen Arbeit auf den Gebieten der IT-Sicherheit
- Vernetzung von Wissenschaft, Praxis und Gesellschaft
- Vernetzung mit der Forschung und den Hochschulen zu Schutz und Zuverlässigkeit informationstechnischer Systeme

Organisation des Fachbereichs (Personalia)

Sprecher des Fachbereichs ist Bernhard C. Witt (it.sec GmbH), **stellvertretende Sprecherin** ist Delphine Reinhardt (Universität Göttingen).

Folgende Personen wurden vom Fachbereich als **Fachexperten** benannt:

- Hannes Federrath – Anbindung an GI-Gremien
- Ulrich Flegel – Vertreter des Fachbereichs im LNI-Herausgebergremium
- Andreas Heinemann – Organisation des Promotionspreises IT-Sicherheit
- Matthias Jänichen – Pflege der Mailinglisten und der Kommunikationsinfrastruktur
- Hanno Langweg – Tagungsorganisation der Sicherheit 2018 in Konstanz
- Michael Meier – Vertreter in der Allianz für Cybersicherheit und Tagungsunterstützung
- Isabel Münch – Kontakt zum BSI und Tagungsunterstützung
- Kai Rannenbergh – ständiger Vertreter des FB im PAK Datenschutz und Sicherheit und Sprecher des Editorial Boards
- Delphine Reinhardt – Tagungsorganisation der Sicherheit 2020 in Göttingen
- Edgar Weippl – Tagungsorganisation der Sicherheit 2014 in Wien
- Christian Wressnegger – Tagungsorganisation der Sicherheit 2022 in Karlsruhe



Im Berichtszeitraum wurde aus den Reihen der aktuellen FB-Leitungsgremiums-Mitglieder **Matthias Marx** neuer **Junior-Fellow der GI** ernannt. Der Fachbereich Sicherheit gratuliert hierzu ganz herzlich!

Die Fachgruppen und ihre Sprecher zum Ende 2021:

- **Ada** – FG Zuverlässige Software-Systeme: Sprecher ist **Hubert Keller**
- **BIOSIG** – FG Biometrik und elektronische Signaturen: Sprecher ist **Heiko Roßnagel**
- **ECOM** – FG E-Commerce, E-Government und Sicherheit: Sprecher ist **Jörg Helbach**
- **ENCRESS** – FG Zuverlässigkeit und Sicherheit software-basierter Systeme: Sprecherin ist **Francesca Saglietti**
- **EZQN** – FG Evaluation, Zertifizierung, Qualitätssicherung, Normung: Sprecher ist **Peer Reymann**
- **FERS** – FG Fehlertolerierende Rechensysteme: Sprecher ist **Bernhard Fechner**
- **FoMSESS** – FG Formale Methoden und Software Engineering für sichere Systeme: Sprecher ist **Zoltan Mann**
- **KRYPTO** – FG Angewandte Kryptologie: Sprecher ist **Daniel Loebenberger**
- **NETSEC** – FG Sicherheit in Mobil- und Festnetzen: Sprecher ist **Matthias Marx**
- **PET** – FG Datenschutzfördernde Technik (Privacy Enhancing Technologies): Sprecher ist **Sebastian Pape**
- **SECMGT** – FG Management von Informationssicherheit: Sprecher ist **Frank Damm**
- **SIDAR** – FG Erkennung und Beherrschung von Vorfällen der Informationssicherheit: Sprecher ist **Michael Meier**
- **UseSafeSec** – FG Usable Safety & Security: Sprecher ist **Tilo Mentler**

Mitgliederzahlen des Fachbereichs

| Organisation | 2020 | 2021 |
|----------------------|------------|------------|
| FG Ada | 26 | 30 |
| FG BIOSIG | 175 | 180 |
| FG ECOM | 256 | 247 |
| FG ENCRESS | 120 | 123 |
| FG EZQN | 178 | 186 |
| FG FERS | 27 | 34 |
| FG FoMSESS | 217 | 221 |
| FG KRYPTO | 268 | 263 |
| FG NETSEC | 262 | 254 |
| FG PET | 266 | 267 |
| FG SECMGT | 386 | 389 |
| FG SIDAR | 296 | 305 |
| FG UseSafeSec | 53 | 67 |
| FB SICHERHEIT | 813 | 817 |

Anmerkung: Die Fachgruppen Ada, ENCRESS, FERS und UseSafeSec sind mehreren Fachbereichen zugeordnet.

Aktivitäten des Fachbereichs

Alle zwei Jahre führt der Fachbereich seine Fachbereichstagung durch und vergibt in enger Zusammenarbeit mit dem CAST e.V. einen Preis für die beste Promotion auf dem Gebiet der IT-Sicherheit, der mit 3.000 Euro dotiert ist. Ferner betreibt der Fachbereich eine offene Mailingliste, auf



der aktuelle Informationen zu Tagungen, Workshops und Aktivitäten im Sicherheitsbereich verbreitet werden und bezieht bei Bedarf Stellung zu aktuellen Themen der Sicherheit.

Im Berichtszeitraum hat sich das **Leitungsgremium des Fachbereichs** gleich dreimal **per Webkonferenz** getroffen, dankenswerterweise jeweils gehostet von Peer Reymann (ITQS): Am 22.01.2021 (nachgeholt für das Wintersemester 2020/2021), 30.04.2021 und 05.11.2021.

Schwerpunkte der Arbeit im zurückliegenden Jahr waren

- Aufnahme der Fachgruppe Useable Safety & Security aus dem Fachbereich Mensch-Computer-Interaktion (damit seit 2021 Doppelmitgliedschaft in zwei Fachbereichen).
- Aktive Begleitung der Statutenüberarbeitung der GI.
- Bedarfsbezogene Einrichtung von Adhoc-Arbeitskreisen des Fachbereichs: Im Berichtszeitraum erfolgt zur Positionierung zur stärkeren Unabhängigkeit des BSI (on-going) sowie zum Zuschnitt der DFG-Fachkollegien der Informatik (Arbeit abgeschlossen).
- Einbringen der Stellungnahme zum IT-SiG 2.0 in den parlamentarischen Gesetzgebungsprozess (abgedruckt in BT-Drucksache 19/26106 – Ausschussdrucksache 19(4)714).
- Aktive Begleitung der Fortentwicklung des Informatik Spektrums bzw. einer neuen Mitgliedszeitschrift der GI.
- Nominierung zweier Vertreter des FB Sicherheit für den Herausgeberkreis des Informatik Spektrums: Michael Meier und Kai Rannenber.
- Begleitung der aktuellen Entwicklung des im Vorjahr erfolgten Mailinglistenumzugs.
- Aufnahme von Expert*innenprofilen auf den Webseiten des Fachbereichs.
- Feedback zum "Curriculum digitale Katastrophenhelferin" (ausschließlich aus Sicht von Mitgliedern der FG SECMGT).
- Vorbereitung der nächsten Fachbereichstagung GI SICHERHEIT 2022 vom 5. – 8. April 2022 in Karlsruhe.
- Vorbereitung des CAST/GI Promotionspreis IT-Sicherheit 2022.
- Identifikation einer potenziell vorhandenen Rechtslücke im neuen TTDSG.

Die Einstufung zum **Aktivitätsindex** (Grün = aktiv, gelb = mittel, rot = inaktiv) erfolgt im GI-Fachbereich Sicherheit anhand folgender Kriterien:

- Zeitraum seit letzter LG-Wahl: ≤ 4 Jahre: grün, > 4 und ≤ 6 Jahre: gelb, > 6 Jahre: rot
- Aktualität der Webseite: Einträge aus dem aktuellen Jahr vorhanden: grün, letzte Änderung stammt aus dem Vorjahr: gelb, letzte Änderung erfolgte vor dem Vorjahr: rot
- letztvorliegender Bericht über durchgeführte Aktivitäten: FG-Bericht im aktuellen Jahresbericht vorhanden: grün, letztzugesandter FG-Jahresbericht aus dem Vorjahr: gelb, letztzugesandter FG-Jahresbericht vor dem Vorjahr: rot
- Anwesenheit auf FB-LG-Sitzungen: FG wurde auf den letzten 3 FB-LG-Sitzungen laut Protokoll wenigstens einmal vertreten: grün, FG wurde in den letzten 3 FB-LG-Sitzungen nicht, aber in den letzten 6 FB-LG-Sitzungen laut Protokoll wenigstens einmal vertreten: gelb, FG wurde in den letzten 6 FB-LG-Sitzungen kein einziges Mal vertreten: rot
- Organisation einer Veranstaltung: letzte Veranstaltung, die von der FG (co-) organisiert wurde, fand im aktuellen Jahr statt: grün, im Vorjahr: gelb, vor dem Vorjahr: rot
- Für die Einstufung gilt der Durchschnittswert, d.h. ein rot kann durch ein grün zugunsten ein gelb ausgeglichen werden; bei Gleichstand zwischen zwei Indizes wird der bessere Wert ausgewählt

Auch für 2021 konnte auf dieser Grundlage erfreulicherweise festgestellt werden, dass alle Fachgruppen als aktiv einzustufen sind. Allerdings ist zu konstatieren, dass die Vertretung der FG FERS im Leitungsgremium der Fachbereichs Sicherheit mittlerweile kaum noch als gegeben anzusehen ist.

CAST/GI Promotionspreis IT-Sicherheit 2020/2021

Im Rahmen des 17. Deutschen IT-Sicherheitskongresses des Bundesamtes für Sicherheit in der Informationstechnik wurde zum zehnten Mal der Promotionspreis IT-Sicherheit verliehen. Dieser



gemeinsam vom CAST e.V. und dem Fachbereich Sicherheit - Schutz und Zuverlässigkeit - der Gesellschaft für Informatik e.V. ausgeschriebene Preis würdigt hervorragende Dissertationen im Bereich der IT-Sicherheit. Gesucht waren Arbeiten, die einen Fortschritt für die IT-Sicherheit bedeuten und solche, die einen Zugewinn von Sicherheit in IT-Anwendungen ermöglichen. Aus den vorliegenden Einreichungen stellten vier Kandidaten in einem Fachvortrag ihre Arbeiten vor, die zuvor von der CAST/GI Jury aus allen Einreichungen ausgewählt worden waren. Anschließend wurde der Preisträger auf Basis seines Vortrags und der anschließenden Online-Diskussion durch die Teilnehmerinnen und Teilnehmer des Kongresses gewählt.

Der Gewinner des CAST/GI Promotionspreises IT-Sicherheit 2020/2021 ist Herr Dr. **Daniel Demmler** (TU Darmstadt / Universität Hamburg) mit seiner Arbeit **Towards Practical Privacy-Preserving Protocols**.

Zum Inhalt der Arbeit: Der Schutz der Privatsphäre von Nutzerdaten in digitalen Systemen wird immer schwieriger. Zwei Techniken, die dieses Problem angehen und darauf abzielen praktische Berechnungen unter gleichzeitigem Schutz der Privatsphäre zu ermöglichen, sind sichere Mehrparteienberechnung (MPC) und Private Information Retrieval (PIR).

Die Arbeit von Herrn Demmler präsentiert Ergebnisse, die zeigen wie Anwendungen aus der Praxis mit Privatsphäre-Schutz unter gleichzeitiger Erhaltung der Praktikabilität versehen werden können. Dies ist nicht nur der Wunsch vieler Anwender, sondern auch auf einer starken rechtlichen Basis verankert. Diese Arbeit liefert dabei zahlreiche Werkzeuge, die es ermöglichen Privatsphäre-schützende Techniken zu implementieren und zu evaluieren. In der Arbeit wird außerdem an mehreren Beispielen aus der Praxis demonstriert, wie Privatsphäre-Schutz mittels MPC oder PIR effizient und sicher umgesetzt werden kann. Dazu zählen beispielsweise private Routenberechnung im Internet, die private Auslagerung und das geschützte Durchsuchen von Genomdatenbanken, anonyme Kommunikation oder die private Kontaktfindung in Nachrichten-Apps.

Positionierung zum geplanten Zuschnitt der DFG-Fachkollegien

Zur Sitzung des GI-Präsidiums am 25.06.2021 hat der Fachbereich Sicherheit zu den aktuellen Diskussionen und Planungen über einen neuen Zuschnitt der DFG-Fachkollegien der Informatik Position bezogen. Aus Sicht des Fachbereichs sollten hierbei internationale und nationale Strukturen und Klassifikationen der Informatik, wie z.B. die IFIP Technical Committees und Working Groups, das ACM Computing Classification System und die bestehenden Fachbereiche und Fachgruppen der GI ausreichend berücksichtigt werden. Im Bereich „Sicherheit und Verlässlichkeit“ werden im Besonderen Querschnittsaufgaben adressiert, was sich beim Zuschnitt geeignet widerspiegeln sollte. Die geplante Reduktion für „Sicherheit und Verlässlichkeit“ im Zuge einer Zusammenlegung mit dem bisherigen Bereich Betriebssysteme ist anhand der jetzigen und zu erwartenden Bedrohungslage sowie der Aktualität und Wichtigkeit unseres Bereiches aus Sicht des Fachbereichs Sicherheit nicht wünschenswert.

Positionierung zur tatsächlichen Gesetzesänderung im Zuge vom IT-Sicherheitsgesetz 2.0

Folgende Punkte aus dem verabschiedeten IT-Sicherheitsgesetz 2.0 weisen aus Sicht des GI-Fachbereichs Sicherheit einen Bezug zur abgegebenen Stellungnahme des Fachbereichs auf:

- Zulieferer als Unternehmen im besonderen öffentlichen Interesse: In den Kreis der KRITIS-Verpflichteten wurden Zulieferer der größten Unternehmen in Deutschland aufgenommen, welche wegen ihrer Alleinstellungsmerkmale von wesentlicher Bedeutung sind, was allerdings erst noch im Rahmen einer Rechtsverordnung näher bestimmt werden wird.
- Aufgabe BSI hinsichtlich Stand der Technik: Das BSI beschreibt nur den Stand der Technik und entwickelt diesen nicht, und hat dabei bestehende Normen und Standards zu berücksichtigen und betroffene Wirtschaftsverbände einzubeziehen.
- Organisatorischer Status des BSI: Das BSI hat künftig „auf Grundlage wissenschaftlich-technischer Erkenntnisse“ zu arbeiten, bleibt aber dem BMI zugeordnet und unterliegt weiterhin einigen Restriktionen (insbesondere hinsichtlich einer fortbestehenden eingeschränkten Veröffentlichungsbefugnis über relevante Sicherheitslücken).



- Detektion von Sicherheitsrisiken für die Netz- und IT-Sicherheit: Generell wurde nunmehr klargestellt, dass ein Zugriff auf Informationen sowie informationsverarbeitende Systemen, Komponenten und Prozesse ausschließlich durch autorisierte Personen oder Programme erfolgen darf, was damit insbesondere auch für entsprechende Tests des BSI gilt.
- Aufbewahrungspflicht von Protokolldaten: Die kritisierte überlange Aufbewahrung auf Seiten der KRITIS-Betreiber wurde bereits im Rahmen der BMI-Anhörung rausgestrichen, generell gilt da jetzt für alle 18 Monate, um APT-Angriffen effektiver begegnen zu können.
- Untersagung des Einsatzes kritischer Komponenten: Die zugehörige gesetzliche Regelung wurde komplett überarbeitet. Der geplante, erstmalige Einsatz einer kritischen Komponente, die zu einem Ausfall oder einer erheblichen Beeinträchtigung der Funktionsfähigkeit einer kritischen Infrastruktur führen können, ist künftig dem BMI anzuzeigen und erfordert eine Garantieerklärung des Hersteller, dass die betreffenden Komponenten nicht über technische Eigenschaften verfügen, die geeignet sind, missbräuchlich auf die Sicherheit, Vertraulichkeit, Integrität, Verfügbarkeit oder Funktionsfähigkeit der kritischen Infrastruktur einzuwirken.

Insgesamt sieht sich der GI-Fachbereich Sicherheit darin bestärkt, mit fachlichen Stellungnahmen auf die weitere Fortentwicklung von Regelungen zur Cybersicherheit einzuwirken und verfolgt die aktuelle Entwicklung auch auf europäischer Ebene mit hohem Interesse.

Positionierung zur Novellierung der BSI-KritisV

Der GI-Fachbereich Sicherheit - Schutz und Zuverlässigkeit - hat Stellung bezogen zum Referentenentwurf des Bundesministeriums des Inneren, für Bau und Heimat (BMI) über die zweite Verordnung zur Änderung der BSI-Kritisverordnung und darin im Wesentlichen Änderungsbedarf identifiziert bei den Begriffsbestimmungen und im Rahmen der Anlagenkategorien sowie hinsichtlich der Schwellenwerte im Sektor Informationstechnik und Telekommunikation.

So hat sich GI-Fachbereich Sicherheit insbesondere dafür ausgesprochen, den Begriff „Software und IT-Dienste“ durch „IT-Systeme“ aus Gründen der Konsistenz mit dem BSIG zu ersetzen, da dieser Begriff als ausreichend trennscharf angesehen werden kann und den inneren Sachzusammenhang aus dem IT-Sicherheitsgesetz zugleich besser abbildet als durch ergänzende Hinzuziehung von IT-Komponenten, die i.d.R. sehr kleinteilig ausfallen und insoweit den Blick auf das Wesentliche verstellen würden.

Als betriebsnotwendig gehören in diesem Zusammenhang aus Sicht des GI-Fachbereichs Sicherheit sowohl die eigentlichen zur Funktionsfähigkeit der kritischen Dienstleistung eingesetzten IT-Systeme als auch die zugehörigen sicherheitstechnischen IT-Systeme (z.B. zur Netzwerksegmentierung, zur Anomalie- bzw. Angriffserkennung, zur Datensicherung und -wiederherstellung, zur Verwaltung relevanter Changes, etc.).

Ferner hat der GI-Fachbereich Sicherheit empfohlen, den Begriff „Nutzer“ durch „Endnutzer“ zu ersetzen.

Wahlprüfsteine des Fachbereichs Sicherheit

Aus Sicht des GI-Fachbereichs Sicherheit sollte aus fachlicher Sicht insbesondere folgende Themen nach der anstehenden Bundestagswahl auf die politische Agenda gesetzt werden:

1) Datenschutzkonforme Digitalisierung

In der Digitalisierung verschiedener Dienste (Überwachung der Einhaltung der Pandemie-Regeln, Schulen, Bürgerdienste) gibt es Nachholbedarf. Außerdem wird oft der Anschein erweckt, dass Datenschutz vieler der Vorhaben im Weg steht. Datenschutz ist eine Notwendigkeit und darf nicht als Ausrede vorgeschoben werden. Wir fordern daher eine zügige datenschutzfreundliche Digitalisierung und dazu insbesondere die Unterstützung der Entwicklung von Open Source, Forschung und entsprechender Regulierung mit dem Ziel einer digitalen, datenschutzfreundlichen Souveränität.

2) Konsistenz in der Förderung der IT-Sicherheit in der Wirtschaft

Aktuell wird die IT-Sicherheit von politischen Entscheidungsträgern einerseits unterstützt, andererseits unterlaufen durch Sicherheitsdienste, die Zero-Day-Exploits für eigene Zwecke nutzen, statt die Behebung der zugrunde liegenden Schwachstellen zu forcieren. Wie beispielsweise Heartbreak gezeigt hat, können die Exploits dann aber auch von anderen zum Schaden unserer Wirtschaft genutzt werden.



Ähnliches gilt für die Forderung danach, Hintertüren in verschlüsselte Kommunikationssysteme einzubauen, um eigenen Sicherheitsdiensten zu ermöglichen, die Verschlüsselung zu brechen. Auch hier ist es eine Illusion zu glauben, dass solche Hintertüren vor Angreifern (Kriminelle, fremde Sicherheitsdienste) dauerhaft geschützt werden könnten. Gleichzeitig ist davon auszugehen, dass diejenigen, deren Kommunikation in erster Linie abgehört werden soll, dieser Überwachung ausweichen und auf bestehende und weiterhin verfügbare Verschlüsselungssysteme wie PGP zurückgreifen würden.

3) Safety und Reliability intelligenter, autonomer und in Teilen vernetzter Systeme

Das ist lebensnotwendig, sonst können wir uns auf intelligente Systeme und autonome Unterstützung nicht verlassen.

Kontaktmöglichkeiten:

- E-Mail-Verteiler: <https://lists.gi.de/postorius/lists/fbsec.gi-fb-sicherheit.de/>
- Webseite: <http://fb-sicherheit.gi.de/>



Jahresberichte der einzelnen Fachgruppen

Fachgruppe Ada – Zuverlässige Software-Systeme

Intention der Fachgruppe

Software garantiert häufig direkt die Sicherheit für Menschen. Ada wird in internationalen Sicherheitsstandards empfohlen und unterstützt in einzigartiger Weise moderne Analyse, Design und Programmiermethoden und damit die Entwicklung großer zuverlässiger Software-Systeme. Die Fachgruppe will über die Konzepte von Ada und deren Bedeutung für die Softwaretechnologie informieren.

Fachgruppenleitung

- Sprecher: Hubert B. Keller (KIT, Karlsruhe)
- Stv. Sprecher: Herbert Klenk (EADS Deutschland GmbH, Manching)
- Peter Dencker (ETAS GmbH, Stuttgart)
- Christoph Grein (ESG Elektroniksystem- und Logistik-GmbH, München)
- Peter Hermann (Universität Stuttgart, Institut für Höchstleistungsrechnen, Stuttgart)

Aktivitäten 2020/2021

- Mitgliederversammlung 2020
Die Mitgliederversammlung der FG Ada fand am Dienstag, 24.11.2020 16.00 Uhr statt. Die Tagesordnung umfasste Begrüßung, Bericht des Sprechers über die Aktivitäten im Jahr 2019 und bis dato, Wahlen zum Vorstand der Fachgruppe, Planung der Veranstaltungen in den Jahren 2020 und 2021 angesichts der Corona-Krise sowie Verschiedenes.
- Die geplante Tagung SafeWare 2019 und auch der Workshop SafeWare 2020 im Rahmen der GI-Jahrestagung mussten ausfallen.
- Als Kandidaten für den Vorstand stellen sich zur Verfügung: Peter Dencker, Hubert Keller, Herbert Klenk, Tobias Philipp. Alle wurden einstimmig gewählt. Hubert Keller wurde als Sprecher der Fachgruppe mit Vertretung durch Peter Dencker gewählt.
- Mit dem Titel „Maschinelle Intelligenz - Verfahren und Innovationspotentiale“ hielt Hubert Keller einen Vortrag auf dem Meeting Point Internationalisierung der ClusterAgentur Baden-Württemberg, Künstliche Intelligenz in der Anwendung – Potenziale und Grenzen der Kooperation mit Frankreich und anderen europäischen Ländern, am 22. Januar 2020, im Haus der Wirtschaft, Stuttgart.
- Hubert Keller hat einen Vortrag auf der 7. Berliner Gesamtkonferenz der Sicherheitsinstitutionen am 28. Februar 2020, Berlin, über „Lessons learned – PISEA Ergebnis in Safety und IT-Security (PISEA - Programme for International Science and Engineering Assessment) gehalten, der nun in gedruckter Form vorliegt.
- Auf der INFORMATIK 2020 wurde die Session „Software Engineering“ am Dienstag, 29.09.2020 von Hubert Keller zusammen mit Steffen Becker organisiert. Innerhalb der Session gab es drei Fachvorträge, die über ein Videokonferenzsystem vorgetragen wurden. Die Vorträge waren „Safe and Secure Software Engineering - the SPARK Approach“ von Yannick Moy, AdaCore, Paris; „Agile Organisation und Führung innerhalb der Softwareentwicklung Wie geht das zusammen?“ von Andreas Störzbach, Trumpf, Deutschland und „Wie Cloud-native-Ansätze Architektur(arbeit) verändert“ von Thomas Franz, adesso.
- Auf dem Karlsruher Entwicklertag 2021 vom 9. bis 10. Juni 2021 hatte Hubert Keller den Vortrag „Security byDesign und agiles Vorgehen – Integration oder Widerspruch?“ gehalten. Circa 100 Teilnehmer diskutierten intensiv die Inhalte.

Das langjährige Vorstandsmitglied Dr. Herbert Klenk starb für uns alle überraschend am 27. Juli 2021.



Nachruf: Herbert Klenk war seit Jahrzehnten eine wichtige Stütze in unserer Arbeit mit Ada Deutschland und ist uns als Freund ans Herz gewachsen. Noch vor Kurzem haben wir über die zukünftigen Planungen gesprochen. Herbert hat in der Organisation unserer Konferenzen seit vielen Jahren mitgewirkt, die Anmeldungen bearbeitet, die Konferenzbände erstellt und mit vielen Ratschlägen und Hinweisen den Erfolg unserer Arbeit mit gesichert. Mit seiner sachlichen, ruhigen, überlegten und gleichzeitig freudigen Art haben wir gemeinsam vieles bewegt und erreicht. Sowohl persönlich als Mensch wie auch als Experte hat er uns immer wieder beeindruckt. In unserer Gruppe wird er uns fehlen, er hinterlässt eine Lücke, die wir nicht schließen können. Seiner Familie sprechen wir unser tiefes Beileid aus. Wir sind dankbar, dass wir mit ihm haben arbeiten können. Herbert Klenk wird immer in unseren Gedanken bleiben.

Hubert Keller

Kontaktmöglichkeiten:

- E-Mail-Verteiler: ada@gi-fb-sicherheit.de
- Webseite Fachgruppe: <http://www.ada-deutschland.de/fg-ada>



Fachgruppe BIOSIG

Intention der Fachgruppe

Die Fachgruppe widmet sich thematisch den Grundlagen, Methoden, Techniken, Abläufen und Realisierungen zur Sicherung der Authentizität und Integrität beteiligter Entitäten beim Einsatz von Informations-, Kommunikations- und Betriebssystemen für Anwendungen mit Sicherheitsbedarf sowie deren organisatorischen und rechtlichen Rahmenbedingungen. Hierbei werden konstruktive Vorgehensweisen und Bedrohungsanalysen behandelt.

Fachgruppenleitung

- Sprecher: Heiko Roßnagel (Fraunhofer IAO)
- Stv. Sprecherin: Kristina Unverricht (DIN)
- 2ter Stv. Sprecher und Wart für Wissenschaft, Forschung und Lehre: Arslan Brömme (Vattenfall AG)
- Kassenwart: Christoph Busch (Hochschule Darmstadt)
- Technikwart für Mailinglisten und Webseite: Victor-Philipp Busch (Sybuca GmbH)
- Pressewart und Organisator für Workshops: Alexander Nouak (Fraunhofer IGD)

Verantwortlichkeiten

E-Mail-Verteiler-Moderation: V-P. Busch

Web-Seiten: V-P. Busch

Aktivitäten und Veranstaltungen

- 15.-17. September 2021, Darmstadt (virtuell)
20. internationale BIOSIG Konferenz der Biometrics Special Interest Group, Tagungsband erschienen in LNI:
https://dl.gi.de/handle/20.500.12116/37442/browse?type=title&sort_by=4
Veranstaltungsbericht zur BIOSIG 2021:
<https://fg-biosig.gi.de/mitteilung/conference-report-on-ieee-biosig-2021>
- 01.-02. Juni 2021, Kopenhagen, Dänemark (virtuell)
8. Open Identity Summit
<https://oid2021.compute.dtu.dk/>
Tagungsband erschienen in LNI:
https://dl.gi.de/handle/20.500.12116/36436/browse?type=title&sort_by=4
Veranstaltungsbericht:
In diesem Jahr fand der zum achten Mal durchgeführte Open Identity Summit vom 1.-2. Juni 2021 als virtuelle Veranstaltung statt. Das Programm findet sich unter <https://oid2021.compute.dtu.dk/prog.html> und der Tagungsband ist unter https://dl.gi.de/handle/20.500.12116/36436/browse?type=title&sort_by=4 verfügbar. Der Call for Papers wurde im Herbst 2020 verteilt. Insgesamt wurden 15 Beiträge angenommen (Akzeptanzrate 48%).
Die Auswahl der eingereichten Beiträge wurde durch Kurzbeiträge ergänzt. Der nächste Open Identity Summit wird im Juli 2022 in Kopenhagen (und/oder virtuell) stattfinden. Der Call for Papers ist unter <http://www.openidentity.eu/> erreichbar.

Kontaktmöglichkeiten

- E-Mail-Info: webmaster@biosig.de
- E-Mail-Verteiler: biosig@gi-fb-sicherheit.de
- Webseiten Fachgruppe: <http://www.biosig.de/>



Fachgruppe ECOM

Die Fachgruppe E-Commerce, E-Government und Sicherheit bearbeitet Fragen zur IT-Sicherheit in den Schwerpunkten E-Commerce, E-Government, E-Voting und Usable Security und Privacy. Weitere Informationen sind auf der Webseite der Fachgruppe (<http://fg-ecom.gi.de/>) zu finden.

Fachgruppenleitung

- Sprecher: Jörg Helbach (HSPV Köln)
- Stv. Sprecherin: Oksana Kulyk (KIT Karlsruhe)
- Robert Krimmer (Tallin University of Technology)

Fachexperten

- Rüdiger Grimm (Universität Koblenz)
- Melanie Volkamer (KIT Karlsruhe)

Veranstaltungen

- Workshop “Recht und Technik, Datenschutz im Diskurs“ am 27.09.2021 im Rahmen der INFORMATIK 2021
Organisation: Rüdiger Grimm, Gerrit Hornung, Christoph Sorge, Indra Spiecker mit etwa 40 Teilnehmern
- Konferenz E-VOTE-ID 2021, 06.-08.10.2021, International Conference for Electronic Voting (online)
Organisation: Krimmer, Volkamer

Kontaktmöglichkeiten

- E-Mail: Kontaktformular ECOM (<http://fg-ecom.gi.de/fachgruppe-ecom/kontakt.html>), joerg.helbach@hspv.nrw.de bzw. oksana.kulyk@secuso.org
- Webseite: <http://fg-ecom.gi.de>



Fachgruppe ENCRESS (Zuverlässigkeit und Sicherheit software-basierter Systeme)

Intention der Fachgruppe

Die Fachgruppe ENCRESS befasst sich mit der Erzielung und der Bewertung der Zuverlässigkeit komplexer Softwaresysteme und der technischen Sicherheit software-basierter Steuerungen mit dem Ziel einer länder- und anwendungs-übergreifenden Normierung der Entwicklungs- und Genehmigungsprozesse. Entsprechend dieser Zielsetzung wendet sich die Fachgruppe an alle industriellen und akademischen Beteiligten des Sektors, insbesondere an Entwickler, Forscher und Anwender. Die ENCRESS-Gemeinschaft besteht seit 1994, als sie im Zusammenhang mit der Entstehung eines europäischen Netzwerks (European Network of Clubs for Reliability and Safety of Software-Intensive Systems) auf diesem Fachgebiet gegründet wurde. Seit 1998 besteht ENCRESS als GI-Fachgruppe des Fachbereichs "Technische Informatik"; seit Gründung des Fachbereichs "Sicherheit" im Jahr 2002 ist die Fachgruppe ENCRESS Mitglied beider Fachbereiche.

Fachgruppenleitung

- Sprecherin: Francesca Saglietti (Universität Erlangen-Nürnberg)
- Stv. Sprecher: Karl-Erwin Grosspietsch
- Wolfgang Ehrenberger (Hochschule Fulda)
- Frank Ortmeier (Universität Magdeburg)

Aktivitäten und Veranstaltungen

- SAFECOMP 2021 hat im September 2021 virtuell stattgefunden. Organisiert wurde die Tagung von der University of York unter der Leitung von John McDermid.

Geplante Aktivitäten:

- SAFECOMP 2022 wird im September 2022 in Garching bei München stattfinden; die Tagung wird von Mario Trapp (Fraunhofer-Institut für Kognitive Systeme) und Francesca Saglietti (Universität Erlangen-Nürnberg) gemeinsam organisiert.
- SAFECOMP 2023 soll im September 2023 in Toulouse unter der Leitung von Jérémie Guiochet (LAAS) stattfinden.

Kontaktmöglichkeiten

- E-Mail: saglietti@informatik.uni-erlangen.de
- Web: <http://www11.informatik.uni-erlangen.de/Encress/>



Fachgruppe EZQN

Intention der Fachgruppe

Die Fachgruppe Evaluation, Zertifizierung, Qualitätssicherung, Normung (EZQN) widmet sich der ganzheitlichen Bewertung von Cyber-Sicherheit und Cyber-physical Systems, u.a. Fahrzeugen, sowie querschnittlichen Aspekten wie Metriken von IT-Sicherheit. Sie schlägt dabei eine Brücke zur Normung, vor allem des DIN NIA-01-27 IT-Sicherheitsverfahren und zu FOCUS.ICT.

Fachgruppenleitung

- Sprecher: Peer Reymann (ITQS, Norderstedt)
- Stellvertretender Sprecher: Marian Margraf (FU Berlin)
- Francesca Saglietti (Universität Erlangen-Nürnberg)
- Kai Rannenberg (Universität Frankfurt am Main)
- Stefan Helfert (Helfert Informatik GmbH & Co. KG)
- Hans von Sommerfeld (VOSDAV GmbH)

Verantwortlichkeiten

- Obmann DIN NIA-01-27 IT-Sicherheitsverfahren: Hans von Sommerfeld (bis Ende 2021)
- GI-Vertreter bei FOCUS.ICT am DIN: Hans von Sommerfeld (bis Ende 2021)
- Convenor ISO/IEC JTC 1/SC 27/WG 5: Kai Rannenberg

Aktivitäten und Veranstaltungen

- Eine Wahlversammlung konnte weiterhin aufgrund der Pandemielage auch in 2021 nicht durchgeführt werden; für 2022 wird das Leitungsgremium die Möglichkeiten der Online-Wahl bzw. einer Veranstaltung im Sommer erörtern.
- Eine Anfrage an einen Fachexperten zur Übernahme der Vertretung beim DIN als Nachfolger für Hans von Sommerfeld wird in den kommenden Monaten entschieden.
- Beteiligung an der Normung Datenschutz und Informationssicherheit

Kontaktmöglichkeiten

- E-Mail: ezqn@gi-fb-sicherheit.de
- Webseite: <http://fg-ezqn.gi.de> sowie <https://www.ezqn.de>



Fachgruppe FERS

Intention der Fachgruppe

Fehlertoleranz - die Eigenschaft eines Systems, trotz interner Fehler nach außen das korrekte Verhalten zu zeigen - steht immer dann im Mittelpunkt des Interesses eines Rechnerarchitekten, wenn es um Zuverlässigkeit, Verfügbarkeit, Robustheit und auch Sicherheit, kurz Verlässlichkeit eines Rechners geht. Es gilt zu vermeiden, dass durch ein Versagen des Rechners große wirtschaftliche Verluste entstehen oder gar Menschenleben gefährdet werden.

Ein fehlertolerierendes Rechensystem genügt in seiner Architektur Fehlertoleranzanforderungen und ist zuverlässiger als die Gesamtheit seiner Teile. Zusätzlich lassen sich durch

Fehlertoleranzmaßnahmen seine Wartbarkeit erhöhen und die Lebenszykluskosten verringern.

Zunehmende Bedeutung gewinnen derartige Systeme durch ihr Vordringen in Anwendungsgebiete, die ein Höchstmaß an garantierter und damit verifizierbarer Verlässlichkeit verlangen. Deshalb muss sich die Systementwicklung auch mit Verfahren zur Bewertung von Verlässlichkeit und dazu geeigneten Werkzeugen beschäftigen.

Fehlertolerierende Rechensysteme sind vor allem in den Bereichen Transaktions- und Prozessverarbeitung sowie verteilter und massiv-paralleler Systeme von Bedeutung und machen zukünftig viele Anwendungen für Rechner erst möglich.

Fachgruppenleitung

- Sprecher: Bernhard Fechner (FernUniversität in Hagen)
- Stv. Sprecher: Peter Sobe (Hochschule für Technik und Wirtschaft, Dresden)

Aktivitäten

Nach eigenem Verständnis berichtet die Fachgruppe FERS dem GI-Fachbereich Technische Informatik und hat diesem fristgerecht einen entsprechenden Jahresbericht zugesandt.

Kontaktmöglichkeiten

- E-Mail: bernhard.fechner@fernuni-hagen.de
- Webseite: <https://fg-fers.gi.de>



Fachgruppe FoMSESS

Intention der Fachgruppe

Zielsetzung der Fachgruppe "Formale Methoden und Software Engineering für sichere Systeme" (FoMSESS) ist es, im Bereich Computer- und Informationssicherheit ein Diskussionsforum im deutschsprachigen Raum zu bieten, das sich mit der Grundlagenforschung und Anwendung formaler oder mathematisch präziser Techniken im Software-Engineering beschäftigt. Von Interesse für die FG ist Sicherheit im Sinne sowohl von Safety als auch von Security. Besonders wichtig ist die Erkenntnis, dass Sicherheit eine ganzheitliche Eigenschaft von Systemen ist.

Fachgruppenleitung

- Sprecher: Zoltan Mann (Universität Amsterdam)
- Stv. Sprecher: Dieter Hutter (DFKI Bremen)
- Bernhard Beckert (KIT)
- Maritta Heisel (Universität Duisburg-Essen)
- Andreas Nonnengart (DFKI Saarbrücken)

Aktivitäten und Veranstaltungen

Die Fachgruppe FoMSESS hat 2021 zwei Online-Workshops zu ausgewählten Themen organisiert. Im Januar fand der Workshop „FormalDSGVO: Mehr Digitale Souveränität durch Formalisierung und automatische Verarbeitung von Datenschutzerklärungen“ statt. Im Juli folgte der Workshop „Formalisierung von Fairness und Diskriminierungsfreiheit“. Trotz des pandemiebedingten Onlineformats waren die Workshops gut besucht und ermöglichten eine rege Diskussion. Im September erschien ein Beitrag als „Thema im Fokus“ im GI-Radar zu Online-Wahlen, an dem mehrere FoMSESS-Mitglieder beteiligt waren.

Im Oktober erfolgte das 18. Jahrestreffen der Fachgruppe. Das Programm enthielt unter anderem drei eingeladene Vorträge zum Thema Sicherheit von Online-Wahlen. Die extended Abstracts der Vorträge wurden auf der Website der Fachgruppe veröffentlicht.

Nach der Erstausgabe im Dezember 2020 erschien die zweite Ausgabe des Newsletters der Fachgruppe im Juni 2021. Die dritte Ausgabe ist für Dezember 2021 geplant.

Kontaktmöglichkeiten

- E-Mail: fomsess@gi-fb-sicherheit.de
- Webseite: <http://fg-fomsess.gi.de/>



Fachgruppe KRYPTO

Intention der Fachgruppe

Die Fachgruppe für Angewandte Kryptologie des Fachbereichs Sicherheit - Schutz und Zuverlässigkeit will deutschsprachige Anwender und Forscher im Bereich der Kryptologie vernetzen. Besonderes Augenmerk liegt dabei in der Förderung des wissenschaftlichen Nachwuchses. Der Hauptschwerpunkt der Arbeit liegt in Deutschland. Nach Auffassung der Fachgruppe umfasst Kryptologie den Entwurf, die Analyse, die Implementierung und den praktischen Einsatz von Kryptosystemen.

Fachgruppenleitung

- Sprecher: Daniel Loebenberger (Ostbayerische Technische Hochschule Amberg-Weiden/Fraunhofer AISEC)
- Stv. Sprecher: Michael Nüsken (Universität Bonn)
- Frederik Armknecht (Universität Mannheim)
- Stefan-Lukas Gazdag (genua GmbH)
- Sophia Grundner-Culemann (Ludwig-Maximilians-Universität München)
- Tobias Guggemos (Ludwig-Maximilians-Universität München)
- Alexander Koch (Karlsruher Institut für Technologie)
- Mathias Kohler (SAP)
- Juliane Krämer (Universität Regensburg)
- Kerstin Lemke-Rust (Hochschule Bonn-Rhein-Sieg)
- Mario Strefler (KIT)
- Marcel Tiepelt (Karlsruher Institut für Technologie)

Verantwortlichkeiten

- Web-Seite: Michael Nüsken, Juliane Krämer, Daniel Loebenberger
- Organisation Krypto-Tag: Stefan-Lukas Gazdag, Daniel Loebenberger, Michael Nüsken
- Organisation crypt@b-it: Michael Nüsken, Sophia Grundner-Culeman, Marcel Tiepelt

Aktivitäten und Veranstaltungen

- Workshop PQKP @ INFORMATIK 2021
<https://fg-krypto.gi.de/veranstaltung/workshop-post-quanten-kryptographie-in-der-praxis>
- Kryptotage
Corona-bedingt wurden zwei Kryptotage 2021 digital mit großem Erfolg durchgeführt:
32. Krypto-Tag, 15. Januar 2021
1st Digital Summit, Germany
33. Krypto-Tag, 17. September 2021
2nd Digital Summit, Germany

Pläne für 2022

Für 2022 planen wir zwei Kryptotage, sowie eine Sommerschule crypt@b-it gemeinsam mit der RUB Bochum, der Uni Bonn, in Kooperation mit der IACR.

Veröffentlichungen

- "crypto day matters", die Proceedings des Krypto-Tags werden online in der GI Digital Library veröffentlicht. Verweise sind zu finden unter <https://fg-krypto.gi.de/krypto-tag>.

Kontaktmöglichkeiten

- E-Mail: FG Krypto krypto-lg@gi-fb-sicherheit.de
- E-Mail: Daniel Loebenberger <daniel.loebenberger@aisec.fraunhofer.de>
- Webseite: <http://fg-krypto.gi.de>





Fachgruppe NETSEC

Intention der Fachgruppe

Die Fachgruppe Sicherheit in Mobil- und Festnetzen (NETSEC) beschäftigt sich mit Gefahren und deren Abwehr, die durch die zunehmende Vernetzung von ITK-Systemen entstehen. Auf der einen Seite sollen Gefahren betrachtet werden, die durch die technische Vernetzung an sich entstehen. Auf der anderen Seite hat die Vernetzung von Systemen ein erhebliches Missbrauchspotenzial. Die jüngsten zerstörerischen Angriffe von Hackern oder Virenautoren sind allgemein aus den Medien bekannt. Die Fachgruppe fördert die Entwicklung von Verfahren und Werkzeuge, die sowohl beim Schutz existierender Netze helfen als auch bei der Entwicklung neuer Vernetzungen greifen.

Fachgruppenleitung

- Sprecher: Matthias Marx (Universität Hamburg)
- Stv. Sprecherin: Monina Schwarz (Universität Hamburg)
- Florian Tschorsch (TU Berlin)
- Paul Duplys (Bosch)
- Christian Schlehuber (DB Netz AG)

Aktivitäten und Veranstaltungen

- Monatliche Telefonkonferenzen des Leitungsgremiums
- Erfolgreiche Nachwuchswerbung für die Mitarbeit in der Fachgruppe und im Leitungsgremium sowie gemeinsame Neuausrichtung der Fachgruppe

geplante Aktivitäten

Wir möchten einen Newsletter initiieren, in dem halbjährlich von Konferenzen, neuen Forschungsvorhaben, abgeschlossenen Dissertationen und aus dem Fachbereich berichtet wird. Außerdem möchten wir eine weitere Diskussionsveranstaltung zu einem kontroversen (noch nicht feststehenden) Thema durchführen. Außerdem haben Planungen für eine Ringvorlesung „NetSec Hot Topics“ begonnen, welche verteilt online oder hybrid veranstaltet werden soll.

Kontaktmöglichkeiten

- Webseite: <https://fg-netsec.gi.de/>
- Kontakt: <https://fg-netsec.gi.de/kontakt/>
- Twitter: <https://twitter.com/FGNetsec>



Fachgruppe PET

Intention der Fachgruppe

Die Fachgruppe PET hat sich zum Ziel gesetzt, alle relevanten Aspekte zu "Privacy-Enhancing Technologies" und "Datenschutzfördernder Technik" in die aktuellen Diskussionen sowohl der Wissenschaft, Wirtschaft und Gesetzgebungsorgane als auch der Anwender selbst und in Projekte des Fachbereichs Sicherheit der Gesellschaft für Informatik e.V. im speziellen einzubringen und deren technologischen, gesellschaftlichen und wirtschaftlichen Nutzen im Kontext mit Themen der Informatik zu erklären.

Fachgruppenleitung

- - Sprecher: Sebastian Pape (Goethe-Universität Frankfurt)
- - Stv. Sprecher: Zoltan Mann (Universität Duisburg-Essen)
- - Dominik Herrmann (Universität Bamberg)
- - Frank Pallas (TU Berlin)
- - Kai Rannenber (Goethe-Universität Frankfurt)
- - Delphine Reinhardt (Universität Göttingen)
- - Aleksandra Sowa (PWC GmbH WPG)
- - Florian Tschorsch (TU Berlin)
- - Bernhard C. Witt (it.sec GmbH)

Verantwortlichkeiten

- Webseite: Bernhard C. Witt und Sebastian Pape
- Mailingliste: Bernhard C. Witt und Sebastian Pape
- PetCon: Dominik Hermann und Sebastian Pape

Aktivitäten und Veranstaltungen

- Monatliche Telefonkonferenzen des Leitungsgremiums
- Wahlen des Leitungsgremiums als Online-Wahl
- Diskussion mit anschließendem Feedback zu den Online-Wahlen an die Geschäftsstelle
- Beteiligung an der Session "Privacy-preserving technologies - a key enabler of big data for AI", European Big Data Value Forum (EBDVF)
- Angebot Workshop auf der Informatik 2021 als "DSMS 2021: Es kann nur einen geben? – Effektives Datenschutzmanagement in Wissenschaft und Praxis" mit FG SECMGT, EZQN und FoMSESS, dann durch Zusammenlegung durchgeführt als Workshop "Security, Datenschutz und Anonymisierung", Beteiligung durch Keynote "Datenschutz und -sicherheit im Internet der Dinge"
- Unterstützung CAST/GI Promotionspreis IT-Sicherheit 2021
- Unterstützung CAST-Förderpreis IT-Sicherheit 2021

Kontaktmöglichkeiten

- Webseite: <http://fg-pet.gi.de/startseite.html>
- Mailing-Liste: <https://lists.gi.de/postorius/lists/pet.gi-fb-sicherheit.de/>
- E-Mail (Sprecher): [sebastian.pape\(at\)m-chair.de](mailto:sebastian.pape(at)m-chair.de)
- E-Mail (Stv. Sprecher): [zoltan.mann\(at\)gmail.com](mailto:zoltan.mann(at)gmail.com)



Fachgruppe SECMGT

Intention der Fachgruppe

Die Fachgruppe SECMGT ist ein Praktiker-Forum, das sich seit der Gründung im Jahr 2002 mit dem Management von Informationssicherheit, den entsprechenden Risiken und Lösungen für Unternehmen, Behörden und anderen Organisationen beschäftigt. Dazu gehört auch der Schutz kritischer Informations- und Kommunikationsinfrastrukturen. Wir sehen uns als ein Gremium von Informationssicherheits-Praktikern für Informationssicherheits-Praktiker und bringen uns zukunftsorientiert und ergebnisoffen in die aktuelle Fachdiskussion sowie die Gestaltung von Best Practices zur Informationssicherheit ein. Dabei beziehen wir Stellung zu aktuellen Themen und beschäftigen uns mit gesetzlichen Vorgaben wie dem IT-Sicherheitsgesetz oder der DSGVO sowie praxisrelevanten Standards wie z.B. der ISO/IEC 27001. Über unsere Mitglieder wirken wir aktiv an der Normung zur Informationssicherheit mit. Darüber hinaus fördern wir die berufliche Weiterbildung im Bereich der Informationssicherheit, indem wir auch für Nicht-GI-Mitglieder eine neutrale Plattform zum Erfahrungsaustausch und zur Vernetzung der zugehörigen Community (GI-übergreifend) bieten. Aufgrund der Corona-Situation hat auch die Fachgruppe SECMGT seit dem Jahr 2020 ihre Vorgehensweise angepasst.

Wir haben im September 2020 unseren ersten digitalen Workshop veranstaltet. Unter dem Titel ‚Corona-Lessons learned‘ haben wir ein aktuelles Thema und dessen Bezug zu Informationssicherheit mit einer großen Bandbreite an Referenten bearbeitet. Der Workshop war gut besucht.

Unsere Workshops ermöglichen GI-Mitgliedern und auch Nicht-Mitgliedern, in einen fruchtbaren fachlichen Austausch mit starkem Praxisbezug zu treten. Für die Workshops werden keine Tagungsgebühren erhoben und der GI keine Kosten belastet. Sie werden vollständig durch das Leitungsgremium organisiert.

Die Fachgruppe hat dauerhafte Kooperationen mit

- • CAST e.V.
- • D-A-CH Security
- • GI-FG PET

Die Mitgliederzahl ist weiterhin stabil (389 Mitglieder/Stand Dezember 2021). Der Webauftritt der FG SECMGT wird ständig aktualisiert. Er ist unter der URL <https://fg-secmgt.gi.de/> zu erreichen. Auch werden regelmäßig Blog-Beiträge zu unterschiedlichen Fragen des Managements von Informationssicherheit auf der Webseite der Fachgruppe veröffentlicht. Auch außerhalb der Workshops sind wir zu Fachthemen über die auf der Webseite angegebenen Email Adressen erreichbar.

Zur Klärung inhaltlicher und organisatorischer Fragen kommt das Leitungsgremium mindestens einmal pro Monat in einer Telefonkonferenz sowie nach allen Workshops zu einer LG-Sitzung zusammen.

Fachgruppenleitung

- Sprecher: Frank Damm (KPMG AG)
- Stellv. Sprecher: Peer Reymann (ITQS GmbH)
- Thomas Görlich (DB System GmbH)
- Ralf Kneuper (IU Internationale Hochschule)
- Isabel Münch (Bundesamt für Sicherheit in der Informationstechnik)
- Georg Reiss (Stadtwerke Frankfurt a.M.)
- Christopher Rupprich (paydirekt GmbH)
- Marion Steiner (IT-Security@Work GmbH)
- Benedict Voßbein (UIMC GmbH)
- Bernhard C. Witt (it.sec GmbH)

Fachexperten

- Alexander Lawall (IU Internationale Hochschule)



Aktivitäten und Veranstaltungen

- 5. März 2021 Online-Workshop der Fachgruppe zum Thema: Privacy Shield adé!
Standardvertragsklauseln passé?!? ...und dann auch noch der Brexit
- 28. Mai 2021 Online-Workshop der Fachgruppe zum Thema: Cloud Security? Made in
Europa!
- 27. September bis 1. Oktober 2021 Workshop bei der Konferenz Informatik 2021 zum Thema
Nachhaltiges Sicherheitsmanagement

geplante Aktivitäten

- Freitag, 18. März 2022, digitaler Workshop: " Informationssicherheit in der Lieferkette"

Kontaktmöglichkeiten

- E-Mail: mail@fg-secmgt.gi.de
- Webseite: www.fg-secmgt.gi.de



Fachgruppe SIDAR

Intention der Fachgruppe

Die Fachgruppe beschäftigt sich mit der Erkennung und Beherrschung von Sicherheitsvorfällen im Bereich der Informationstechnik und fokussierte in Veranstaltungen insbesondere die Themen

- Verwundbarkeitsanalyse,
- Intrusion Detection,
- Malware,
- Incident Management und
- Forensik.

Fachgruppenleitung

- Sprecher: Michael Meier (Universität Bonn, Fraunhofer FKIE)
- Stv. Sprecher: Ulrich Flegel (Infineon)
- Sebastian Schmerl (Computacenter)
- Thomas Biege (Finanz Informatik GmbH)
- Holger Morgenstern (Hochschule Albstadt-Sigmaringen)
- Konrad Rieck (TU Braunschweig)
- Matthias Meyer

Fachexperten

- Ulrich Flegel (Infineon)
- Michael Meier (Universität Bonn, Fraunhofer FKIE)
- Dirk Schadt (SPOT)

Aktivitäten und Veranstaltungen

- 28. DFN-Konferenz „Sicherheit in vernetzten Systemen“, 15.-18. März 2021, Online-Webinar, Typ d (u.a. Beteiligung im Programmkomitee), <https://www.dfn-cert.de/veranstaltungen/vortrage-vergangener-workshops/28Siko2021.html>
- 18. internationale DIMVA-Konferenz der FG „Detection of Intrusions and Malware, and Vulnerability Assessment“, Virtual Event, July 14-16, 2021, Typ a1, <https://www.dimva.org/dimva2021/>

Veröffentlichungen

- Detection of Intrusions and Malware, and Vulnerability Assessment, Leyla Bilge, Lorenzo Cavallaro, Giancarlo Pellegrino, Nuno Neves (Eds.), 18. International Conference, DIMVA 2021, Virtual Event, July 14-16 2021. Proceedings. Springer 2021, Lecture Notes in Computer Science No. 12756, ISBN 978-3-030-80825-9.

Kontaktmöglichkeiten

- Webseite: <http://fg-sidar.gi.de/>



Fachgruppe UseSafeSec

Intention der Fachgruppe

Computerbasierte Systeme können nur dann sicher sein, wenn sowohl die primär technischen Aspekte (z.B. Zuverlässigkeit) als auch die nutzungsorientierten Aspekte (z.B. Gebrauchstauglichkeit) angemessen und ihrem Zusammenwirken berücksichtigt werden. Gute Benutzbarkeit ist dabei ein zentraler Bestandteil für die Verbesserung der Systemsicherheit.

Die Fachgruppe beschäftigt sich aus Perspektive der Mensch-Computer-Interaktion mit Sicherheitskonzepten und betrachtet dabei die beide Dimensionen des Sicherheitsbegriffs: Safety (Schutz vor unbeabsichtigten Ereignissen, auch: funktionale Sicherheit) und Security (Schutz vor Angriffen, auch: Informationssicherheit). Der Schwerpunkt Usable Security setzt sich mit der Nutzbarkeit der Sicherheitskonzepte selbst auseinander und entwickelt Konzepte zur Steigerung des Sicherheitsbewusstseins der Nutzer. Das Themenfeld Usable Safety beschäftigt sich mit der MCI in sicherheitskritischen Kontexten, wie in Leitwarten, der Medizin, im Katastrophenschutz oder im Automobil, sowohl unter Berücksichtigung möglicher Bedrohungsszenarien als auch im Sinne der funktionalen Sicherheit.

Die Fachgruppe wurde im Frühjahr 2015 gegründet. Die Mitgliederzahlen haben sich in den letzten 3 Jahren wie folgt entwickelt:

Zum 31.12.2019: 31 Mitglieder

Zum 05.12.2020: 52 Mitglieder

Zum 14.12.2021: 60 Mitglieder

Fachgruppenleitung

- Sprecher: Tilo Mentler (Hochschule Trier)
- Stv. Sprecher: Christian Reuter (Technische Universität Darmstadt)
- Simon Nestler (Technische Hochschule Ingolstadt)

Aktivitäten und Veranstaltungen

- Durchführung des 8. Workshops „Mensch-Computer-Interaktion in sicherheitskritischen Systemen“ auf der Mensch und Computer 2021 als Online-Ausgabe mit 7 angenommenen Beiträgen und ca. 30 Teilnehmenden insgesamt. Der jeweilige Vortrag nahm dabei nur einen kleinen Teil der Zeit ein. Schwerpunkt war darauf aufbauend die Teilnehmenden des Workshops mithilfe interaktiver Elemente einzubeziehen.
- Durchführung des Workshops “Control Rooms in Safety Critical Contexts (CRiSCC): Design, Engineering and Evaluation Issues” auf der INTERACT 2021 mit 6 Beiträgen und ca. 20 Teilnehmenden (hybrides Format)

Sonstige Aktivitäten / Planungen

- Die Fachgruppe hat den Austausch mit anderen Gruppen und Mitgliedern der Fachbereiche Mensch-Computer-Interaktion und Sicherheit verstärkt. Dies zeigt sich beispielsweise in gegenseitigen Bekanntmachungen und Unterstützungen entsprechender Workshops, z.B. auf der Mensch und Computer 2021.
- Gemeinsam mit einem Sprecher des UPA-Arbeitskreises „Usable Security & Privacy“ wird derzeit ein Special Issue zu „Usable Security and Privacy with User-Centered Interventions and Transparency Mechanisms“ im Journal Behaviour and Information Technology herausgegeben (erscheint 2022; Gast-Editoren: Christian Reuter, Luigi Lo Iacono, Alexander Benlian)
- Das Springer-Lehrbuch „Sicherheitskritische Mensch-Computer-Interaktion“ ist in einer 2. Auflage erschienen. Es wird vom stellvertretenden Sprecher der Fachgruppe herausgegeben. An den Beiträgen sind u.a. mehrere Mitglieder der Fachgruppe beteiligt.
- Prof. Nestler war als einer der beiden General Conference Chairs für die Mensch und Computer 2021 mitverantwortlich.



- Der Sprecher der Fachgruppe ist Mitglied der Jury für den CAST/GI Promotionspreis IT-Sicherheit 2022.

Kontaktmöglichkeiten

- E-Mail Sprecher: mentler@hochschule-trier.de
- E-Mail Stellvertretung: reuter@peasec.tu-darmstadt.de