MEDCONF 2021

Datum: 21. Oktober 2021
Raum: Paris
Zeitfenster: 11:50 – 16:35 Uhr

Trackchair-Briefing: 20.10. um 08.30 Uhr

MEDCONF 2021

Vortragszeit: 11:50-12:35

Security, die neue Konstante in der Medizintechnikentwicklung

Neben Patientsicherheit (Safety) gewinnt IT-Sicherheit (Security) an immer mehr Bedeutung. Dies ist auch der steigenden Vernetzung von Medizingeräten geschuldet, die Security-Attacken einfacher und lukrativer machen.

Der Fokus dieses Vortrags liegt hauptsächlich auf „Pre-market-Aktivitäten“, insbesondere auf der Threatanalyse/ Threatmodelling und der Risikobewertung als Ausgangspunkt jeder Entwicklung. Es werden verschiedene Diskussionspunkte geboten und „Best practices“ beschrieben.

Dies soll in einen interaktiven Austausch mit den Zuhörern münden, in dem der Erfahrungsschatz und „Top Tipps“ der MedConf Community ausgetauscht werden.

Was lernen die Zuhörer in dem Vortrag:
Vertiefende Betrachtung in Security und Threatanalyse und Risikobewertung

Dr. Nadine Stech ist stellv. Teamleiterin Firmware/ Software bei der seleon GmbH, einem der führenden, international tätigen Anbieter von Dienstleistungen in der Medizintechnik mit den Kernkompetenzen Produktentwicklung, Produktion und Consulting.

Nach dem Studium der Technischen Kybernetik an der Universität Stuttgart war sie jahrelang federführend in der Entwicklung von intelligenten Prothesen und Orthesen in England tätig und schloss berufsbegleitend eine PhD in Biomedical Engineering an der University of Surrey ab. Sie präsentierte bei zahlreichen internationalen Konferenzen u.a. in Deutschland, England und den USA.

Seit 2019 betreut sie bei der seleon diverse Soft- und Firmwareprojekte, die je nach Kundenanforderung ein sehr vielfältiges Spektrum der Medizintechnik abdecken. Besondere Schwerpunkte sind dabei normgerechte, pragmatische Softwareentwicklung und IT-Security.

MEDCONF 2021

Vortragszeit: 13:35-14:20

Immer up-to-date oder die unglaubliche Leichtigkeit des Vulnerability Monitoring

Heutzutage kann es jederzeit passieren, dass schwerwiegende Schwachstellen in verbreiteter Software enthüllt werden und sich damit für Angreifer Hintertüren in unsere Produkte öffnen. Hinzu kommt, dass moderne Software oft dutzende bis hunderte 3rd-Party-Komponenten enthält. Diese kontinuierlich im Blick zu behalten, ist eine Herausforderung für viele Unternehmen. Und wenn Sicherheitslücken, wie etwa Heartbleed, kein großes Medienecho erzeugen, kann es schnell passieren, dass man auf eine Schwachstelle erst spät aufmerksam wird.

Praxisnah präsentieren wir deswegen die Methoden und Werkzeuge, mit denen wir bei TOMTEC Imaging Systems unsere 3rd-Party-Komponenten (SOUP) strukturiert erfassen und das Vulnerability Monitoring automatisiert haben. So sind wir jederzeit im Bilde über die aktuellsten Sicherheitslücken und können darauf reagieren, bevor Angreifer es tun.

Was lernen die Zuhörer in dem Vortrag:

In diesem Vortrag bekommen Zuhörer*innen einen praktischen Einblick in die Automatisierung und die damit verbundene Vereinfachung des kontinuierlichen Vulnerability Monitoring.

Dr. Marcus Freyer, TOMTEC Imaging Systems GmbH

Andreas Freudling, TOMTEC Imaging Systems GmbH

MEDCONF 2021

Vortragszeit: 14:35-15:20

Software-Unit-Verifikation in IEC 62304

In Abschnitt 5.5.5 fordert die IEC 62304 kurz und knapp in einem einzigen Satz „Der Hersteller soll Software-Unit-Verifikation durchführen und die Ergebnisse dokumentieren.“ Um herauszufinden, wie man diese Forderung erfüllen kann, muss man die Norm durchforsten, um Fragen zu klären wie „Was ist eine Unit und was ist Verifikation für die IEC 62304?“. Im Zuge dessen stößt man auf Beispiele für Akzeptanzkriterien, deren Erfüllung im Rahmen der Verifikation nachgewiesen werden kann. Leider sind diese Akzeptanzkriterien nicht näher beschrieben, ein solches Kriterium lautet beispielsweise lediglich „boundary conditions“.

Im Rahmen des Vortrags werden Akzeptanzkriterien anhand von Beispielen interpretiert und es wird beispielsweise gezeigt, welche Codier-Richtlinien in anderen Industriezweigen eingesetzt werden und dass diese auch für Medizintechnik-Software passend sind.

Ferner werden auch Akzeptanzkriterien besprochen, die in IEC 62304 fehlen, die aber in anderen Normen wie IEC 61508 oder ISO 26262 wichtig sind, beispielsweise die Messung der durch die Tests der Software-Unit erreichten Codeüberdeckung oder die Methoden, wie man zu Testfällen für die Software-Unit-Verifikation kommt.

Was lernen die Zuhörer in diesem Vortrag?
Die Zuhörer lernen, wie in anderen Bereichen, beispielsweise der Automobilindustrie, dynamische Unit-Tests und statische Quellcode-Analyse durchgeführt werden und welche Anforderungen (die konkreter sind als in der IEC 62304) gestellt werden. Die Zuhörer erhalten Empfehlungen zu Vorgehensweisen und zum Stand der Technik in anderen Bereichen.

Frank Büchner besitzt ein Diplom in Informatik von der Technischen Hochschule Karlsruhe (heute KIT). Seit vielen Jahren widmet er sich dem Thema Testen und Software-Qualität. Seine Kenntnisse vermittelt er regelmäßig durch Vorträge und Fachartikel. Momentan arbeitet er als „Principal Engineer Software Quality“ bei der Fa. Hitex GmbH in Karlsruhe

MEDCONF 2021

Vortragszeit: 15:50-16:35

Eigener Rechner

Defense in Depth in der Medizintechnik

Künstliche Intelligenz (KI), maschinelles Lernen und Big Data sind branchenübergreifend in aller Munde. Ohne Zweifel müssen Erklärbarkeit und Vertrauen sowie eine glaubwürdige Sicherheitsargumentation speziell im medizinischen Bereich zwingend gewährleistet sein. Nach wie vor stehen Hersteller allerdings vor der Schwierigkeit, dass der normative und regulatorische Rahmen noch nicht klar definiert ist, es entwickeln sich aber vielfältige Ansätze, wie z.B. in VDE-AR-E 2842-61 oder ISO/IEC TR 5469.
Mit dieser Präsentation wollen wir den Ansatz „Defense in Depth“ vorstellen und damit skizzieren wie die Beantwortung typischer Fragestellungen in sicherheitsrelevanten Systemen unterstützt werden kann:

- Wie sicher ist sicher genug?
- Wie quantifiziert man Sicherheit von KI?
- Mit welchen Mechanismen kann man KI-Systeme absichern?

Diese Präsentation soll sowohl Assessoren und Auditoren als auch Ingenieure dabei unterstützen, die Sicherheit von Systemen mit KI zu gewährleisten. Basierend auf unseren praktischen Erfahrungen zeigen wir wie mit Hilfe von "Defense in Depth" eine glaubwürdige Sicherheitsargumentation erstellt werden kann.

Was lernen die Zuhörer in dem Vortrag:

Die Teilnehmer dieses Vortrags lernen die Grundkonzepte von „Defense in Depth“ kennen sowie deren Anwendung für sicherheitsrelevante Systeme, die KI-Methoden beinhalten.

Herr **Tim Jones** ist als Functional Safety Consultant bei der exida.com GmbH tätig. Er verfügt über mehr als 10 Jahre an Erfahrung in den Bereichen Systems und Software Engineering, Signalverarbeitung und Projektmanagement für sicherheitsrelevante Produkte.
Herr Jones studierte an der Fakultät für Elektrotechnik und Informationstechnik der TU Dresden. Nachdem er 2007 seine berufliche Laufbahn bei der Corscience GmbH & Co. KG in der Medizintechnik begonnen hatte, wechselte er 2013 als Experte für Funktionale Sicherheit zur Elektrobit Automotive GmbH. Seit 2016 ist Herr Jones als Funktional Safety Consultant bei der exida.com GmbH tätig. Sein Fokus liegt hier sowohl auf der Medizintechnik als auch der Automobilindustrie.
Herr Jones ist Mitglied der VDI Medical SPICE Standardisierungsgruppen und zusätzlich als Lehrbeauftragter an der TH Nürnberg für die Vorlesung „Funktionale Sicherheit“ verantwortlich.