

DoS Robustheit für Embedded Geräte und Essentielle Funktionen

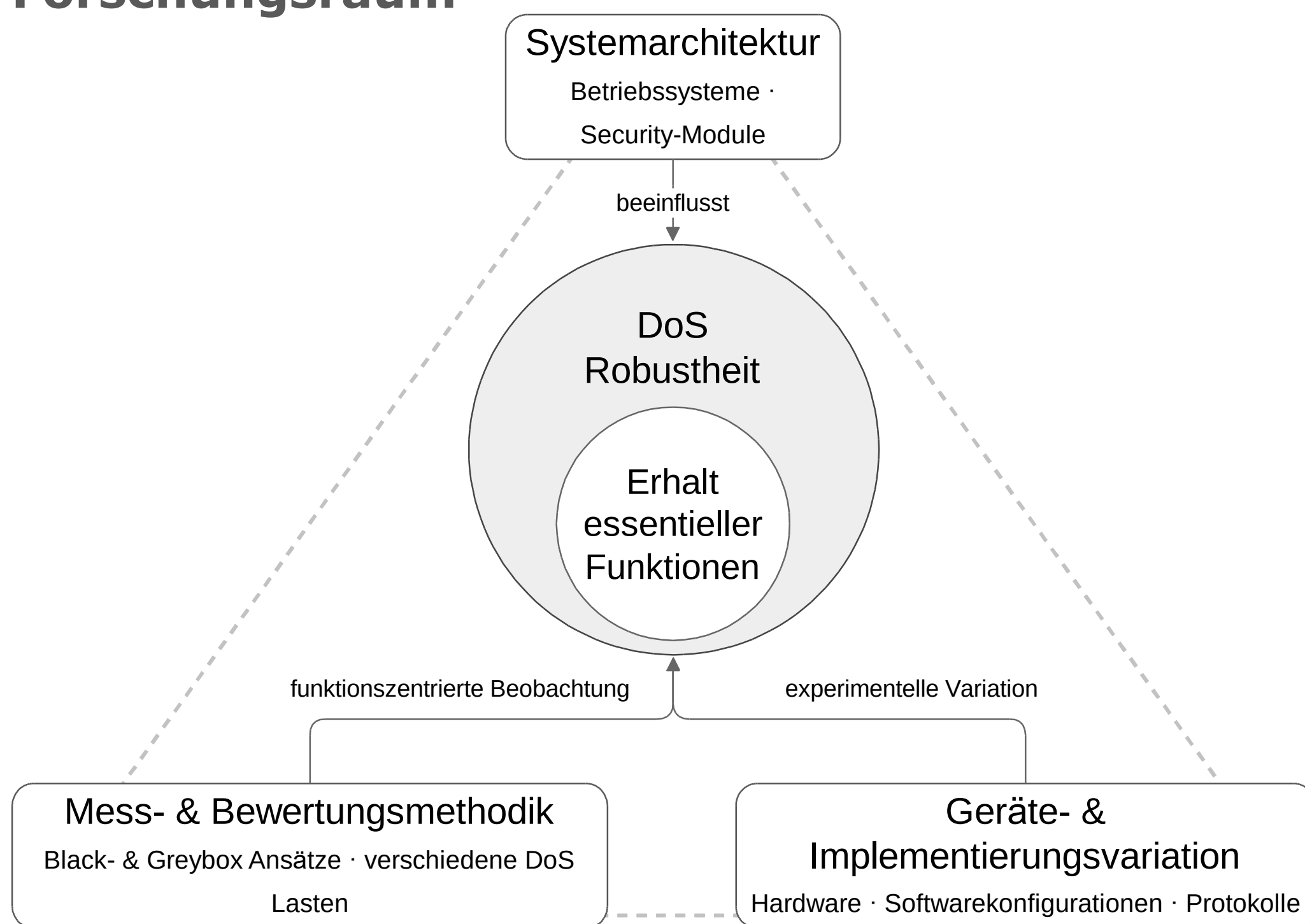
Florian Foerster

Institut für innovative Sicherheit, Technische Hochschule Augsburg
Projekt DS2CCP

Motivation

Denial-of-Service (DoS) Angriffe werden hauptsächlich mit Angriffszielen und Technologien aus der Internet-Domäne in Verbindung gebracht. Allerdings sind auch Embedded Geräte wie industrielle Steuerungen von DoS Angriffen beeinflussbar. Angriffe auf kritische Infrastruktur der Ukraine zeigen auf, dass dies reale Angriffe sind welche aktiv eingesetzt werden. Im Rahmen des Projektes DS2CCP ist es Ziel, bewährte Verfahren und Lösungen für Embedded Geräte aufzustellen um DoS Robustheit zu erhöhen

Forschungsraum



Experimentelle Ergebnisse

Filter-/Firewallwirkung ≠ Funktionserhalt

- Wirksamkeit von Filtermaßnahmen hängt von Angriffsebene, geschütztem Dienst, Filterstrategie und verfügbaren Geräte-Ressourcen ab.
- Reduktion des Angriffsverkehrs bedeutet nicht automatisch, dass relevante Gerätefunktion unter DoS erhalten bleibt.
- Schutzmaßnahmen anhand der zu erhaltenden Funktion bewerten.

Schutzmechanismen sind nicht kostenlos

- Security- und Isolationsmechanismen verändern den Verarbeitungspfad und verbrauchen selbst Ressourcen.
- Security-Funktionen gezielt isolieren & zusätzliche Wechsel zwischen Isolationsbereichen in häufig ausgeführten Verarbeitungspfaden vermeiden.

Schutzebene muss zu Engpass passen

- Schutz auf einer späteren Verarbeitungsebene kann einen früher entstehenden Ressourcenengpass nicht kompensieren.
- Gegenmaßnahmen dort ansetzen, wo kritische Ressource belastet wird, bei Bedarf mehrere Ebenen kombinieren

Gegenmaßnahmen für Embedded Geräte

Angriffsverkehr früh reduzieren

- Rate Limiting, Traffic Shaping und Priorisierung
- Netzwerkdienste, Ports und offene Verbindungen begrenzen
- Filterung früh im Verarbeitungspfad

Ressourcen begrenzen und essentielle Funktionen isolieren

- Parallele Verbindungen, offene Sockets und Warteschlangen begrenzen
- Netzwerkverarbeitung und Interrupt-Last von kritischen Aufgaben trennen

- Core-Pinning für kritische Prozesse
- Deterministisches Scheduling, Task-Isolation und Echtzeitmechanismen
- Ressourcen- und QoS-Begrenzung für Kommunikationspfade

Ressourcen begrenzen und essentielle Funktionen isolieren

- Kommunikationsfunktionen von anderen architektonisch trennen
- Rechenintensive Verarbeitung gezielt auslagern oder hardware-beschleunigen
- Security-Funktionen selektiv isolieren statt pauschal ein Maximum in geschützte Ausführungsumgebungen zu verschieben

Mehrwert für die Bundeswehr

Die Forschung bietet der Bundeswehr Mehrwert in mehreren Bereichen:

Robustheit missionskritischer Embedded Geräte Viele Geräte in Missionseinsätzen, wie zum Beispiel unbemannte Drohnen oder Kommunikationsgeräte, verwenden ähnliche Komponenten und Architekturen wie die untersuchten Embedded Geräte und profitieren ebenfalls von einer erhöhten Robustheit.

Robustheit kritischer Infrastruktur Eine erhöhte Robustheit von Geräten welche in kritischer Infrastruktur zur Anwendung kommen ist ebenfalls zum Vorteile der Sicherheit des deutschen Staates als auch die der Bundeswehr.

Wie Angriffe auf die ukrainische Energieinfrastruktur aufzeigen, kommen auch hier DoS Angriffe zum Einsatz. Sollte kritische Infrastruktur, welche beispielsweise für Truppenverlegung oder -versorgung verwendet wird, angegriffen werden, ist eine erhöhte Robustheit gegenüber DoS Angriffen auch hier von Vorteil.

Robustheit ziviler Embedded Endgeräte Es werden Embedded Geräte aus dem herkömmlichen Markt für IT-Zwecke in der Verwaltung wie Krankenhäusern herangezogen. Diese sind dadurch von zukünftigen Verbesserungen seitens DoS Robustheit positiv beeinflusst.



unibw.de



hsu-hh.de



dtecbw.de

gefördert durch



Zentrum für Digitalisierungs- und
Technologieforschung der Bundeswehr



Finanziert von der
Europäischen Union
NextGenerationEU