dtec.bw JAHRESTAGUNG 2025

ScienceForum – JT25

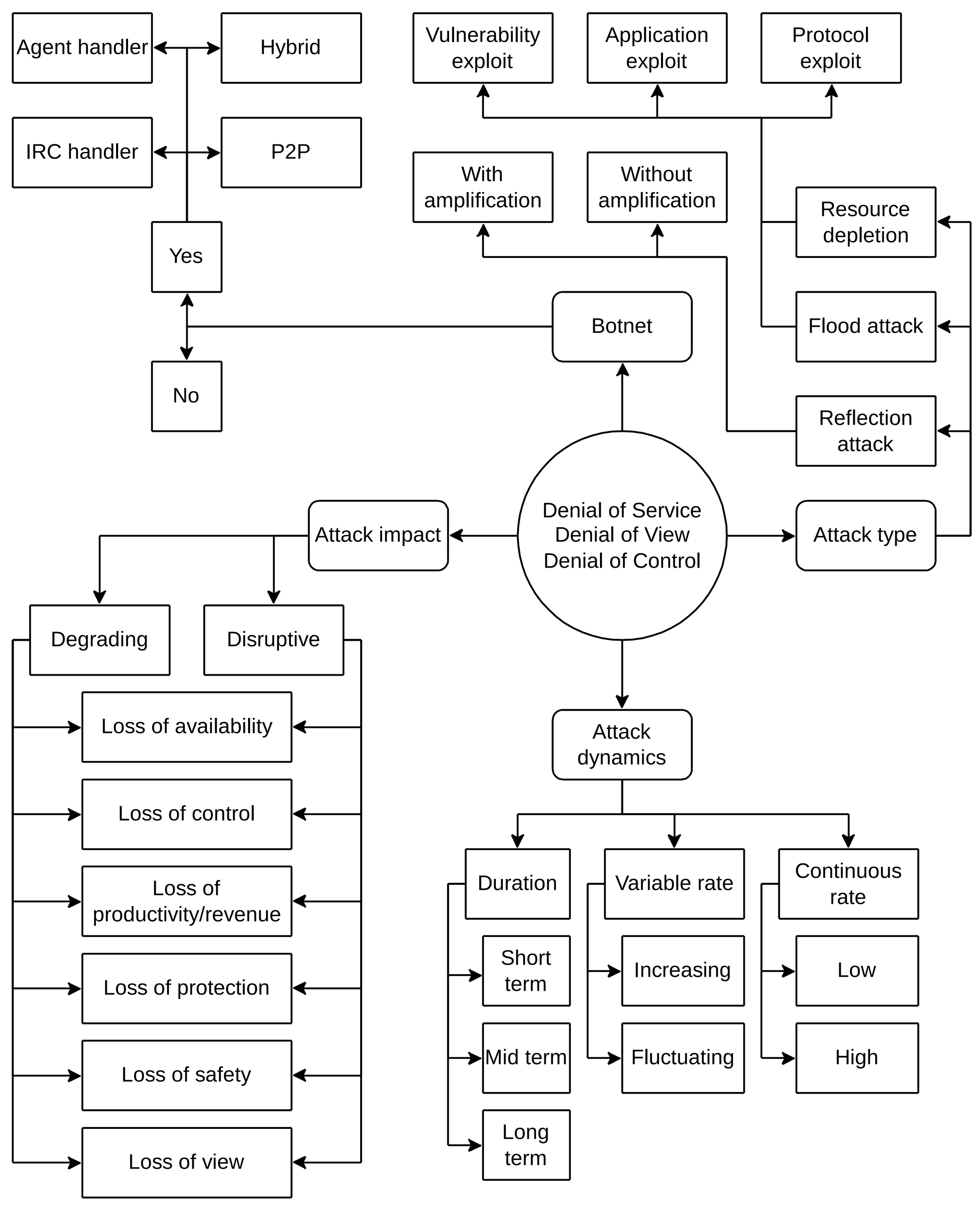
DoS Robustheit für Embedded Geräte und Essentielle Funktionen

F. Foerster[1], S.S. Ha[2], H. Beuster[2], G. Scholl[2], D. Merli[1]
[1]Institut für innovative Sicherheit, Technische Hochschule Augsburg, Augsburg
[2]Elektrische Messtechnik, Helmut-Schmidt-Universität, Hamburg

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 zum Beispiel industrielle Steuerungen von DoS Angriffen beeinflussbar [1]. Angriffe auf kritische Infrastruktur der Ukraine zeigen auf, dass dies reale Angriffe sind welche aktiv eingesetzt werden [2]. Derzeit gibt es keine auf Embedded Geräte bezogenen Best Practices um diese gegen DoS Angriffe möglichst robust zu entwerfen. Stattdessen werden hier Praktiken aus der Internet- und Netzwerkinfrastrukturdomäne herangezogen. Im Rahmen des Projektes DS2CCP ist es Ziel, bewährte Verfahren und Lösungen für Embedded Geräte aufzustellen um DoS Robustheit zu erhöhen.

Klassifikation von DoS Angriffen



Gegenmaßnahmen

Netzwerknahe Schutzmechanismen

- Auswahl robuster und performanter PHY-Komponenten mit integrierten Filterfunktionen
- Einsatz von Hardware-Offloading für die Verarbeitung gängiger Netzwerkprotokolle
- Verwendung geeigneter Netzwerktreiber mit Priorisierungs- und Filterfunktionen
- Implementierung grundsätzlicher Firewall-Regeln direkt auf dem Gerät, z. B. zur Paketlimitierung oder Portfilterung

System- und Kernelkonfiguration

- Optimierung von Netzwerkpuffern und Zeitlimits
- Begrenzung paralleler Verbindungen oder offener Sockets
- Aktivierung von Schutzmechanismen gegen typische Angriffsmuster wie beispielsweise SYN-Floods
- Core-Pinning zur Isolierung kritischer Prozesse
- Bindung von Interrupts und Netzwerkverarbeitung an dedizierte Kerne
- Nutzung von Hardwarebeschleunigern für kryptografische Protokollaufgaben

Geeignetes Echtzeitbetriebssystem

- Unterstützung deterministischer Task-Scheduler
- Möglichkeit zur Isolation kritischer Tasks gegen nicht-kritische Last
- Unterstützung von Netzwerk-Stacks mit QoS-Kontrolle und Ressourcenbegrenzung

Mehrwert für die Bundeswehr

Die Forschung bietet der Bundeswehr Mehrwert in mehreren Bereichen:
Robustheit ziviler Endgeräte Es werden viele 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.
Robustheit missionskritischer Embedded Geräte Viele Geräte in Missionseinsätzen, wie zum Beispiel unbemannte Drohnen oder Kommunikationsgeräte, fallen in die Kategorie von Embedded Geräten und profitieren 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 verwendet wird, angegriffen werden, ist eine erhöhte Robustheit gegenüber DoS Angriffen auch hier von Vorteil.

[1] Matthias Niedermaier et al., 2018. You snooze, you lose: measuring PLC cycle times under attacks. WOOT'18
[2] Win32/Industroyer, https://attack.mitre.org/software/S0604/ (visited on 08/05/2025)

unibw.de hsu-hh.de dtecbw.de

gefördert durch

dtec.bw Zentrum für Digitalisierungs- und Technologieforschung der Bundeswehr

Finanziert von der Europäischen Union NextGenerationEU