PRESSEMITTEILUNG

Für sofortige Veröffentlichung

Sicherheitslücken in Embedded-Systemen aufdecken: Emproof auf der Embedded World 2025

Emproof
Halle 4, Stand 4-139c
Embedded World 2025, Nürnberg
11.-13. März 2025

18. Februar 2025 – Emproof ist nächsten Monat auf der Embedded World vertreten, um auf die wachsende Bedrohung durch Reverse Engineering in Embedded-Systemen aufmerksam zu machen und Herstellern zu zeigen, wie sie ihre Geräte besser vor Exploits schützen können.

Viele OEMs setzen auf Verschlüsselung und Hardware-Sicherheitsmechanismen – doch Angreifer umgehen diese Maßnahmen zunehmend durch Software-Schwachstellen. Mit frei verfügbaren Tools wie Ghidra können Hacker kryptografische Schlüssel extrahieren, geistiges Eigentum stehlen und Firmware modifizieren – oft ohne tiefgehendes technisches Wissen. Angesichts dieser Bedrohungen verschärfen Regulierungsbehörden die Sicherheitsanforderungen für Embedded-Systeme.

Besucher der Halle 4, Stand 4-139c erfahren, wie sich Software-Sicherheit in Embedded-Systemen stärken und regulatorische Vorgaben einhalten lassen. Die Experten von Emproof demonstrieren, wie sich Firmware gegen Reverse Engineering, Code Injection und andere Bedrohungen absichern lässt – ohne Entwicklungsprozesse zu stören oder Zugriff auf den Quellcode zu erfordern.

Mit näher rückenden regulatorischen Fristen wie dem Cyber Resilience Act (CRA) rückt die Einhaltung von Sicherheitsstandards zunehmend in den Fokus. Unabhängige Tests von Cetome bestätigen, dass Emproof Nyx, eine binärbasierte Sicherheitslösung, Angriffsflächen reduziert und Sicherheitsvorfälle eindämmt – eine praxisnahe Lösung zur Erfüllung regulatorischer Anforderungen. Emproof Nyx unterstützt Architekturen wie RISC-V, ARM, Tri-Core und x86_64 und ermöglicht eine nahtlose Integration robuster Software-Sicherheit in bestehende Embedded-Designs.

Für alle, die ein tieferes Verständnis für die Risiken durch Reverse Engineering gewinnen möchten, hält Nils Albartus, Embedded Security Specialist bei Emproof, am 11. März um 12:00 Uhr einen Vortrag mit dem Titel *“Demystifying Reverse Engineering Attacks on Embedded Devices”* in der Safety & Security Session (Session 3.1). Er wird aufzeigen, wie Angreifer

Embedded-Software analysieren, welche Tools sie nutzen und mit welchen Strategien sich Unternehmen gegen diese Bedrohungen wappnen können.

<ENDE>

Bildunterschrift: Angreifer umgehen OEM-Schutzmaßnahmen durch Software-Schwachstellen

Über Emproof
Emproof wurde an der Ruhr-Universität Bochum gegründet, einer international führenden Universität und Forschungseinrichtung mit weltweitem Renommee für ihre innovativen Maßnahmen gegen Cyberangriffe. Die Gründer Marc Fyrbiak, Philipp Koppe und Tim Blazytko lernten sich dort während ihrer Forschung im Bereich IT-Sicherheit kennen. Die Sicherheitslösung Emproof Nyx bietet ein hohes Maß an Schutz und sichert die Integrität geistigen Eigentums in Embedded-Systemen. Sie nutzt einzigartige Technologien, um Algorithmen und Daten zu schützen und gleichzeitig das gesamte Gerät abzusichern. Emproof Nyx verhindert Reverse Engineering, schützt geistiges Eigentum und wehrt Exploitation-Angriffe ab. Die Lösung ist hardware- und softwareunabhängig und kann in jeder Phase des Produktlebenszyklus implementiert werden – wodurch Unternehmen Zeit, Kosten und Ressourcen sparen.

Bio Nils Albartus
Nils Albartus ist Embedded-Security-Spezialist bei Emproof und Doktorand am Max-Planck-Institut für Sicherheit und Privatsphäre in Bochum, Deutschland. Mit umfassender Expertise in Embedded Systems und einer Spezialisierung auf Reverse Engineering konzentriert er sich auf die Entwicklung robuster Schutzmaßnahmen gegen Reverse-Engineering-Techniken. Neben seiner technischen Arbeit engagiert sich Nils leidenschaftlich für die Weiterbildung von Fachkräften und Studierenden in effektiven Sicherheitspraktiken und trägt so zur Ausbildung der nächsten Generation von Sicherheitsexperten bei.

Weitere Informationen: Besuchen Sie www.emproof.com

Für redaktionelle Anfragen: Bitte senden Sie eine E-Mail an **melanie@kava-agency.com**