AYI NEDJIMI Consultants

Reverse Engineering Firmware IoT

2 mai 2026 • Mis à jour le 17 mai 2026 • 55 min de lecture • 12028 mots •

L'Internet des Objets représente aujourd'hui la surface d'attaque la plus so
milliards de dispositifs embarquent des systèmes d'exploitation complets,
et des interfaces réseau, le tout compilé pour des architectures.

L'Internet des Objets représente aujourd'hui la surface d'attaque la plus sous-esti
dispositifs embarquent des systèmes d'exploitation complets, des serveurs web, d
réseau, le tout compilé pour des architectures MIPS, ARM, PowerPC ou RISC-V pa
le time-to-market plutôt que la sécurité. Le *reverse engineering de firmware IoT* es
comprendre le code embarqué dans ces dispositifs afin d'identifier les vulnérabilit
malveillants. Cette démarche couvre l'extraction physique du firmware via des inte
JTAG, l'analyse automatisée avec Binwalk pour identifier les systèmes de fichiers
reverse engineering statique avec Ghidra, et l'émulation dynamique avec QEMU p
contrôlé sans le matériel physique. Les vulnérabilités découvertes via ces techniq
les parseurs réseau, absence de secure boot, backdoors de débogage laissées en
affectant des dizaines de millions de dispositifs dépl ure critique

Architecture des systèmes embarqués IoT

Avant d'aborder les techniques de reverse engineering, comprendre l'architecture
majorité des routeurs, caméras IP, thermostats connectés et équipements industri

Composants matériels typiques

Composant	Rôle	Exemples courants
SoC (System on Chip)	CPU + périphériques intégrés	Broadcom BCM63xx, Media Qualcomm IPQ
Flash NOR/NAND	Stockage du firmware	Winbond W25Q128, Macron
DRAM	Mémoire d'exécution	DDR3/DDR4 128MB-1GB
Port UART	Console série de débogage	3.3V TTL (pins TX, RX, GND
Interface JTAG	Debug hardware	20 pins standard, OpenOCD
Bus SPI	Communication flash	4 pins (MOSI, MISO, CLK, C

Réponse sous 24h

Devis gratuit →