The Internet of INSECURE Things

From Stuxnet to Mirai to whatever insecurity comes next, billions of Internet-connected devices are under threat from an evolving arsenal of hacks and attacks.

Why aren’t IoT devices more secure?
Too many embedded systems designers are more focused on shipping products than the security of the devices and their users. Nearly 22% say they don’t even have security on their to-do list. Many design best practices that raise security levels aren’t followed.

BUG TRACKING
Bug tracking is critical to ensure that problems don’t fall through the cracks.

54%
Don’t perform regular source code reviews for bugs and security holes

CODE REVIEWS
A second set of eyes on source code can identify many security weaknesses.

49%
Don’t use a static analysis tool to check the source code.

STATIC ANALYSIS
Inexpensive static analysis tools can be configured to identify “low-hanging fruit” problematic coding flaws.

STATISTICAL ANALYSIS
Don’t have a bug database or other system to track known issues

CODING STANDARDS
Observance of bug-killing coding rules can help keep bugs and security weaknesses out of products while also improving the readability of the source code.

33%
Don’t utilize a written coding standard, and others don’t enforce theirs consistently

ENCRIPTION
Encryption of data and commands sent over the Internet is an important layer of security for all systems.

MORE THAN 50%
Do not encrypt their data

Source: Barr Group 2018 Embedded Systems Safety & Security Survey. Copyright © 2018 Barr Group. All rights reserved. BARRGROUP.COM