Embedded Cyber-security & Vulnerabilities

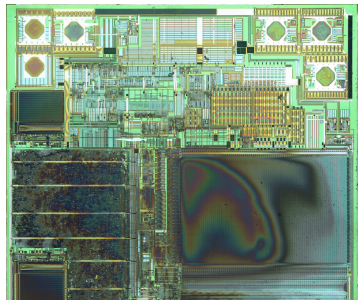
Daniel Casner

Sandia National Laboratories

2012 August 7th

Exceptional service in the national interest

Sandia National Laboratories



black hat®

U.S. DEPARTMENT OF ENERGY

NNSA National Nuclear Security Administration

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

UUR

Agenda

Sandia National Laboratories

- Overview
- Hacking techniques and defenses
  - Devices
  - External interfaces
  - Chips
- Examples
- Testing
- Best Practices
- Questions and more examples

Embedded Security Overview

Sandia National Laboratories

- Security vulnerabilities in embedded systems
  - Utilities – Stuxnet
  - Cars
  - Medical devices
  - Everything
- **Threat space** >> Solution space
- You can't bolt security on
  - Most "security" has been merely a roadblock
    - Security through obscurity isn't
  - Security (& reliability & correctness) must be part of the design process
  - **Constant vigilance**
- **Developers need to start thinking like hackers**

Embedded Systems Hacking

Sandia National Laboratories

- Information Gathering
  - Obtaining data about the target by any means necessary
- Hardware Teardown
  - Product disassembly, component/subsystem identification, modification
  - Attackers *will* have your hardware
- Firmware Reverse Engineering
  - Extract/modify/reprogram code or data
  - OS exploitation/device jailbreaking
- External Interface Analysis
  - Communications monitoring, protocol decoding/emulation
  - All ports lead to the Internet – see stuxnet
- Silicon Die Analysis
  - Chip-level modification/data extraction

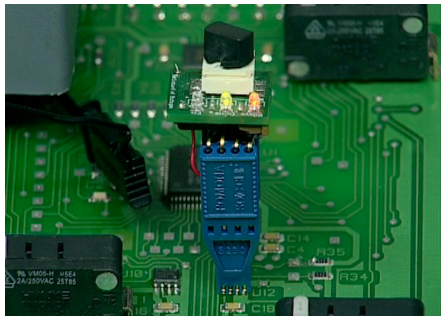
Based on slide © Grand Idea Studio

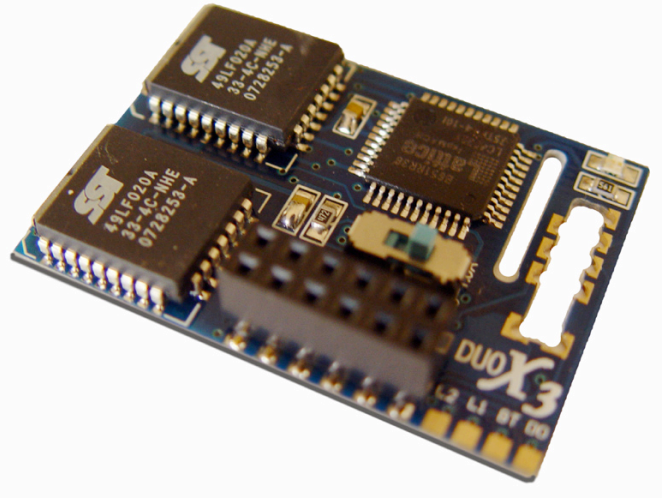
Embedded Systems Hacking

Sandia National Laboratories

- Common Attack surfaces
  - Memory & firmware – EEPROMs especially
  - Exposed buses & interfaces
  - Passwords & cryptography

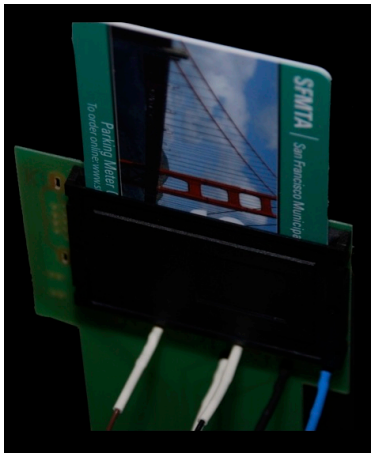
- Glitching Hardware
  - Clocks, power, memory, etc.
  - Try many, many times
  - Hacking the Xbox – Andrew Huang
- External Interfaces



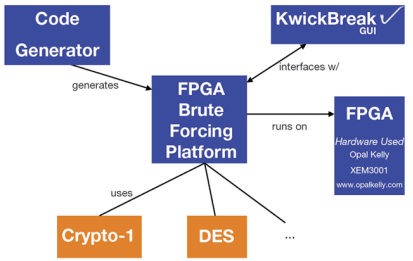


External Interface Hacking

- Man in the middle attacks
- Replay attacks
- Fuzzing – Sulley
- Gateways
- Sniffing and manipulating
  - Bitstir
  - GNU Radio
  - Breakout boards / boxes
  - Manufacturer dev kits
- FPGAs
  - Interfaces
  - Crypto breaking



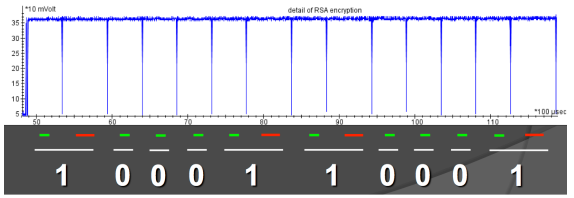
KwickBreak Brute Forcing Platform

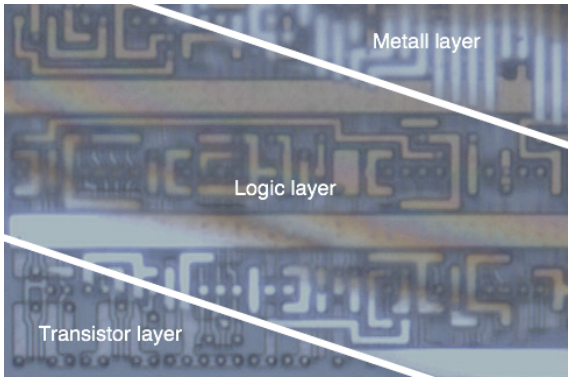


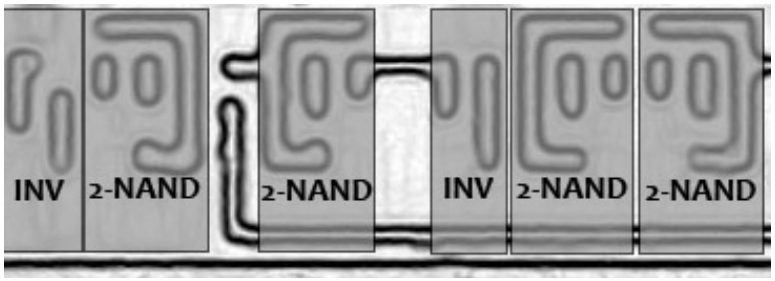
The KwickBreak FPGA brute forcing platform allows users to define crypto plugins and then execute known-plaintext attacks.

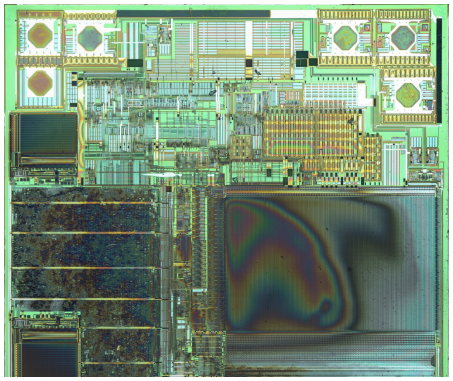
Chip Hacking

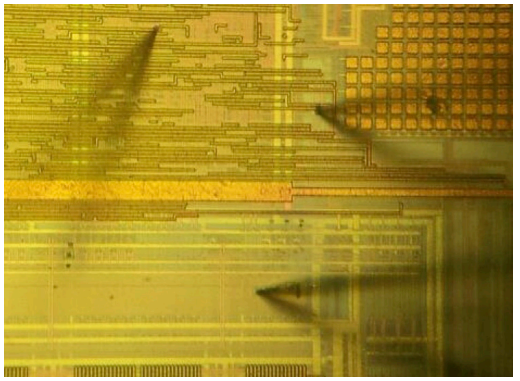
- Differential Power Analysis (DPA)
- Chip disassembly
  - Inspection
  - Probing
  - Optical Glitching
- Advanced tools in use today
  - FPGA based timers and glitchers
  - degate.org











Life-threatening Vulnerabilities

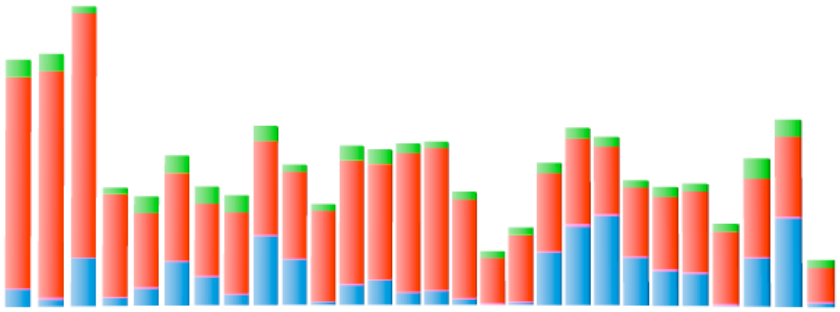
Sandia National Laboratories

Embedded medical device solutions

Sandia National Laboratories

- Acknowledgement and taking responsibility by manufacturers
  - End the knee-jerk reactions
  - Vulnerabilities to date have been negligent
  - Realize you are a target and start thinking like a hacker

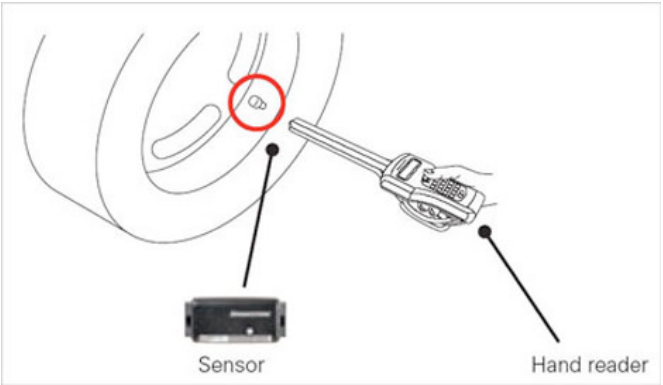
- Personal Area Network (PAN) monitoring firewall device
  - Statistical anomalous activity detection
  - Purdue University – Medmon



Vehicle Vulnerabilities

Sandia National Laboratories

- Network of Networks
- Gateways
- Attacks
  - Locks and ignition
    - side mirror CAN bus
    - RFID key duplication
  - Breaks through tire pressure monitor
    - Required by law
  - Entertainment system through MP3
    - Same vulnerability in Kindle



White Hat & Black Box

- Black box Testing
- Grey Box Testing
- White Box Testing

} Independent

} Internal

Security Testing

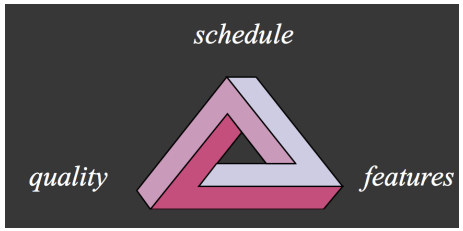
Sandia National Laboratories

- Continuous process: Testing leads to more tests
  - Learn about the system
  - Reverse Engineering
  - Testing provides unexpected results
  - Retesting once mitigations are implemented
- Test plan is updated
  - Adding tests
  - Changing risk ratings
- Measuring Success
  - Better understanding
  - Risk rating decrease
  - Fewer additional tests

Firmware Development Best Practices

Sandia National Laboratories

- **Correctness**: Quality *and* Security



- Jack Ganssle
  - Numerous books

- Firmware is the most expensive thing on earth
- No bug lists
- Version control
- Clean builds
- Test everything
- Coding standards
- Small teams
- Partitioning
- Fegan inspecitons
  - Software Inspection. *Tom Glib, Dorthy Graham. Addison Wesley.*

Questions (and/or more examples)

Sandia National Laboratories