Security Analysis of a Cryptographically-Enabled RFID Device

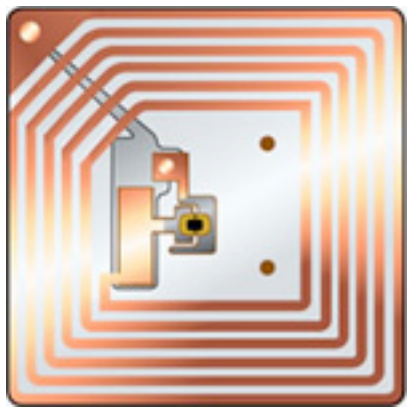
Authors: Stephen Bono, Matthew Green, Adam Stubblefield, Ari Juels, Aviel Rubin, Michael Szydlo
Published: 14th USENIX Security Symposium
Presenter: Gaelen Hadlett

Main Contributions

- Reverse engineered working details of widely used RFID cryptographic device
- Demonstrated exploit for quickly cracking DST keys and spoofing responses

RFID Basics

- Radio-Frequency Identification
- Small objects containing silicon chips and antennas
  - EEPROM for data
- Powered by incoming RF signal
  - Passive or active



Digital Signature Transponders

- Cryptographic functionality
  - Challenge-response protocol
- Unique key identifies device authenticity
- Complex algorithm increase power consumption
- Useful for electronic payments and entry

Related Work

- Reverse engineering
  - Purple cipher
  - RC4
- Key recovery techniques
  - Hellman time-space tradeoff
  - Deep Crack

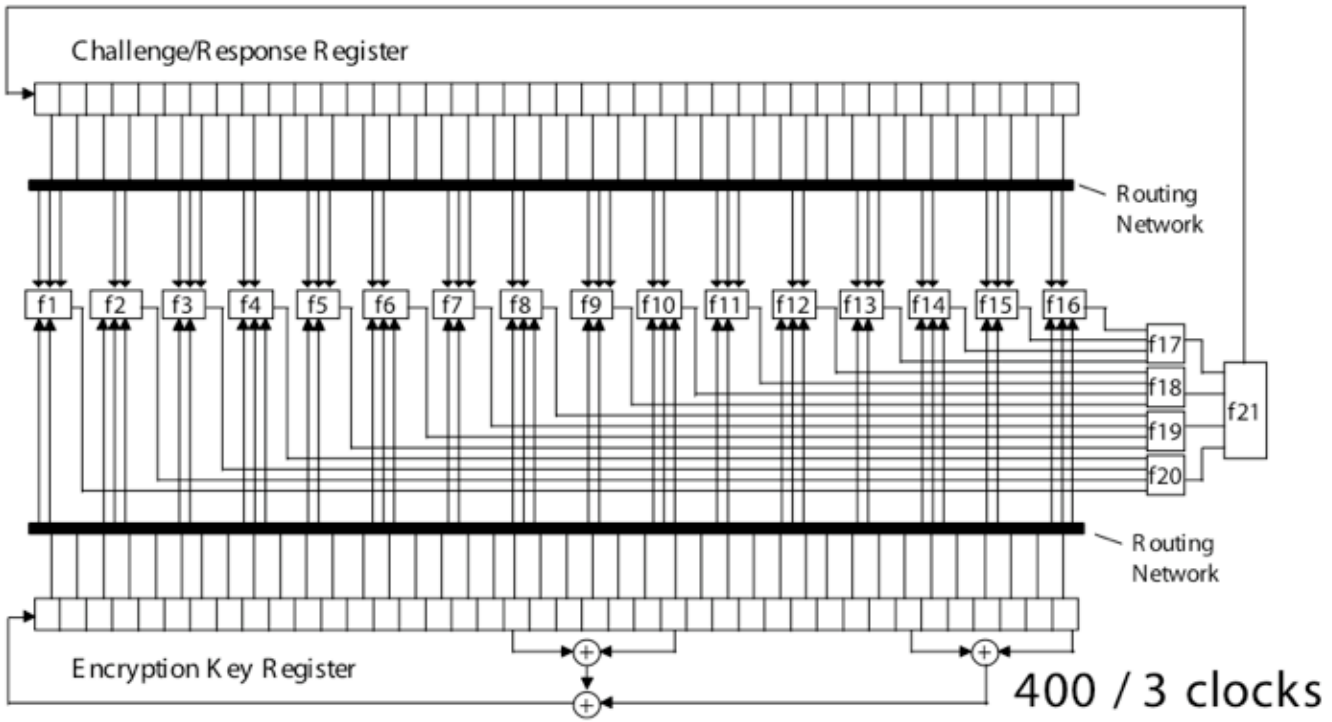
Research Progression

- Reverse engineer structure of DST
- Determine hidden key of DST
- Simulate challenge-response authentication

TI DST40 Overview

Digital Signature Transponder (3)

400 clocks ➔ 10 rounds



Digital Signature DST40 Algorithm implementation

Dr. Ulrich Kaiser Texas Instruments Deutschland GmbH

TI DST40 Overview

- Feedback shift register
  - Shifting and logical operation on input
- 40-bit key and challenge
- 24-bit response
- 200 cycles
- Three layers
  - 16 f-boxes
  - 4 g-boxes
  - 1 h-box

Reverse Engineering DST40

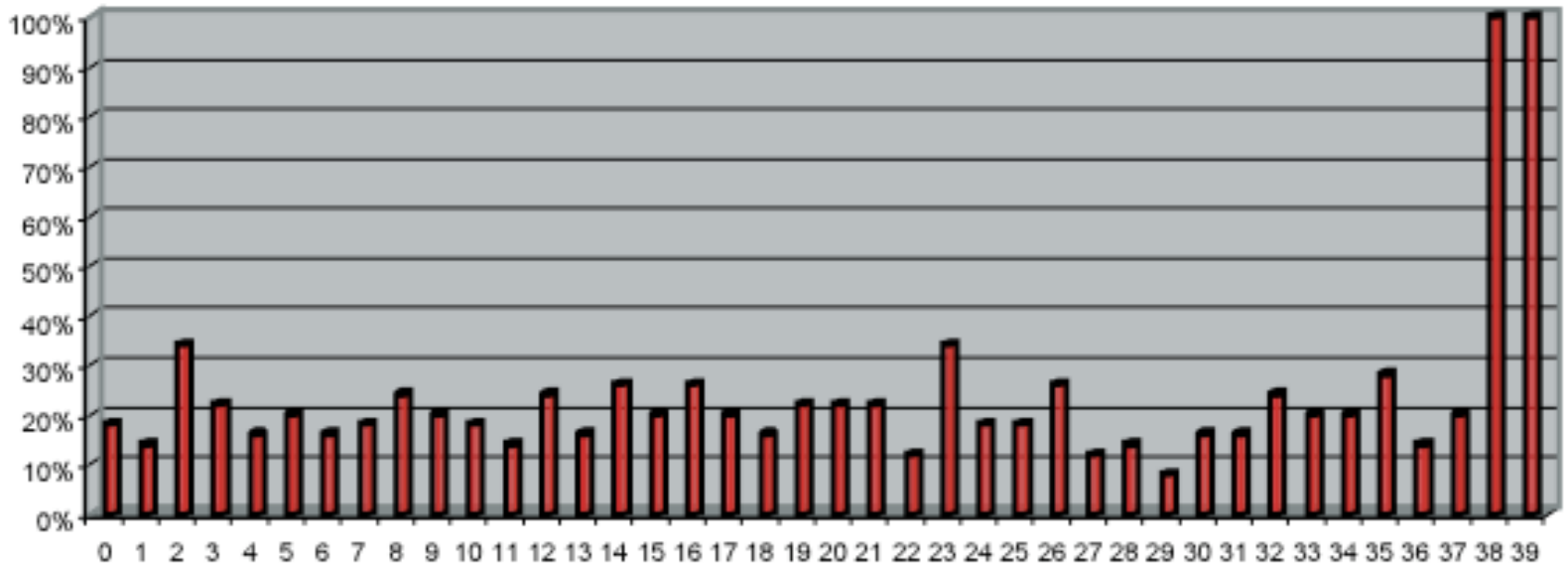
- Obtaining single-round output
  - Key string does not change across rounds
  - Challenge string results in small changes
- Use (C,R) pair to determine changes
  - DST40 works as an oracle
- Observe each round from oracle
  - h-boxes output two bits to rightmost challenge registers
  - Established 200 cycles

Reverse Engineering DST40

- All 0's limits knowledge
- Recover key schedule
  - Key updates every 3 cycles
  - Determined four XOR'ed bits
- Non-zero keys require more tests
  - Guess consecutive pairs correctly

Reverse Engineering DST40

- Uncover Feistel structure
  - Unbalanced Feistel



Uncover Bit Network

- Assume boxes output one value
- Test through observation
  - Fix all but two challenge or key bits
  - Determine where bits are routed
- Build tables of f, g, h-boxes outputs
  - Maps inputs to outputs

Cracking the Key

- Implemented in hardware with FPGA array
  - Low cost, faster than software
- Two challenge-responses required
  - Second one to verify
- Keyspace exhausted in 21 hours
  - Hellman time-space tradeoff decreases to 1 hr

Simulation

- Emulated DST challenge request
  - Send request from spoofed authenticator to real DST
- Emulated DST request response
  - Send response from spoofed DST to real authenticator

Significance of Research

- Off-line systems more vulnerable
- Attacks
  - Actively query transponders
    - short range
  - Passively eavesdrop
    - long range
- Fixes
  - Base on standard, public algorithms
  - Longer key length
  - Faraday shield

Strength

- Presented flaw in popular RFID device
- Clear without explaining full details
- Tested in real world environment

Weaknesses

- DST40 relatively weak to start
- Requires valid keys

Future Work

- Power analysis
  - Study power consumption of DST's
  - Patterns in power usage
- Adi Shamir (SHA-1)
  - Direction antenna and digital oscilloscope
    - Passive monitoring with cellphone
  - Biggest brands complete unprotected