ECEN 5053-002

Developing the Industrial Internet of Things

Dave Sluiter – Spring 2018

Presented by Don Matthews

Disclaimer

- All material and options presented by the author and speaker, Don Matthews, are expressly from the author and do not represent any opinions of any employer of the author.

Material

- What Algorithm/Protocols to use
- Anti-Tamper
- Threat Model
- Attacks
- Hard Drives
- Password Tables

Algorithm/Protocol to Use

- Always use a standard algorithm
  - Millions of combined hours of analysis
  - Secret is the KEY not the ALGORITHM
- Always use standard protocols
  - Same arguments
- Use proven code
  - Very hard to get it right with the multiple attack avenues
  - Open SSL is a good choice

Attacks

- eBeam
  - Read out storage elements
  - Read the key or other critical values
- Focused Ion Beam (FIB)
  - Make changes to a chip circuit
  - Bypass security bits
- Light leakage
  - Observed stored values based on emitted light

Attacks – Page 2

- Fault Injection
  - Power glitches, clock glitches, Low power, fast clocks
  - Force the chip to misbehave
    - Clock glitch when software checks an authentication value
  - Side Channel
    - Power usage (raw power, EM radiation)
    - Time

Attacks – Timing on RSA

- RSA: compute Y^X mod n
- Y, X, and n are 2, 3, or 4K bits in size (w)
- Series of Square operations and conditional multiply operations

- Let s0 – 1
- For k = 0 upto w-1
  - If (bit k of x) is 1 then
    - Let $R_k = (s_k * y) \bmod n$
  - Else
    - Let $R_k = s_k$
  - Let $s_{k+1} = R_k^2 \bmod n$
- End For
- Return (R_{w-1})

Attacks – RSA Timing Fixes

- Fix
  - Only use multiply ($A*A = A^2$)
  - Dummy multiplies
- Possible Issues
  - A*A has a different power profile than A*B
  - Compiler may remove the dummy operation

Attacks – Discussion Points

- Power/EM analysis
  - Don’t need all the bits can use analysis plus brute force
- Cache Attacks
  - Some implementations use tables

Threat Model

- What am I protecting
  - Information
  - Money
- What is the value and to who
  - Stored value card (gift card)
    - I add money, I'm rich
    - I posses the card
  - Credit Card Number
    - Usually doesn't cost me if stolen

Threat Model – Page 2

- What are the attack avenues
  - Who possesses it
    - Owner or User
  - Access
    - Fixed location or mobile
    - Visible location (people might observe someone tampering with it)
  - Internet enabled
  - Wireless

Attacks Again

- Let's go into some additional attacks
- Remember Dave's Electronic lock?
- What can go wrong with it?
- How do I go from 10K combinations to 24?

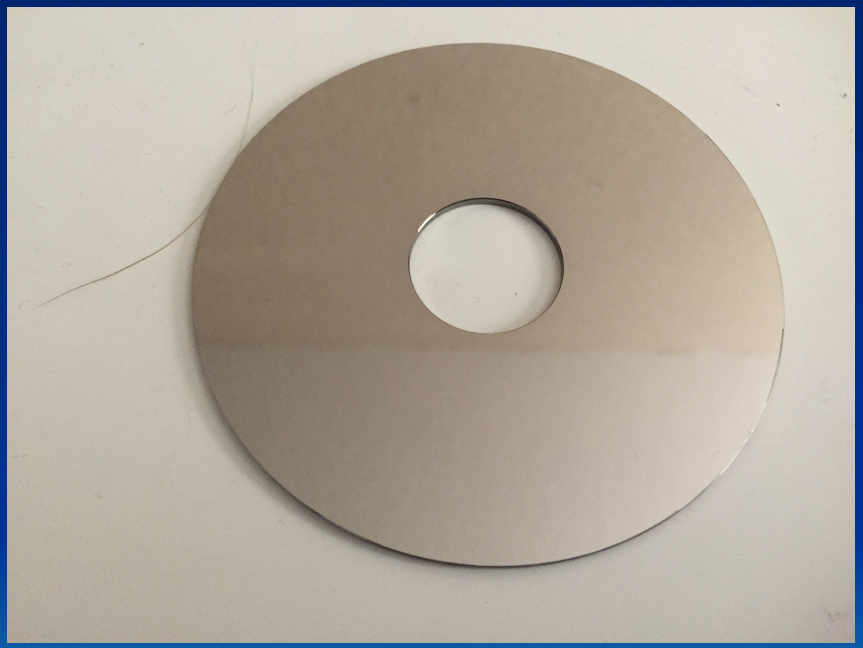
Push Button Lock

More Attack Discussion Points

- RFID chip (DefCon)
  - Attackers have time on their hands
- Key Fob
  - Man in the middle attack
- EEPROM
  - Reset the security bit
- USB encryption device
  - Do I need to know your key

Hard Drives

- Theory – It is hard to build a device to read platters removed from a Hard Drive
- Theory – Critical security data is stored on the platters where only WE can access them



Hard Drives – Pg 2

- Data Recovery companies build them and will recover data for you – Thousands of dollars
- Fortunately we don't need to do that, the drive companies have given us a tool to do that – The Hard Drive

Hard Drive – Pg 3

- Q: Who is WE in the theory that states only WE can access?
- A: Whoever controls the hard drive processor

- Attacks
  - Find bugs in the firmware
  - Write your own firmware
  - Make requests through a debug port

Password Table Attacks

- Dave discussed the use of hashing algorithms for password checking
- Can you spot a problem with this password table?

Username	Hashed PW
Joe	DyeCaEyfn
Lucy	jzeDhvue6
Xi	HeivC83Nd
Amit	C8Dnadevy
Anu	DyeCaEyfn

Password Table Attacks

- What Attacks Can I perform?
  - Hash many samples
    - Brute force
    - Dictionary
  - One hash operation compare to all users
- Counter measure
  - Increase the number of times I hash something
  - Make each user hash operation different