No MAS:
(misadventures in high security lock design)

Mike Davis
Introduction

• I Hack stuff for IOActive
  - Weird embedded stuff
• Amateur lock picker
  - I’m not very good
• Pretty good understanding of how the pixies flow
• I’m not interested in hacking one thing, I want to hack all of the things.
Todays plan

• We’re going to (try to) think like a lock vendor
• Quick look at the evolution of ”High Security” lock design
  - and a look at the seemingly pervasive flaw that these design requirements and decisions lead to.
• Look at how the same flaw keeps expressing itself.
• Discuss responsible cdisclosure a bit
Design Requirements!

• Lock
• Electronic
• Audit trail
• Long lived power solution
  - Replacing batteries isn’t really an option.
• Permissions systems not entirely related to physical possession of the key
• Drop-in replacement for the traditional mechanisms.
  - Mmm physical constraints…
• More secure-er then traditional (mechanical) designs!
  - Because… electronic!
Lock Design
Lock Design + Security
“As the CyberLock is directly powered through the communications port, it appears that an SPA (power analysis) attack may succeed against a CyberLock in-situ, as the lock leaks a significant power side-channel to any potential “key” as the processor slowly clocks the key across an I2C bus at the Fcpu/4 bps. However, this approach seems somewhat overboard given the existing issues.”

- IOActive Cyberlock Advisory
Cyberlock – power hungry
Some lessons learned

• Pluses
  - Drop in replacements for classical design
  - Locks don’t need batteries
  - Audit trails and permission systems

• Minuses
  - Bullshit crypto
  - Reliant on external power
  - Could not be fixed
A Quick Tangent
Yet Another Design

DEF CON 24 - Plore - Side channel attacks on high security electronic safe locks
DEFCONConference • 3.9K views • 2 years ago
Electronic locks are becoming increasingly common on consumer-grade safes, particularly those used to secure guns. This talk ...

EEVblog #762 - How Secure Are Electronic Safe Locks?
EEVblog • 675K views • 4 years ago
How secure are electronic locks used on safes? Dave tries a basic first attempt power line analysis attack on a standard La Gard...
Some lessons learned

• Pluses
  - Cheap
  - Battery failure doesn’t kill safe

• Minuses
  - Still reliant on external power
  - Introduction of secondary side-channels (beep)
Another quick Tangent
“So, here’s where the money is stored in an ATM, as you can see it’s protected with this heavy door; which in the old days criminals were trying to break into this, so by now they are more sophisticated” – Guy I owe a beer to.
No MAS:

Mike Davis

(misadventures in high security lock design)
"Encrypted"

The combinations, ATM, bank and master, are typically stored in encrypted form as an added security factor; the form of encryption is not critical. The preferred encryption is to distribute the bits of a binary representation of the combination in various locations of a memory and filling the unoccupied locations in the memory with random binary bits to disguise the combination. Decryption involves removal of the random binary bits and reassemblage of the remaining bits representing combination. Other encryption/decryption schemes may be used in lieu of the preferred scheme if desired.

- Patent US5488660A

- There is no cryptography used, there is just no room for it
- The Locks load their personality on every single boot before accepting combinations
- Every lock is identical with the exception of their EEPROM contents
- Each type of lock works a bit differently
What exactly is encrypted?
Soft I2C

![Graph showing Soft I2C data with CHAN1 and CHAN3+C channels.](image-url)
Hardware I2C
Pop!
“… but what about Gen2?”

“Gen2”

*gen2 is... interesting..
Done Right?

- Write advisory
- Do disclosure
- ...DEFCON
Fuuuuuuuu.

• Sometimes Kaba != Kaba
• We called the wrong Kaba, but they make locks too!
• From pictures of their locks found online they seem to share the same design pattern
• “I believe that you will find that the X-09 design different enough to be much more of a challenge. If you are experimenting on an X-10 lock, you have obtained the lock illegally and whoever from the U.S. provided / sold you the lock will be pursued by U.S. Federal agents.”
GSA-approved combination locks are only used by the US Government and its contractors for the protection of classified information. They are not used by any financial institution or the general public therefore; the practice of only notifying the manufacturer of discovered security issues is unacceptable due to the potential impact on the worldwide protection of US Government classified information. In addition, the publication of security information in this case would not serve the public interest; conversely it would put the National Security of the United States at great risk.

Again, if your company has information to report to the US Government regarding combination locks approved under Federal Specification FF-L-2740B please contact GSA, Mr.

Sincerely,

CC: GSA/IACSE Members
General Services Administration, Q1
Information Security Oversight Office, National Archives and Records Administration
National Counterintelligence and Security Center, Office of the Director of National Intelligence
Office of the Under Secretary of Defense for Intelligence
Central Intelligence Agency
Federal Bureau of Investigation
Department of State
National Security Agency
No MAS:
Mike Davis (misadventures in high security lock design)
WHY REDUNDANT DESIGN MATTERS..
No MAS:

Mike Davis

(misadventures in high security lock design)
But... What about the X-10?

X-10 features a Backlit LCD Display!
“Based on the information presented at the meeting, it does not look like it would be beneficial to spend any time looking at the X-10 model.”

- GSA
Questions?

Did I even leave time for questions?

MDavis@IOActive.com