Authenticated Exchanges

Nathan Jones

Mindstorms Engineering, LLC
Embedded Systems Design & Education

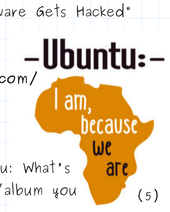
mindstormsengineering.github.io



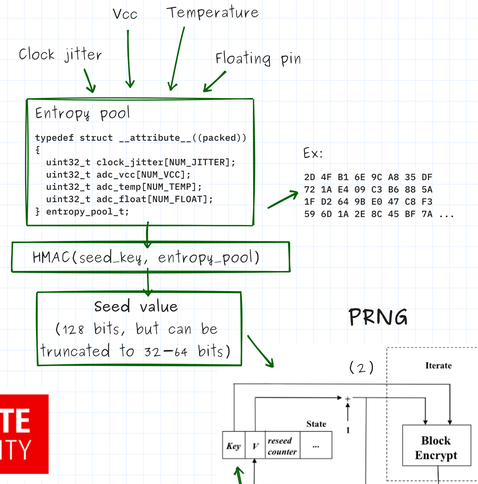
Teardown
- "Build Hackerbox #0040" (workshop)
- "Make Your Own MCU Boards"
- "Building a Simple CLI"
- "Retro Computing with the Hackaday Supercon badge" (workshop)
- "You Don't Need an RTOS"

EmbeddedRelated.com: "Simulate Your Embedded Project"
Hackaday Supercon: "Inside the Vojaë"
Embedded Online Conference: "Hardware (In)Security"
Maker.io (DigiKey): "How Hardware Gets Hacked"

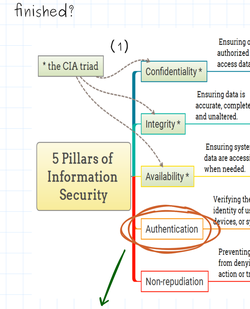
Step 1:
- Navigate to https://www.github.com/nathancharlesjones/authenticated_exchanges
- Ubuntu!
- Ask the person sitting next to you: What's the last good book/TV show/movie/album you finished?

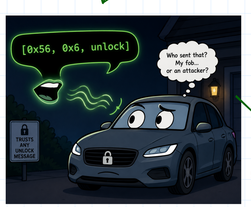


(5)



- Resistant to forgery
- Outputs appear random
- Also provides integrity
- Ex: HMAC, KMAC, CMAC





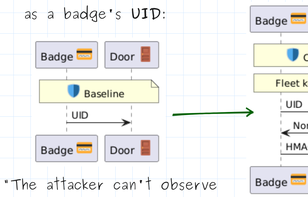


I didn't send that message!

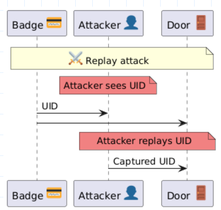
Yes, you did!

Authentication is established by providing a **secret** to the receiver that only *you* could possibly have known.

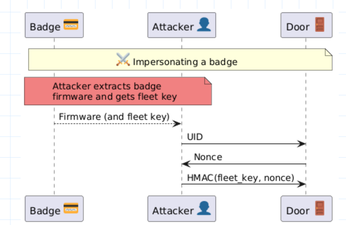
Brainstorm: What are some places in embedded where authentication matters?



"The attacker can't observe the conversation."

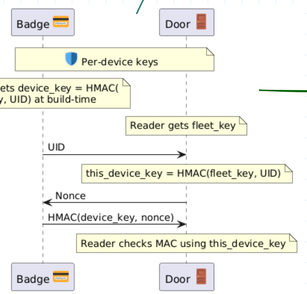


Could be from:
- observing an actual transmission,
- reading source code, etc

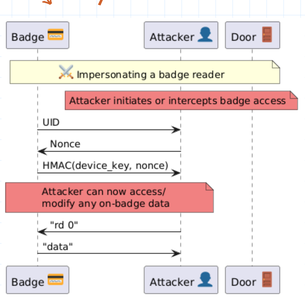


"The attacker can't access the badge binary."

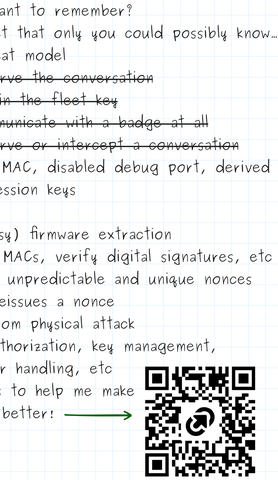
Could also acquire via:
- social engineering,
- leaked credentials in source control,
- table look-up, etc



"The attacker can't communicate with a badge."

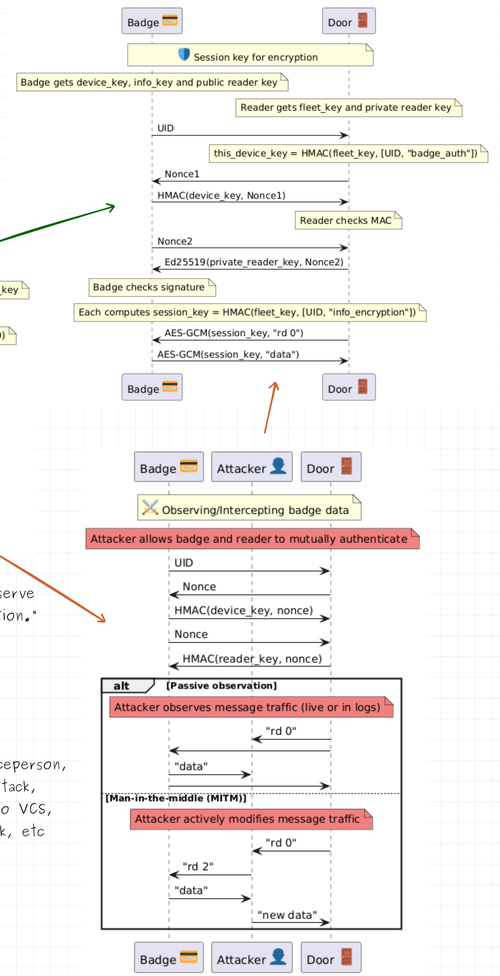


By:
- installing on reader,
- walking around with portable reader in pocket and "bump" into people with badges, etc



"The attacker can't observe or intercept a conversation."

From:
- malicious serviceperson,
- supply chain attack,
- logs leaked into VCS,
- relay attack, etc



Learning Objectives

1. Define "authentication" and its operating principle
2. Describe the function and purpose of the following in establishing authenticity:
   - MACs
   - key derivation algorithms
   - digital signatures
   - symmetric encryption
3. Identify vulnerabilities that threaten a system's authentication mechanism
4. Compute and use MACs, derived keys, digital signatures and symmetric encryption in Python to establish authenticity

Closing thoughts

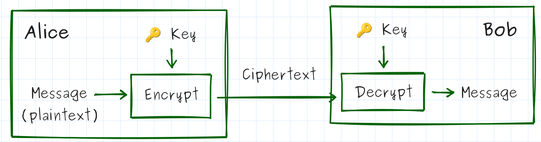
- What's one thing you want to remember?
- Authentication = a secret that only you could possibly know… in an ever-increasing threat model
  - ~~Attacker can't observe the conversation~~
  - ~~Attacker can't obtain the fleet key~~
  - ~~Attacker can't communicate with a badge at all~~
  - ~~Attacker can't observe or intercept a conversation~~
- "Key" (🔑) techniques: MAC, disabled debug port, derived keys, digital signatures, session keys
- "Key" (🔑) assumptions
  - Badge prevents (easy) firmware extraction
  - Badge can compute MACs, verify digital signatures, etc
  - Badge can generate unpredictable and unique nonces
  - The reader never reissues a nonce
  - Readers are safe from physical attack
- Other considerations: authorization, key management, resource constraints, error handling, etc
- Please spend 60 seconds to help me make my next workshop even better!

Key management

- How is the key being generated? What information is the manufacturer keeping?
  🏭 → 🔑 → 💳, 📕
  ↳ 🗐
- How is the key being stored on the device?
  → Flash? HSM?
  → Encrypted at rest?
- When and how is the key used on the device?
  → One key per use!
  → RAM scrubbed after use?
- How is a key updated/revoked? 🔑

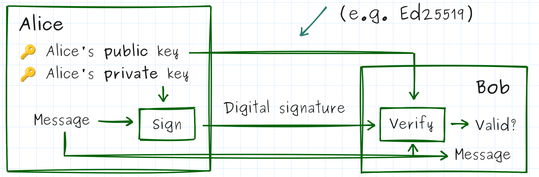
⚠️ For education only. Use only on systems you own or are authorized to test – not audited for production use.

Symmetric cryptography (e.g. AES)



Asymmetric cryptography

↳ Encryption, Key exchange, Digital signature (e.g. Ed25519)



(1) https://miro.medium.com/v2/1*tUBjDPi_foZIg7rQb8Flow.png
(2) https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-90Ar1.pdf
(3) https://www.researchgate.net/figure/General-architecture-diagram-for-TRNG-based-on-Ring-Oscillator_fig1_353965849
(4) https://www.fortinet.com/content/dam/fortinet/images/cyberglossary/http-vs-https.jpg
(5) https://cdn.creativefabrica.com/2020/05/07/1588834749/Ubuntu-I-am-because-we-are-580x386.jpg