Crypto Pitfalls

Or: Beware the MSDN sample code

Central PA Open Source Conference, 17-Oct-2015

Contrived Business Case

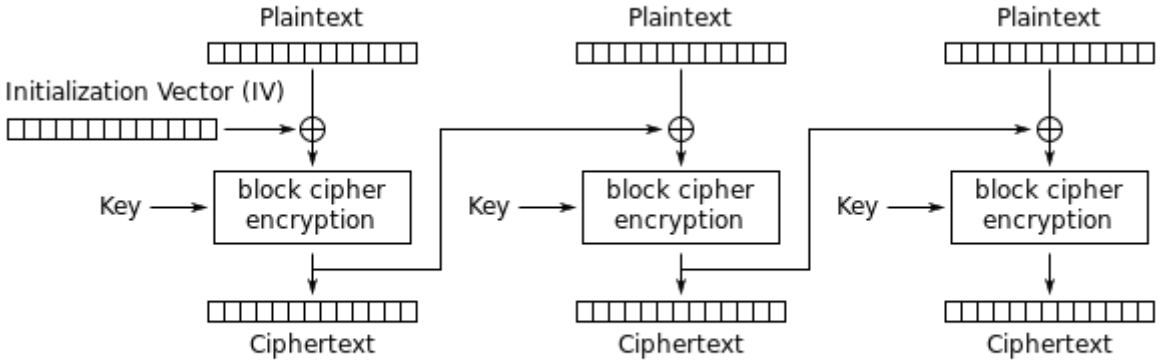
- Business partners exchange some transaction securely
  - Secrecy in transit
  - Verified origin
  - Not changed in transit
- Not using _____

A Common Solution

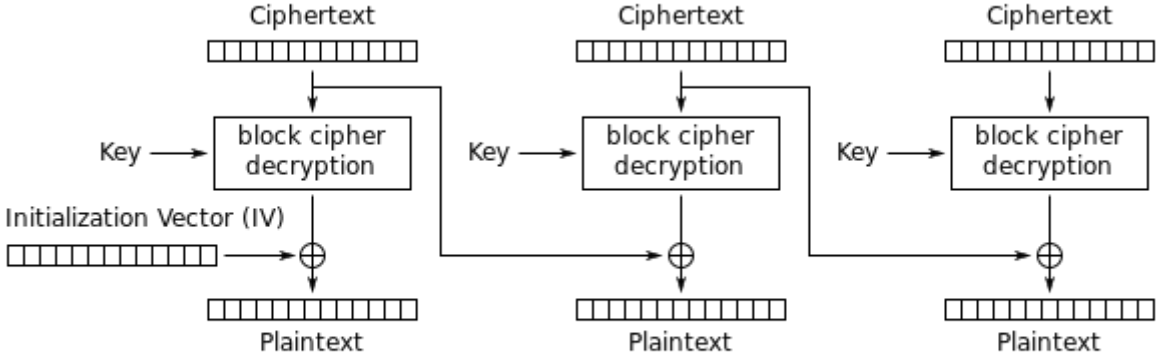
- Use AES encryption for both secrecy and integrity
  - AES is current standard
  - Won’t decrypt successfully without same encryption key both ends
- Copy some example AES code from MSDN or Stack Overflow

Let’s Code

Cipher Block Chaining (CBC) Mode



Cipher Block Chaining (CBC) mode encryption



Cipher Block Chaining (CBC) mode decryption

Source: http://en.wikipedia.org/wiki/Block_cipher_mode_of_operation

The Cryptographic Doom Principle

“If you have to perform *any* cryptographic operation before verifying the MAC on a message you’ve received, it will *somehow* inevitably lead to doom.”

- Moxie Marlinspike

http://www.thoughtcrime.org/blog/the-cryptographic-doom-principle/

Bonus Pitfall

non-constant time comparison of the MAC

What should we have done?

Encrypt-then-Authenticate

1. After generating the encrypted token (with IV), run HMAC on it (with separate key) and send the hash along
2. Before decrypting, verify the hash
3. Only once we're confident of the token's integrity should we begin to decrypt it

Note also AES-GCM

Lessons Learned

- Never use a static Initialization Vector
- Don’t expose error status codes over the public API
- Never use encryption without authentication e.g. HMAC
  - Do not use same key for authentication and encryption
- Use cryptography with extreme caution and extra code reviews
  - http://www.happybearsoftware.com/you-are-dangerously-bad-at-cryptography.html
- Use higher level-constructs whenever you can
  - JWT/JWE, OAuth2, SAML, etc

Further reference

- There are more elegant versions of padding oracle and CBC-R code in other languages, e.g.
  - http://www.limited-entropy.com/po_cbc-r_and_timing/
- Other explanations of this material:
  - CBC-R Paper - Juliano Rizzo & Thai Duong
    http://static.usenix.org/events/woot10/tech/full_papers/Rizzo.pdf
  - The Padding Oracle Attack – Why Crypto Is Terrifying
    http://robertheaton.com/2013/07/29/padding-oracle-attack/