Introduction

Friday, 9 March 2018
8:39 pm

Assessments
Quizzes - 2.5% total
Project - 25%

- Part 1: 9% – Due Week 7 (29th April)
- Part 2: 9% – Due Week 9 (13th May)
- Part 3: 7% – Due Week 12 (3rd June)

Assignment - 10% (Week 12/13)
Wargames - 12.5% (Week 13)
Exam - 50%

Lecture 1a

Sunday, 4 March 2018
10:25 pm

Risk matrix used to prioritize action against risk

	Extreme	High	Medium	Low	Negligible
Certain	1	1	2	3	4
Likely	1	2	3	4	5
Moderate	2	3	4	5	6
Unlikely	3	4	5	6	7
Rare	4	5	6	7	7

Axioms of security

- Information security is a resource game
- All systems have flaws
- The bigger the system, the more flaws
- Nothing works in isolation
- Humans are the weakest link
- It is easier to break a system, then to secure it

Definitions

Confidentiality	• Keep information secret, protecting information even when intercepted • Information is only confidential for a give time (cannot be confidential forever)
Integrity	• Detect whether information has been tampered with during transit
Authenticity	• Ensure we know who the sender is • Prove a message's origin

	• Prove the message is not a replay
Non-repudiation	• Allow someone to demonstrate to a judge that the message did come from some other • Sender cannot deny the message was sent

Availability	Guarantee the information can be accessible when needed
Covertness	Hide the fact that the message exists
Secrecy	Limit access to the information
Anonymity	To keep the message sender or receiver confidential

Passive attacks

- Do not modify or fabricate data
- For example, eavesdropping on network traffic

Active attacks

- Fabrication, attacks authenticity
- Interruption, attacks availability
- Modification, attacks integrity

Security through obscurity does not work

- Better to have more eyes on the code to pick out mistakes
  - E.g. Linux vs windows
- Kirchhoff's Principle
  - For a system to be secure, all secrecy must reside in the key

Lecture 1b Hashes

Friday, 9 March 2018
4:07 pm

The image of x is f(x)
The preimage of f(x) is x

One way function (OWF)
- It is easy to compute f(x) for all x
- Given f(x), it is computationally infeasible to find a preimage

Hash functions
- Compression
- Ease of computation

A hash function is **secure** if:
1. Preimage resistance
   - Given a hash value, it is hard to find the preimage
2. Second preimage resistance
   - Given some x, find x' which will hash to the same value
3. Collision resistance
   - It is hard to find ANY pair x and x' which hash to the same value

Note: #3 implies #2, since the inverse of #2 implies the inverse of #3.

One way hash function
- Satisfies #1 and #2

Collision resistant hash function
- Satisfies #3

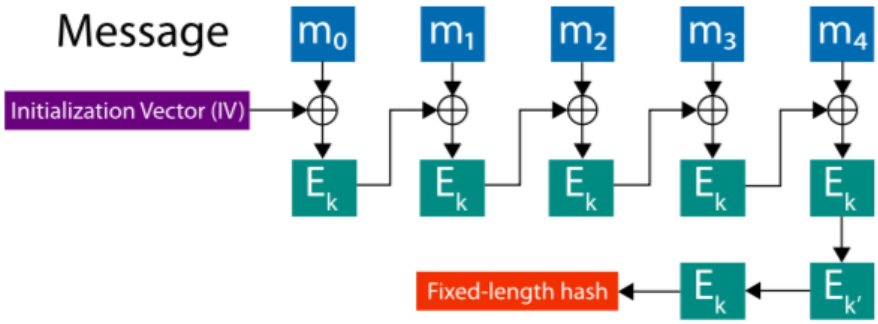
Attacks on hash functions
- Brute force (attack on preimage)
- Dictionary attack (attack on preimage)
- Birthday attack (attack on collision resistance)

Merkle-Damgard construction
- Message is divided into blocks
- Pad last block if it does not fill required bits

Keyed hash function
- Hash secret key and message pair
- Message authentication codes (MAC)
- For integrity, NOT secrecy

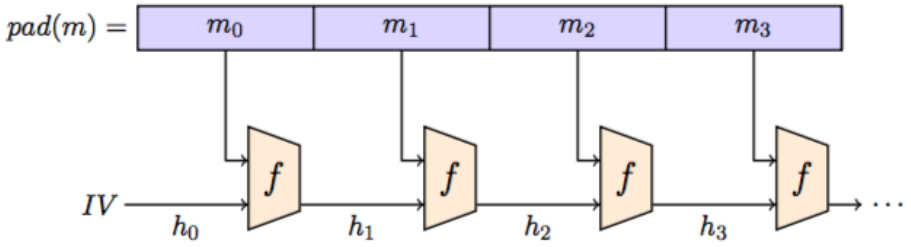
HMAC (Hash based message authentication code)

CBC-MAC (Cipher block chaining)
- Split message into blocks
- Blocks are XOR'ed together


Message
m0
m1
m2
m3
m4
Initialization Vector (IV)
Ek
Ek
Ek
Ek
Ek
Fixed-length hash
Ek
Ek'

Lab 1

Saturday, 10 March 2018
9:34 pm



NOTE:
A collision resistant hash function is still susceptible to the birthday attack.

- If your input space is larger than your output space, there will always be a collision
- Pigeonhole principle

Secret prefix method

1. Not possible to recover secret key because a secure hash function is preimage resistant
2. Take the existing hash (MAC) and the next block of the new message, and input it into the next iteration of Merkle-Damgard.
3. Computationally easy: O(1)

Secret suffix method

If you can compute another message with the same hash as h1, h2, h3 … you can swap out the original message for your own. This is a collision attack.

1. sqrt(2^n)
2. You can precompute a rainbow table of hashes offline.
3. MD5 is not collision resistant