



College of Information Studies

University of Maryland Hornbake Library Building College Park, MD 20742-4345

Access Control

Session 10

INST 346

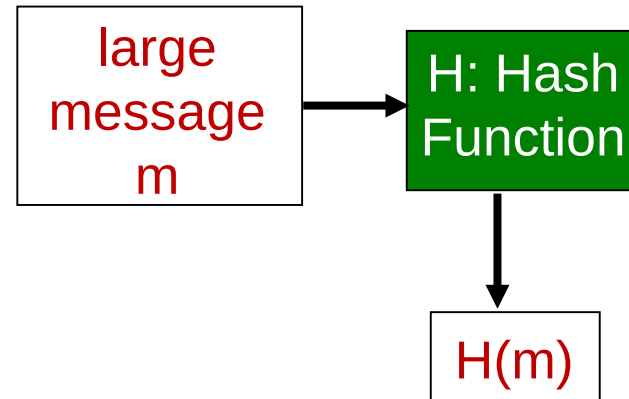
Agenda

- Hashing
- Access Control
- Usable Security

Message digests

goal: fixed-length, easy-to-compute digital “fingerprint”

- apply hash function H to m , get fixed size message digest, $H(m)$.



Hash function properties:

- many-to-1
- produces fixed-size msg digest (fingerprint)
- given message digest x , computationally infeasible to find m such that $x = H(m)$

TCP checksum: poor crypto hash function

Internet checksum has some properties of hash function:

- produces fixed length digest (16-bit sum) of message
- is many-to-one

But given message with given hash value, it is easy to find another message with same hash value:

<u>message</u>	<u>ASCII format</u>		<u>message</u>	<u>ASCII format</u>
I O U 1	49 4F 55 31		I O U <u>9</u>	49 4F 55 <u>39</u>
0 0 . 9	30 30 2E 39		0 0 . <u>1</u>	30 30 2E <u>31</u>
9 B O B	39 42 D2 42		9 B O B	39 42 D2 42
	<u>B2 C1 D2 AC</u>	different messages but identical checksums!		<u>B2 C1 D2 AC</u>

Widely used hash functions

- MD5 (RFC 1321) has known vulnerabilities
 - computes 128-bit message digest in 4-step process
- SHA-1 is widely used but is deprecated
 - US standard [NIST, FIPS PUB 180-1]
 - 160-bit message digest
 - Collision attack with 1000 GPUs in a month
- SHA-2 and SHA-3 are now available
 - Also standardized by NIST
 - More secure, but slower (in software)

Authentication

- First, say who you are
 - Userid, ID card, Nametag, ...
- Second, check to see if that's who you are
 - False positive: decide its you, when its not
 - False negative: decide its not you, when it is

Three-Factor Authentication

- What you know
- What you have
- What you are

Passwords

- Hard to guess
 - Not a word, date, userid, ...
 - Common approach: multiple types of characters
- Easy to remember
- Easy to set and reset
 - “Cognitive passwords”
- Rotated periodically
- Different on every system
- Not written or stored anywhere

Something You Have

- Phone (phone call, SMS)
- Email address
- Machine-readable ID card
- Authentication app
- One-time pad

Something About You

- Signature
- Fingerprint
- Face
- Voice
- Eye (iris, pupil)
- Typing (inter-keystroke timing)

Usable Security

- Usability and security are in tension
 - The most secure system allows nobody to use it!
- Goal: find the best balance
 - Required security based on anticipated threat
 - Required usability based on user abilities
 - Optimal tradeoffs within that design space

Getahead: Malware

Before You Go!

- On a sheet of paper (no names), answer the following question:

What was the muddiest point in today's class?