6.857 Hash fns

3/10/21

$$h : \{0,1\}^* \to \{0,1\}^d$$

$h(x)$ = hash value, message digest

ROM = gives "random" value for each input x

Properties: OW, CR, TCR, PR

(OW, CR: last time; TCR, PR: this time)

Applications:

- Password Storage
- File modification
- Digital Signature
- Commitments

~~

- Voting Equipment Security
- MD construction
- Merkle Trees

Properties: $H = \{h_s\}$ $h_s(x) = y$ $y \in \{0,1\}^d$

↖ seed

One-way: Given y in range of h
infeasible to find any x s.t. $h(x) = y$

Collision-Resistance: Infeasible to find x, x'
s.t. $h(x) = h(x')$

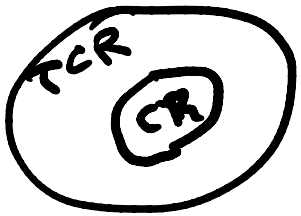
Target Collision Resistance:

Given x (random), infeasible to find $x' \neq x$
s.t. $h(x') = h(x)$

Given x compute $x' \in h^{-1}(x)$ ⇒ collision

$\neg TCR \Rightarrow \neg CR$

$CR \Rightarrow TCR$



Pseudo-random: infeasible to distinguish between
- box with RO
- " with h_s

Applications:

- Password storage
  User has password pw

Naive

Table: (U, pw)
↑ name ↖ password

Modified: Store (U, h(pw)) in table

Requires: OW

~~pw~~ (forbidden)

fails often in practice because pw's poorly chosen

⇒ exhaustive search works for Adv

$h_s(pw)$ often
↖ seed or salt
per system

$h_s(pw) = h(s \| pw)$
↖ SHA-256

$h_s(U \| pw)$

|| = concatenation operator

"ab" || "cd" = "abcd"

"ab" || "," || "cd"

- File modification detection

  store $(s, h_s(F))$ — s = seed, F = file

  securely (on thumb) — $h_s(F)$ ← target

  for each file F on disk
  recompute $h_s(F)$
  to see if it matches

  Requires! TCR: Adv wants to find F' s.t. $h_s(F') = h_s(F)$

- Digital Signatures:

  PK public key for signature verification

  SK

  signature on message: $SK(M)$ ← might belong too long!

  So: Signature as $SK(h_s(M))$ ← short!

Requires: CR

not find m, m' $h_s(m) = h_s(m')$

- Commitments: (Auction)

  bid m message

  send commitment $Com(m,r)$ to auctioneer

  open commitment by revealing m, r

Binding: $Com(m,r)$ binds me to revealing m later

Hiding: $Com(m,r)$ doesn't reveal m

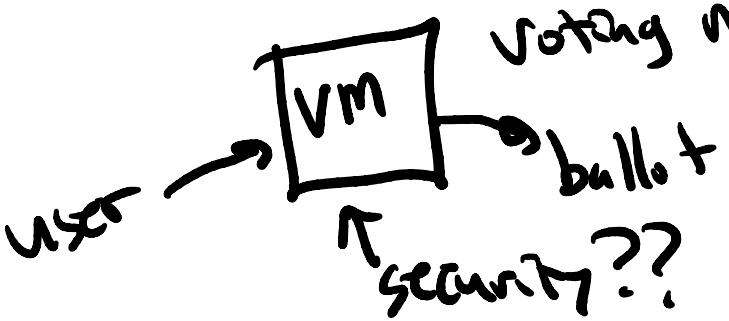
$$h_s(m||r) = Com(m,r)$$

$\neg$ Binding $\Rightarrow h_s(m||r) = h_s(m'||r')$ collision

$\neg$ Hiding $\Rightarrow$ $\underbrace{h_s(m||r)}_{Com(m||r)}$ reveals m, r $\overset{CR}{=\!=}$ $\overset{OW}{=\!=}$ ↯

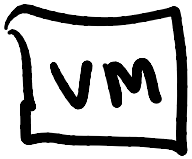
↑ OW on m

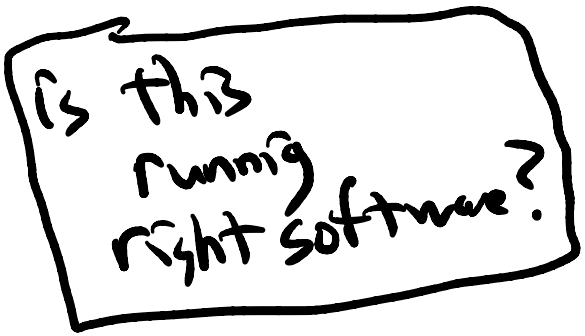
Voting Equipment Security



VM Certified
For particular software suite

Election:





Is this possible?
Can you check without running software on VM
hash(VM software) = h(certified software)
Is any part of VM trusted?
read VM memory from outside

① VM asked to check hash code!

② VM always says "yes, Ok!" (bug)

③ Doesn't check against certified software

checks $h(\text{VM software}) = h(\text{VM } 1^{st} \text{ software})$

Terrible!

④ Contract with vendor says acceptance testing must be done by vendor not E.O.! (Else voids warranty)

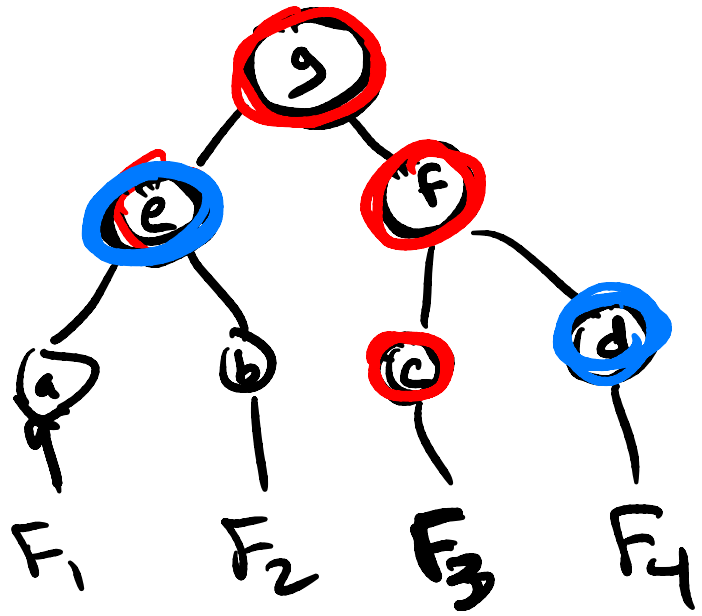
(∴ ⇒ Use paper ballots!)

Merkle Trees:

Goal: authenticate many files

$F_1, F_2, \ldots, F_{10^6}$

Build a tree to authenticate all, given hash(root)



~~Ext~~

$e = h(a \| b)$

$\Rightarrow g$ = hash value at root

F_3
c, d, e

Requires: CR