Announcements

HW6 Due April 23rd
HW7 Due April 30th
Previously on COS 433...
Digital Signatures
(aka public key MACs)
Message Integrity in Public Key Setting

Goal: If Eve changed $m$, Bob should reject
Digital Signatures

Algorithms:
• $\text{Gen}() \rightarrow (sk, pk)$
• $\text{Sign}(sk, m) \rightarrow \sigma$
• $\text{Ver}(pk, m, \sigma) \rightarrow 0/1$

Correctness:
$\Pr[\text{Ver}(pk, m, \text{Sign}(sk, m)) = 1: (sk, pk) \leftarrow \text{Gen()} ] = 1$
Security Notions?

Much the same as MACs, except adversary gets verification key
Today

The Public Key Infrastructure
Digital Signatures and the Public Key Infrastructure
Digital Signatures and the Public Key Infrastructure
Digital Signatures and the Public Key Infrastructure

$c' = \text{Enc}(pk', m)$
Digital Signatures and the Public Key Infrastructure

$c' = \text{Enc}(pk', m)$

$m = \text{Dec}(sk, c)$
Takeaway

Need some authenticated channel to ensure distribution of public keys

But how to authenticate channel in the first place without being able to distribute public keys?
Solution: Certificate Authorities

CA

Business
Government Agency
Department within company

sk_{CA}

pk_{CA}
Solution: Certificate Authorities

\[ \text{Cert}_{CA \rightarrow B} = \text{Sign}(sk_{CA}, \text{"Bob's public key is } pk_B\text{"}) \]
Solution: Certificate Authorities

Bob is typically some website
• Obtains **Cert** by, say, sending someone in person to CA with \( \text{pk}_B \)
• Only needs to be done once

If Alice trusts CA, then Alice will be convinced that \( \text{pk}_B \) belongs to Bob

Alice typically gets \( \text{pk}_{CA} \) bundled in browser
Limitations

Everyone must trust same CA
  • May have different standards for issuing certs

Single point of failure: if $sk_{CA}$ is compromised, whole system is compromised

Single CA must handle all verification
Multiple CAs

There are actually many CA’s, $\text{CA}_1, \text{CA}_2,...$

Bob obtains cert from all of them, sends all the certs with his public key

As long as Alice trusts one of the CA’s, she will be convinced about Bob’s public key
Certificate Chaining

CA issues $\text{Cert}_{\text{CA} \rightarrow \text{B}}$ for Bob

Bob can now use his signing key to issue $\text{Cert}_{\text{B} \rightarrow \text{D}}$ to Donald

Donald can now prove his public key by sending $(\text{Cert}_{\text{CA} \rightarrow \text{B}}, \text{Cert}_{\text{B} \rightarrow \text{D}})$

• Proves that CA authenticated Bob, and Bob authenticated Donald
Certificate Chaining

For Bob to issue his own certificates, a standard cert should be insufficient

• CA knows who Bob is, but does not trust him to issue certs on its behalf

Therefore, Bob should have a stronger cert:

$$\text{Cert}_{CA\rightarrow B} = \text{Sign}(\text{sk}_{CA}, \text{“Bob’s public key is } p_{kB} \text{ and he can issue certificates on behalf of CA”})$$
Certificate Chaining

One root CA

Many second level CAs $CA_1$, $CA_2$, ...
• Each has $\text{cert}_{CA \rightarrow CA_i}$

Advantage: eases burden on root

Disadvantage: now multiple points of failure
Invalidating Certificates

Sometimes, need to invalidate certificates
• Private key stolen
• User leaves company
• Etc

Options:
• Expiration
• Explicit revocation
Identification Protocols
Identification
Identification
Identification

To identify yourself, you need something the adversary doesn’t have

Typical factors:
• What you are: biometrics (fingerprints, iris scans,...)
• What you have: Smart cards, SIM cards, etc
• What you know: Passwords, PINs, secret keys
Types of Identification Protocols

Secret key:

Public Key:
Types of Attacks

Direct Attack:
Types of Attacks

Eavesdropping/passive:

\[ \text{sk} \quad \leftrightarrow \quad \text{vk} \]
Types of Attacks

Eavesdropping/passive:

- sk
- vk
Types of Attacks

Man-in-the-Middle/Active:

[Diagram with characters and arrows indicating communication flow]
Types of Attacks

Man-in-the-Middle/Active:

\[ \text{sk} \rightarrow \text{vk} \]
Basic Password Protocol

Never ever (ever ever...) use

\[ \text{sk} = \text{pwd} \]
\[ \text{vk} = \text{pwd} \]

\[ \text{sk} = \text{vk} ? \]
Problem with Basic Pwd Protocol

\textbf{vk} must be kept secret at all costs

Issue:

<table>
<thead>
<tr>
<th>User</th>
<th>Pwd</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alice</td>
<td>(pwd_A)</td>
</tr>
<tr>
<td>Bob</td>
<td>(pwd_B)</td>
</tr>
<tr>
<td>Charlie</td>
<td>(pwd_C)</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
</tr>
</tbody>
</table>
Problem with Basic Pwd Protocol

vk must be kept secret at all costs

Issue:
Slightly Better Version

STILL never ever (ever ever...) use

Let $H$ be a hash function

Let $sk = pwd$

$vk = H(pwd)$

$H(sk) == vk$?
Slightly Better Version

STILL never ever (ever ever...) use

Let $H$ be a hash function
Slightly Better Version
STILL never ever (ever ever...) use

Advantage of hashing:
• Now if pwd database is leaks, adversary only gets hashes passwords

• For identification protocol, need actual password

• Therefore, adversary needs to invert hash function to break protocol

• Presumed hard
Weak Passwords

Data from 10M passwords leaked in 2016:

<table>
<thead>
<tr>
<th>RANK</th>
<th>PASSWORD</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>123456</td>
</tr>
<tr>
<td>2.</td>
<td>123456789</td>
</tr>
<tr>
<td>3.</td>
<td>qwerty</td>
</tr>
<tr>
<td>4.</td>
<td>12345678</td>
</tr>
<tr>
<td>5.</td>
<td>111111</td>
</tr>
<tr>
<td>6.</td>
<td>1234567890</td>
</tr>
<tr>
<td>7.</td>
<td>123456</td>
</tr>
<tr>
<td>8.</td>
<td>password</td>
</tr>
<tr>
<td>9.</td>
<td>123123</td>
</tr>
<tr>
<td>10.</td>
<td>987654321</td>
</tr>
<tr>
<td>11.</td>
<td>qwertyuiop</td>
</tr>
<tr>
<td>12.</td>
<td>mynoob</td>
</tr>
<tr>
<td>13.</td>
<td>123321</td>
</tr>
<tr>
<td>14.</td>
<td>666666</td>
</tr>
<tr>
<td>15.</td>
<td>18atcskd2w</td>
</tr>
<tr>
<td>16.</td>
<td>7777777</td>
</tr>
<tr>
<td>17.</td>
<td>1q2w3e4r</td>
</tr>
<tr>
<td>18.</td>
<td>654321</td>
</tr>
<tr>
<td>19.</td>
<td>555555</td>
</tr>
<tr>
<td>20.</td>
<td>3rjs1la7qe</td>
</tr>
<tr>
<td>21.</td>
<td>google</td>
</tr>
<tr>
<td>22.</td>
<td>1q2w3e4r5t</td>
</tr>
<tr>
<td>23.</td>
<td>123qwe</td>
</tr>
<tr>
<td>24.</td>
<td>zxcvbnm</td>
</tr>
<tr>
<td>25.</td>
<td>1q2w3e</td>
</tr>
</tbody>
</table>

50% of available passwords

https://blog.keepersecurity.com/2017/01/13/most-common-passwords-of-2016-research-study/
Weak Passwords

Of course, pwds that have been leaked are likely the particularly common ones

Even so, 360M pwds covers about 25% of all users
Online Dictionary Attacks

Suppose attacker gets list of usernames

Attacker tries logging in to each with `pwd = ‘123456’`

5-17% of accounts will be compromised
Online Dictionary Attacks

How to slow down attacker?
• Lock out after several unsuccessful attempts
  • Honest users may get locked out too

• Slow down response after each unsuccessful attempt
  • 1s after 1\textsuperscript{st}, 2s after 2\textsuperscript{nd}, 4s after 3\textsuperscript{rd}, etc
Offline Dictionary Attacks

Suppose attacker gets hashed password $vk = H(pwd)$

Attack:
• Assemble dictionary of 360M common passwords
• Hash each, and check if you get $vk$
• If so, you have just found $pwd$!

On modern hardware, takes a few seconds to recover a passwords 25% of the time
Offline Dictionary Attacks

Now consider what happens when adversary gets entire hashed password database
• Hash dictionary once: $O(|D|)$
• Index dictionary by hashes
• Lookup each database entry in dictionary: $O(|L|)$

To get 25% of passwords takes $O(|D|+|L|)$ time
• Amortize cost of hashing dictionary over many passwords
Salting

Let $H$ be a hash function

$s_i$ random

<table>
<thead>
<tr>
<th>User</th>
<th>Salt</th>
<th>Pwd</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alice</td>
<td>$s_A$</td>
<td>$H(s_A, pwd_A)$</td>
</tr>
<tr>
<td>Bob</td>
<td>$s_B$</td>
<td>$H(s_B, pwd_B)$</td>
</tr>
<tr>
<td>Charlie</td>
<td>$s_C$</td>
<td>$H(s_C, pwd_C)$</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
<td>...</td>
</tr>
</tbody>
</table>
Salting

Salt length? Enough to make each user’s salt unique
• At least 64 bits

Salting kills amortization:
• To recover Alice’s key, adversary must hash entire dictionary with $s_A$
• To recover Bob’s key, adversary must hash entire dictionary with $s_B$
• Must hash entire dictionary again for each user

Running time: $O(|D| \times |L|)$
Unique Passwords

Different websites may employ different standards for password security
• Some may store passwords in clear, some may hash without salt, some may salt

If you use the same password at a bank (high security) and your high school reunion (low security), could end up with your password stolen
Unique Passwords

Solutions:
• Password managers

• Salt master password to generate website-specific password (e.g. pwdhash):

  Master password: \texttt{pwd}
  Pwd for abcdefg.com: $H(\text{abcdefg.com, pwd})$
My Personal Favorite

Stanford PwdHash

PwdHash generates theft-resistant passwords. The PwdHash browser extension invisibly generates these passwords when it is installed in your browser. You can activate this protection by pressing F2 before you type your password, or by choosing passwords that start with `!!`. If you don't want to install PwdHash on your computer, you can generate the passwords right here.

- Visit the Stanford project website.
- Install PwdHash for Firefox. It has been ported to Chrome and Opera.
- Read the USENIX Security Symposium 2005 paper (PDF).

This site and plugin are no longer under active development and the code is available for use. See individual files for license details.
What Hash Function to Use

In LinkedIn leak (using Sha1), 90% of passwords were recovered within a week

Problem: Sha1 is very fast!

To make hashing harder, want hash function that is just slow enough to be unnoticeable to user
What Hash Function to Use

Examples: PBKDF2, bcrypt

• Iterate hash function many times:
  \[ H'(x) = H(H(H(....H(x)....))) \]

• Set #iterations to get desired hashing time

Still problem:

• Adversary may have special purpose hardware
  \[ \Rightarrow \text{Can eval much faster than you can (50,000x)} \]
What Hash Function to Use

Memory-hard functions: functions that require a lot of memory to compute

• As far as we know, no special purpose memory
• Attacker doesn’t gain advantage using special purpose hardware

Examples: Scrypt, Argon2i
Encrypt Passwords?

<table>
<thead>
<tr>
<th>User</th>
<th>Pwd</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alice</td>
<td>Enc(k,pwd_A)</td>
</tr>
<tr>
<td>Bob</td>
<td>Enc(k,pwd_B)</td>
</tr>
<tr>
<td>Charlie</td>
<td>Enc(k,pwd_C)</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
</tr>
</tbody>
</table>
Encrypt Passwords?

Again, never ever (ever ever....) use
• To check password, need to decrypt
• Must store decryption key $k$ somewhere
• What if $k$ is stolen?

Need to use one-way mechanism
• With hash function, not even server can recover password
Security Against Eavesdropping

\[ \text{sk} = \text{pwd} \]

\[ \text{vk} = H(s_A, \text{pwd}) \]

\[ H(s_A, \text{sk}) = \text{vk}? \]
Security Against Eavesdropping

One solution: update $sk, vk$ after every run
One-time Passwords

Let $F$ be a PRF

$sk = (k, 0)$

$vk = (k, 0)$

$s_{k_0} = F(k, 0)$

$s_{k_0} = F(k, 0)$?
One-time Passwords

Let $F$ be a PRF

$$sk_1 = F(k,1)$$

$$sk = (k,1)$$

$$vk = (k,1)$$

$$sk_1 \equiv F(k,1)?$$
One-time Passwords

Let $F$ be a PRF

$s_{k_0} = F(k,0)$

$s_{k} = (k,0)$

$v_{k} = (k,0)$
One-time Passwords

Let $F$ be a PRF

$sk = (k, 1)$

$sk_0 = F(k, 0)$

$v_k = (k, 1)$
One-time Passwords

Advancing state:
- Time based (e.g. every minute, day, etc)
- User Action (button press)

Must allow for small variation in counter value
- Clocks may be off, user may accidentally press button
Stateless Schemes?

So far, all schemes secure against eavesdropping are stateful

Easy theorem: any one-message stateless ID protocol is insecure if the adversary can eavesdrop

• Simply replay message

If want stateless scheme, instead want at least two messages
Challenge-Response
C-R Using Encryption

\[ sk = k \]

\[ ch = Enc(k, r) \]

\[ res = Dec(k, ch) \]

Random \( r \)

\[ vk = k \]

\[ ch = Enc(k, r') \]

\[ res \? \]

\[ res == r \? \]
Theorem: If $(Enc, Dec)$ is a CPA-secure secure SKE/PKE scheme, then the C-R protocol is a secret key/public key identification protocol secure against eavesdropping attacks.
C-R Using MACs/Signatures

sk = k

ch = r
res = MAC(k, ch)

Random r
or r = Time

vk = k

ch = r'
res?

Ver(k, ch, res)?
Theorem: If $(\text{MAC,Ver})$ is a CMA-secure secure MAC/Signature scheme, then the C-R protocol is a secret key/public key identification protocol secure against eavesdropping attacks.
Active Attacks
Active Attacks

For enc-based C-R, CPA-secure is insufficient
• Instead need CCA-security (lunch-time sufficient)

For MAC/Sig-based C-R, CMA-security is sufficient
Announcements

HW6 Due April 23\textsuperscript{rd}
HW7 Due April 30\textsuperscript{th}