Introduction to

Cybersecurity

David J. Malan
malan@harvard.edu

Securing Systems

Encryption

Wi-Fi

Wi-Fi Protected Access

HTTP

Alice ↔ Eve ↔ Bob

Machine-in-the-Middle Attacks

```
<!DOCTYPE html>

<html>
  …
  <body>
    …
  </body>
</html>
```

```
<!DOCTYPE html>

<html>
  …
  <body>
     <script src="ad.js"></script>
     …
  </body>
</html>
```

```
<!DOCTYPE html>

<html>
  …
  <body>
    <script src="ad.js"></script>
    …
  </body>
</html>
```

Packet Sniffing

```
GET /search?q=cats HTTP/3
Host: example.com
```

```
GET /search?q=cats HTTP/3
Host: example.com
```

```
POST /checkout HTTP/3
Host: example.com

number=4242424242424242
```

```
POST /checkout HTTP/3
Host: example.com

number=4242424242424242
```

Cookies

```
HTTP/3 200
Set-Cookie: session=1234abcd
```

```
HTTP/3 200
Set-Cookie: session=1234abcd
```

```
GET / HTTP/3
Cookie: session=1234abcd
```

```
GET / HTTP/3
Cookie: session=1234abcd
```

Session Hijacking

```
GET / HTTP/3
Cookie: session=1234abcd
```

HTTPS

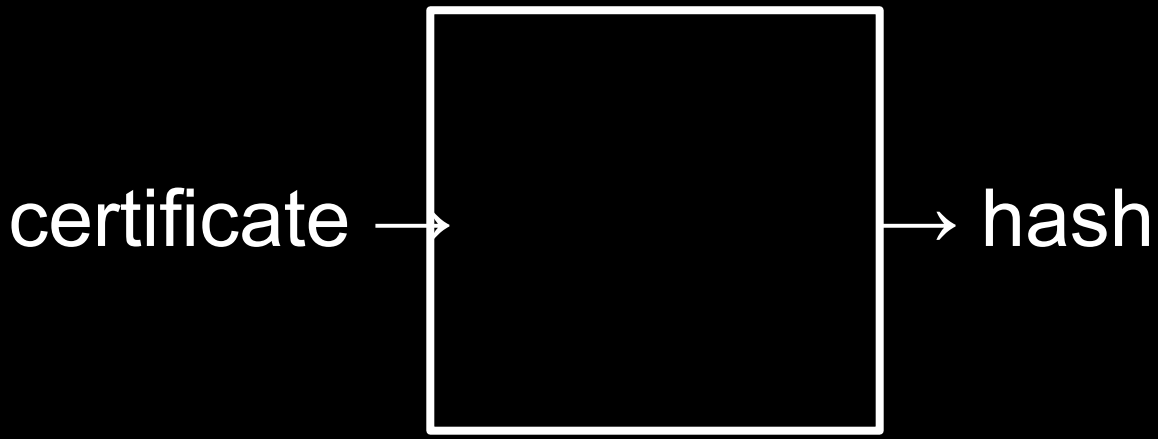
Alice ↔ Bob

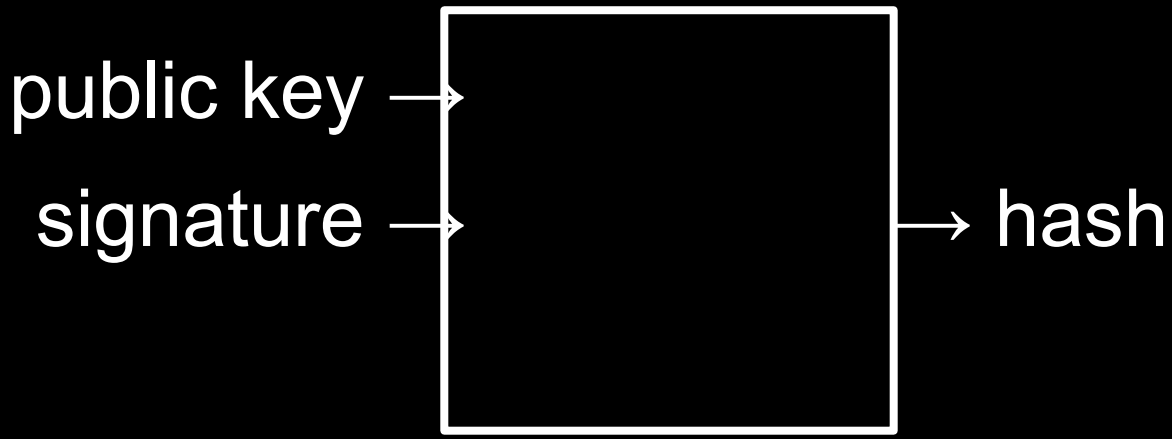
TLS

Certificate

X.509

Certificate Authority (CA)


certificate
hash


public key
signature
hash

SSL Stripping

```
GET / HTTP/3
Host: example.com
```

```
HTTP/3 307
Location: https://examp1e.com/
```

```
HTTP/3 307
Location: https://examp1e.com/
```

```
HTTP/3 307
Location: https://examp1e.com/
```

HSTS

```
Strict-Transport-Security: max-age=31536000
```

```
Strict-Transport-Security: max-age=31536000; includeSubDomains
```

```
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
```

VPN

Alice ↔ Bob

SSH

Alice ↔ Bob

$

```
$ d
```

```
$ da
```

$ dat

```
$ date
```

```
$ date
Thu Jan  1 12:00:00 AM EST 1970
```

```
$ date
Thu Jan  1 12:00:00 AM EST 1970

$
```

```
$ date
Thu Jan  1 12:00:00 AM EST 1970

$ s
```

```
$ date
Thu Jan  1 12:00:00 AM EST 1970

$ ss
```

```
$ date
Thu Jan  1 12:00:00 AM EST 1970

$ ssh
```

```
$ date
Thu Jan  1 12:00:00 AM EST 1970

$ ssh s
```

```
$ date
Thu Jan  1 12:00:00 AM EST 1970

$ ssh st
```

```
$ date
Thu Jan  1 12:00:00 AM EST 1970

$ ssh sta
```

```
$ date
Thu Jan  1 12:00:00 AM EST 1970

$ ssh stan
```

```
$ date
Thu Jan  1 12:00:00 AM EST 1970

$ ssh stanf
```

```
$ date
Thu Jan  1 12:00:00 AM EST 1970

$ ssh stanfo
```

```
$ date
Thu Jan  1 12:00:00 AM EST 1970

$ ssh stanfor
```

```
$ date
Thu Jan  1 12:00:00 AM EST 1970

$ ssh stanford
```

```
$ date
Thu Jan  1 12:00:00 AM EST 1970

$ ssh stanford.
```

```
$ date
Thu Jan  1 12:00:00 AM EST 1970

$ ssh stanford.e
```

```
$ date
Thu Jan  1 12:00:00 AM EST 1970

$ ssh stanford.ed
```

```
$ date
Thu Jan  1 12:00:00 AM EST 1970

$ ssh stanford.edu
```

```
$ date
Thu Jan  1 12:00:00 AM EST 1970

$ ssh stanford.edu
$
```

```
$ date
Thu Jan  1 12:00:00 AM EST 1970

$ ssh stanford.edu
$ d
```

```
$ date
Thu Jan  1 12:00:00 AM EST 1970

$ ssh stanford.edu
$ da
```

```
$ date
Thu Jan  1 12:00:00 AM EST 1970

$ ssh stanford.edu
$ dat
```

```
$ date
Thu Jan  1 12:00:00 AM EST 1970

$ ssh stanford.edu
$ date
```

```
$ date
Thu Jan  1 12:00:00 AM EST 1970

$ ssh stanford.edu
$ date
Wed Dec 31 09:00:00 PM PST 1969
```

Port

22
80
443
…

Port Scanning

Penetration Testing

Ethical Hacking

Firewall

IP Address

Deep Packet Inspection

Proxy

Alice ↔ Eve ↔ Bob

https://example.com/?url=...

https://example.com/?url=...

Malware

Virus

Worm

Botnet

Denial-of-Service Attack (DoS)

Distributed Denial-of-Service Attack (DDoS)

Antivirus

Automatic Updates

Zero-Day Attacks

Introduction to

Cybersecurity

David J. Malan
malan@harvard.edu