Software and Web Security 2

MitM attacks on sessions

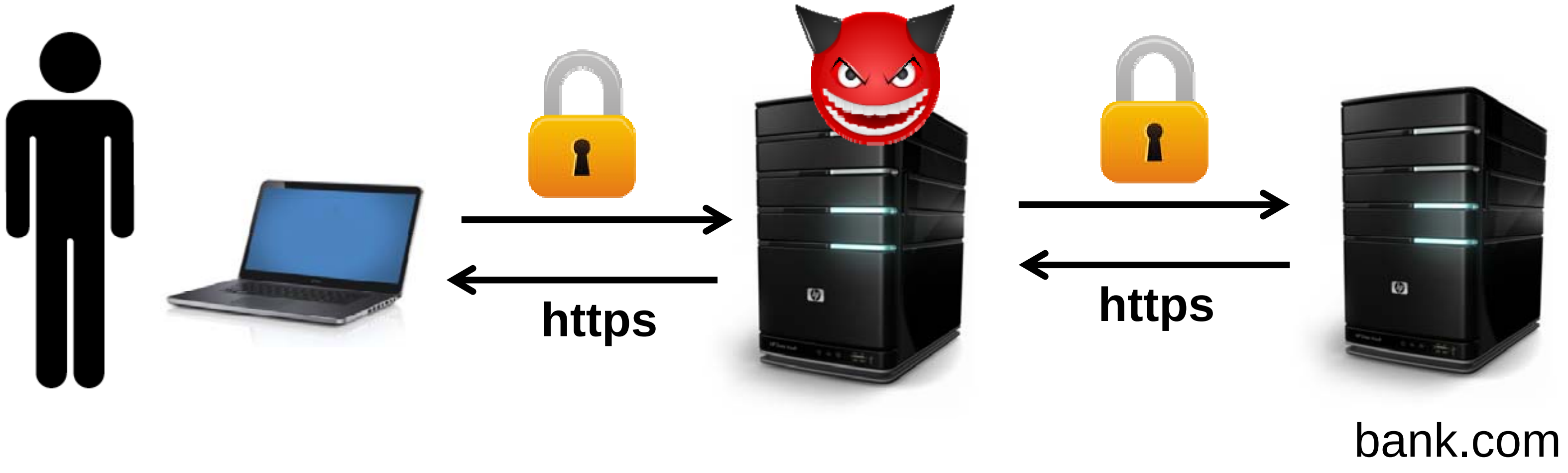
MitM (Man-in-the-Middle)attacks

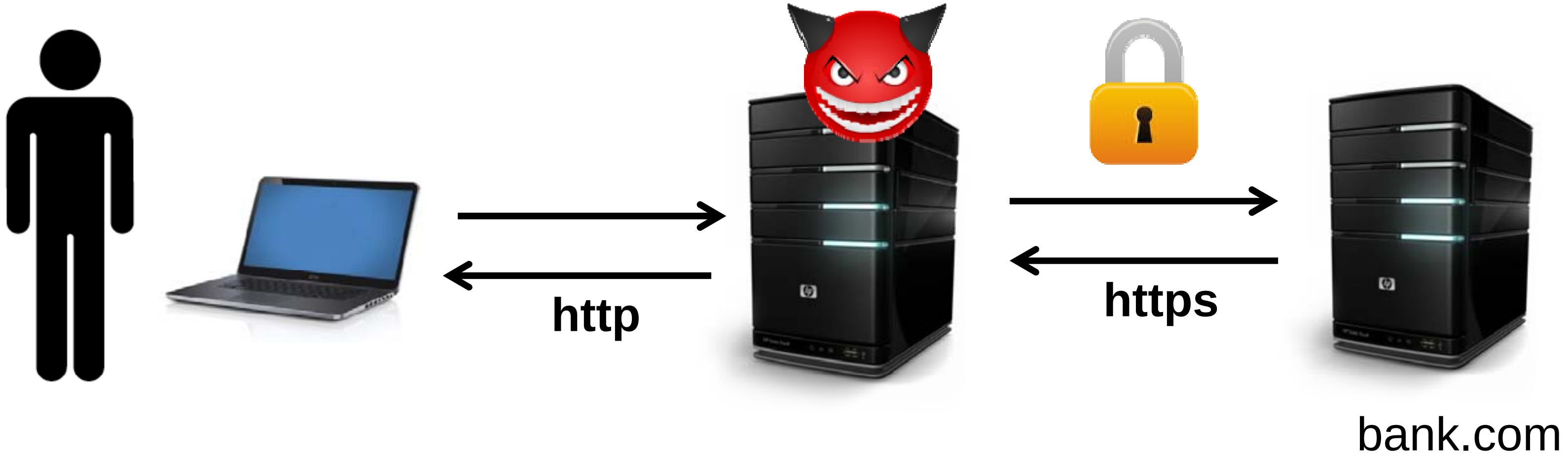
- MitM attack: attacker gets between the browser and the web server, eg
  - by setting up a wifi access point
  - by luring victim to his website and passing on traffic to another site

- https (ie TLS/SSL) should protect against this...

- Recorded presentation by Moxie Marlinspike highlights the problem that *https* connection is often set up by an *http* request
  - first step is then unprotected...

Two variants of SSL stripping





SSL stripping (1): https+https

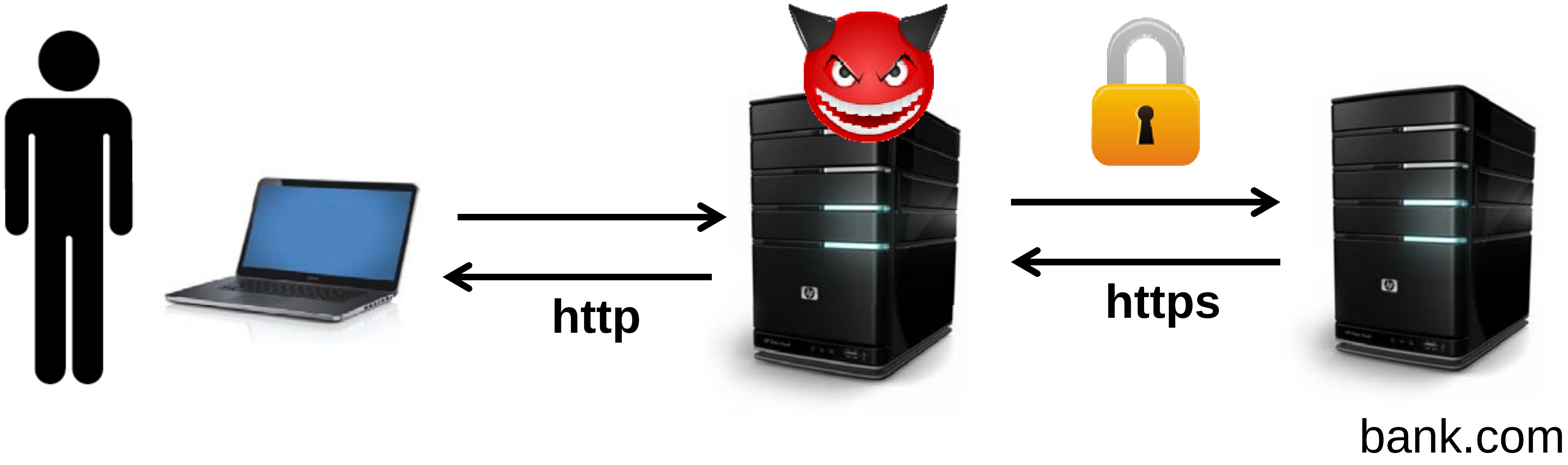
Different ways for attacker to set up the first https tunnel to himself

1. Use a self-signed certificate for bank.com
   - but warnings will scare most users away ☹
2. Buggy https implementations in browser may be tricked by attacker using his genuine leaf certificate for mafia.com to sign a certificate for bank.com
3. Attacker can buy domain name that looks like bank.com with international characters
   - but browser using puny-code will reveal this to user ☹
4. Attacker can redirect to mafia.com
   a) and hope the user does not notice the mafia.com in address bar
   b) better, use characters that look like / and ? to make URL that looks like the bank's (eg http://bank.com/Somelongname?.mafia.com)
      - but browser highlighting domain part of URL may warn user ☹

(The recorded Blackhat presentation discusses 2 and 4b)

SSL stripping (2) http+https

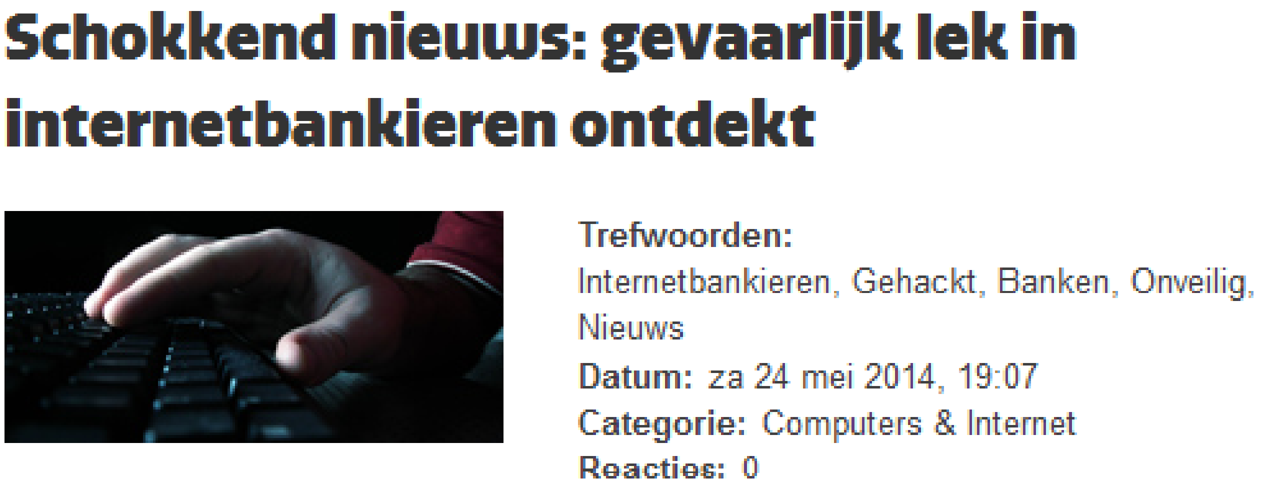
- A MitM attacker can simply not bother with setting up an https tunnel to the client, and simply use for the first leg, hoping the user won't notice the missing s



(The recorded Blackhat presentation discusses this option too)

(oud) nieuws

- http://kassa.vara.nl/tv/afspeelpagina/fragment/schokkend-nieuws-gevaarlijk-lek-in-internetbankieren-ontdekt/speel/1/
- http://webwereld.nl/beveiliging/82658-geld-stelen-via-hotspots-kon-door-lek-in-internetbankieren



Schokkend nieuws: gevaarlijk lek in internetbankieren ontdekt

Trefwoorden: Internetbankieren, Gehackt, Banken, Onveilig, Nieuws
Datum: za 24 mei 2014, 19:07
Categorie: Computers & Internet
Reacties: 0

Countermeasures

- HSTS (HTTP Strict Transport Security)

  Server declares *“I only talk HTTPS”*

  ```
  HTTP(S) Response Header:
  Strict-Transport-Security: max-age=15768000;
  includeSubDomain
  ```

- use HTTPS Everywhere browser plugin

- Other possible solutions in the pipeline: CERT Pinning & DNSSEC for TLS

Alternative MitM attack: stealing https cookies

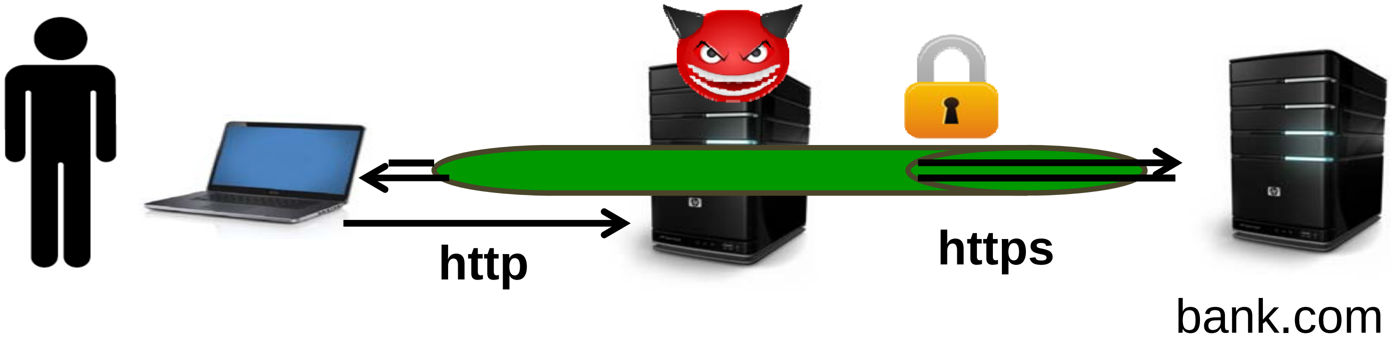
- If secure flag is not set for a cookie, then the cookie set in an https session will also be sent over with http requests

- A MitM attacker can then try to steal the cookie

Alternative MitM attack: stealing https cookies

Attack steps

1. user logs on to https://bank.com
2. server sets session ID for bank.com in cookie
   - which is encrypted in https-traffic
3. users ask for an unencrypted HTTP request (eg for http://nu.nl)
4. MitM attacker replies with a redirect to http://bank.com
5. Browser follows redirect and sends the bank’s cookie over http
6. Bingo! Attacker has the cookie


http
https
bank.com