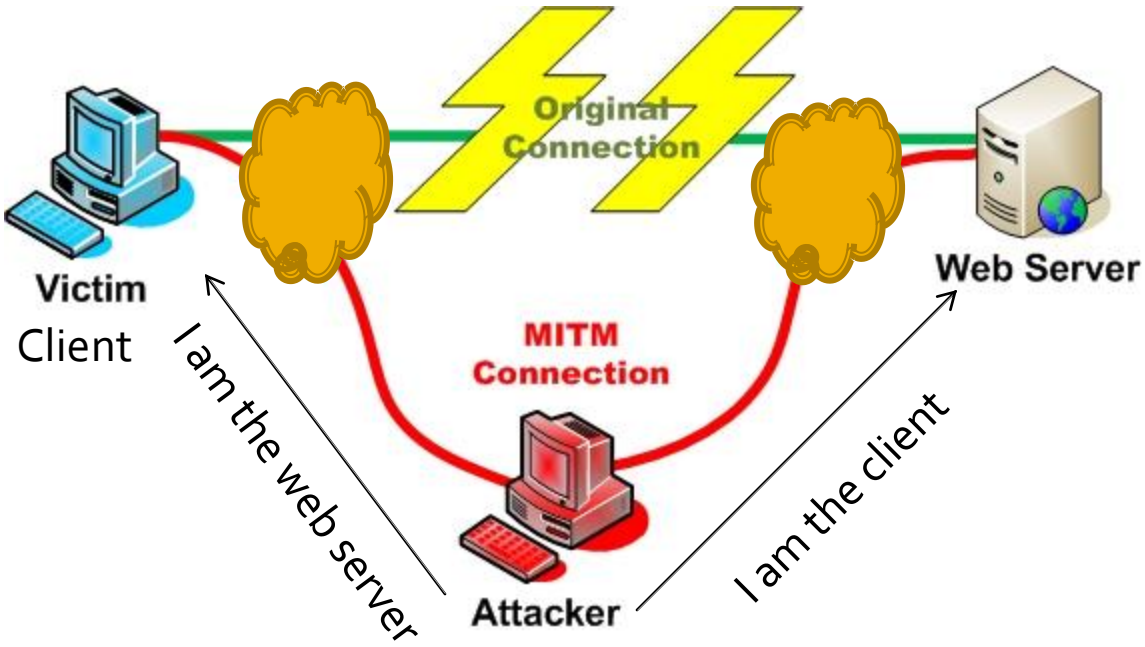
Using Secure Search Engine to Counter Web based Man-in-the-Middle and Phishing attacks

MITM

- In cryptography, the **man-in-the-middle attack** or **bucket-brigade attack** (often abbreviated **MITM**), sometimes **Janus attack**, is a form of active eavesdropping in which the attacker makes independent connections with the victims and relays messages between them, making them believe that they are talking directly to each other over a private connection when in fact the entire conversation is controlled by the attacker. (Definition from Wikipedia)
- MITM is due to the lack of strong mutual authentication.

MITM in Web based Applications

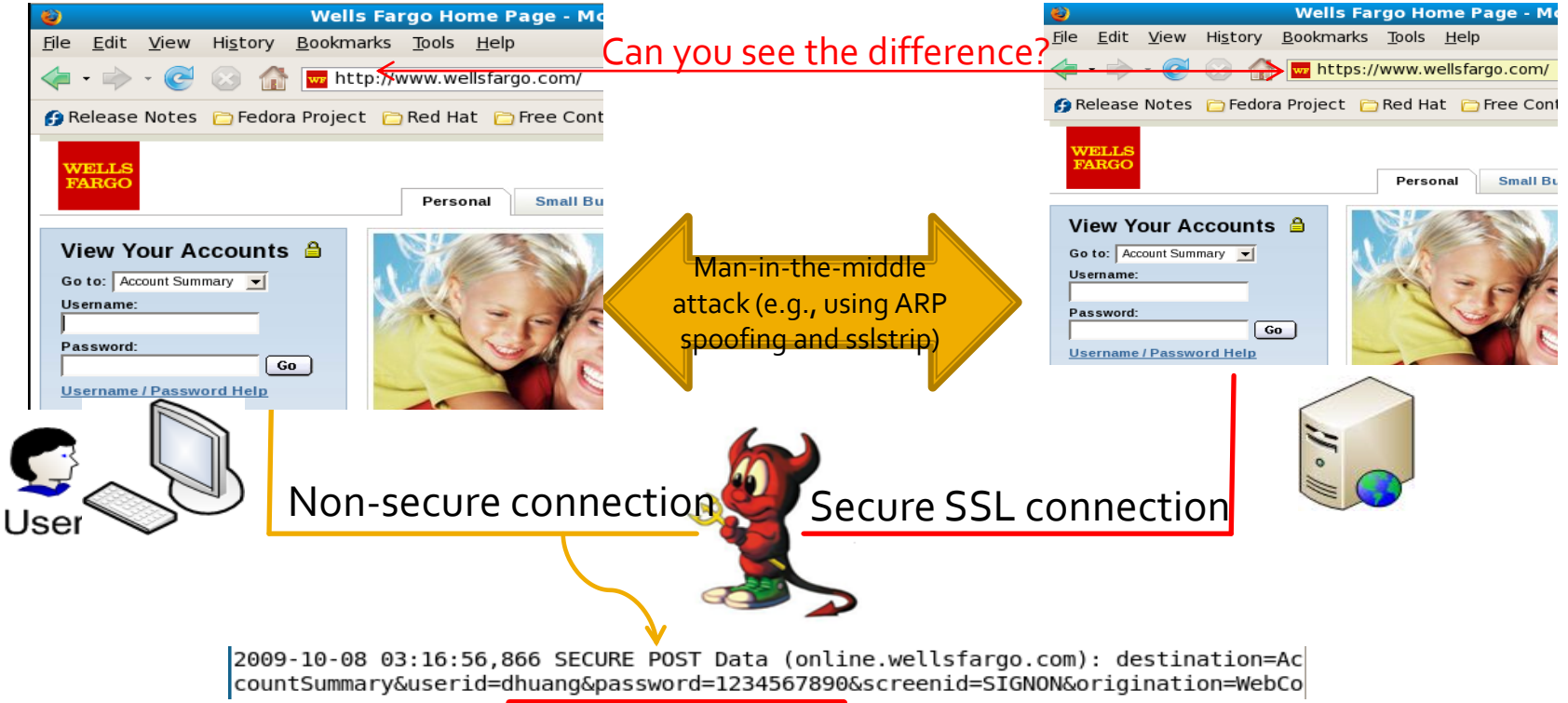


SSLStrip Man-In-The-Middle Attacks

MITM: attackers hijack in the communication session between the user and web server. One of newest attack is SSLStrip MITM, presented at BlackHat Conference, DC, 2009.

Vulnerability: It is users' responsibility to check if the secure connection is established or not. Human-in-the-loop approaches always cause security problems!!!

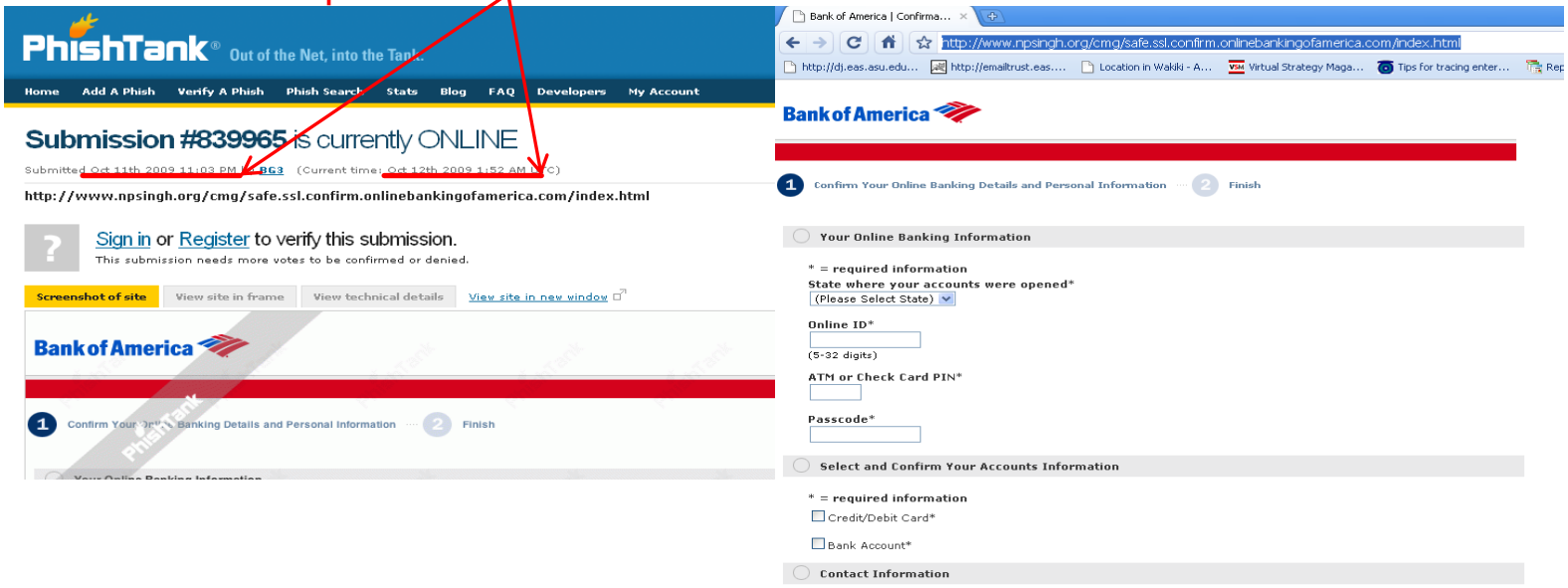
Current Solutions: There is no known technical solution to counter web-based MITM attacks.



Phishing Attacks

- Web browser based phishing filters are not effective
  - Too many false positive and false negative.
- Social network-based ranking system, e.g., Web-Of-Trust (WOT), PhishTank, cannot keep up the changing of phishing sites
  - Many new phishing sites are not identified and reported.
  - They depend on users' reports, which can cause long delay.

Reported more than 12 hours Chrome can still access

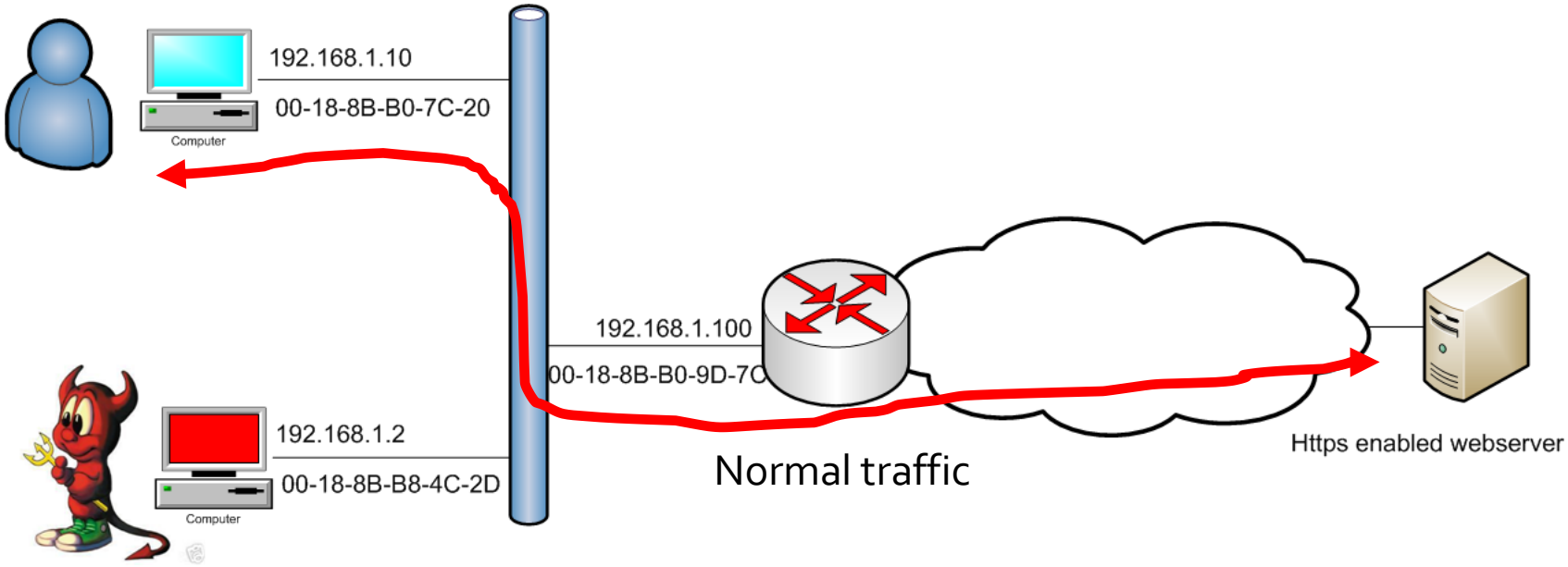


The way to encounter https

1. http 302 is used to redirect http to https
2. Click a link with https
3. Manually input the https in the address bar

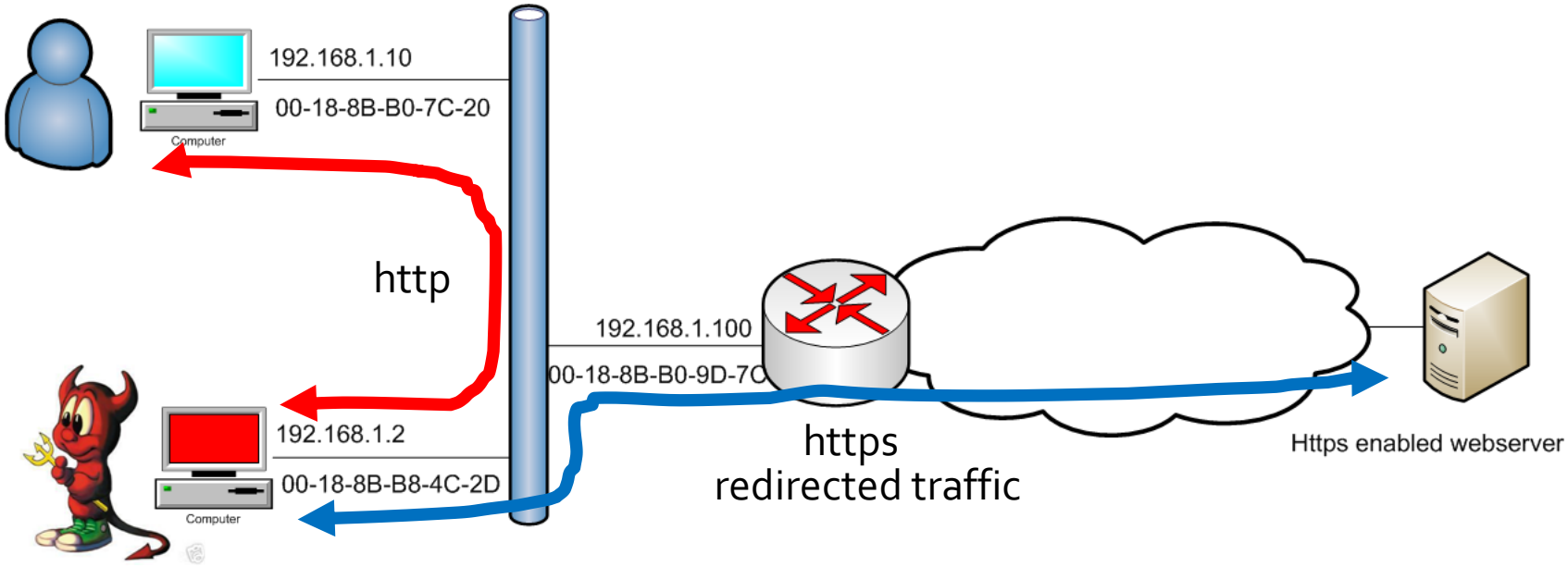
sslstrip demo

- Network Configuration



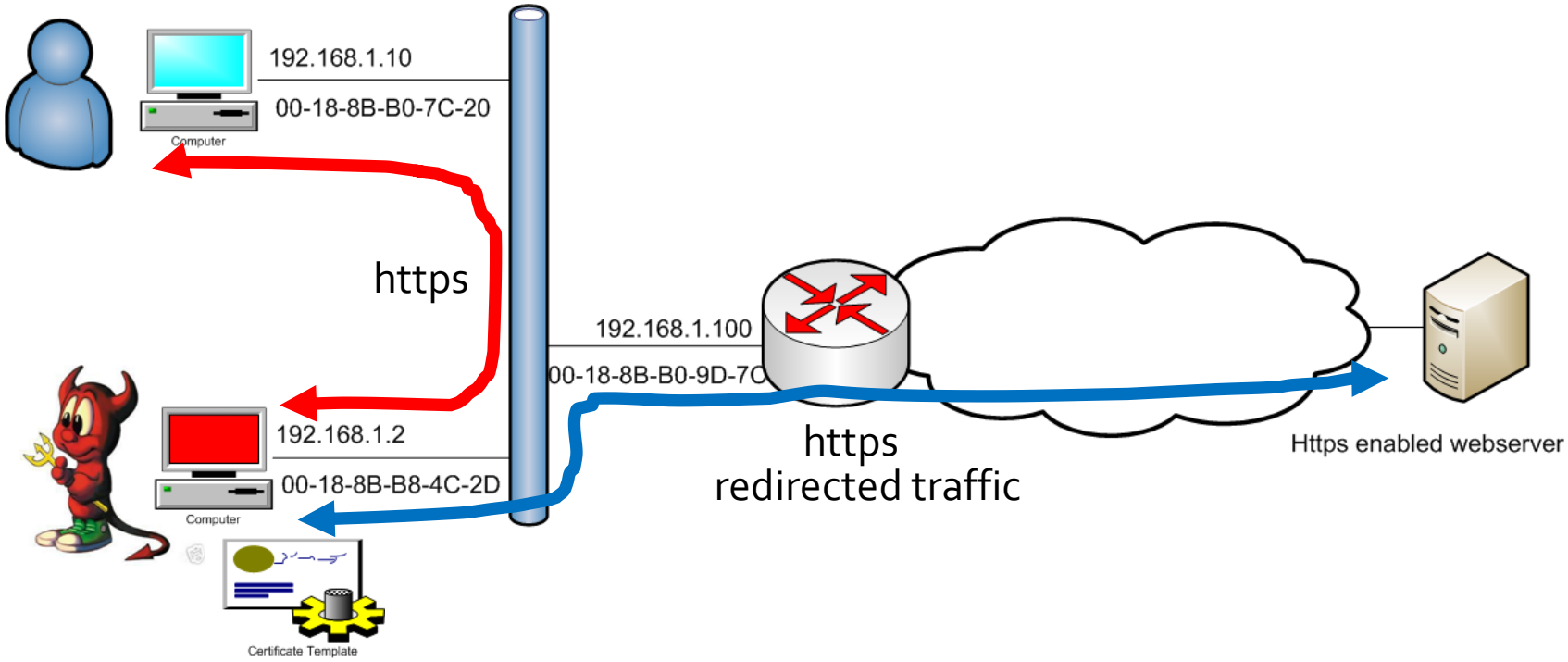
sslstrip demo

- Network Configuration



sslstrip demo

- Network Configuration



When certificate is used. This can be done by exploring the certificate chain vulnerability.

sslstrip demo

- Procedures:
  1. Setting up IP Forwarding:

  ```
  echo 1 > /proc/sys/net/ipv4/ip_forward
  ```

  2. ARP MITM attack between Victim and Gateway:

  ```
  arpspoof -i eth0 -t 192.168.1.100 192.168.1.2
  ```

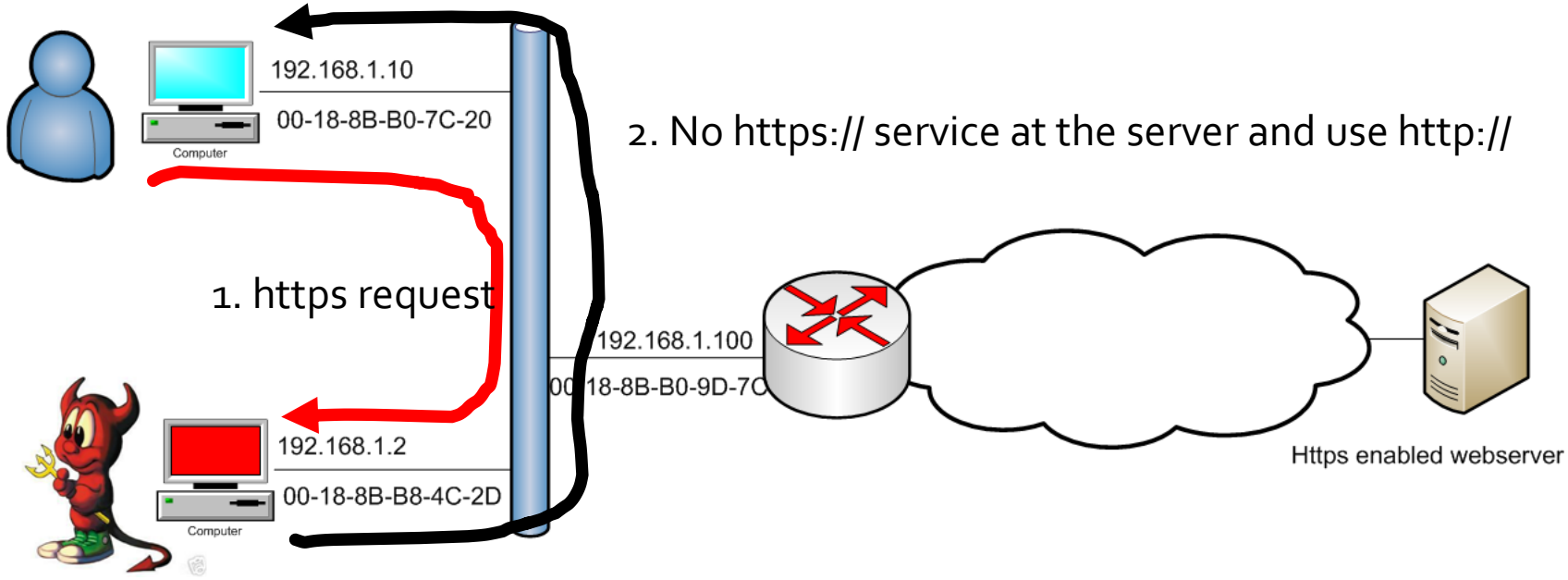
  3. Setting up port redirection using Iptables:

  ```
  iptables -t nat -A PREROUTING -p tcp --
  destination-port 80 -j REDIRECT --to-ports
  10000
  ```

  4. Start the SSLstrip tool and make it listen to port 10000

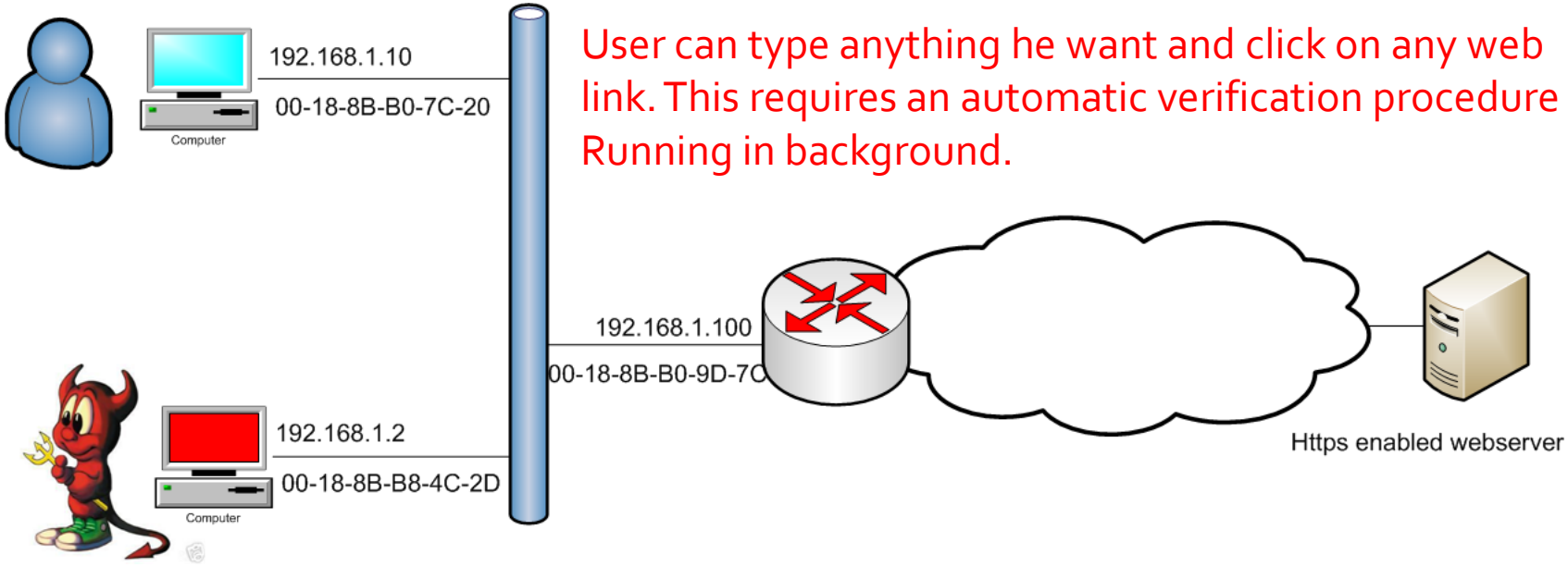
Solution Design requirements

- Requirement 1
  - The attacker cannot reject the https:// request by saying there is no such a connection at the sever side



Design requirements

- Requirement 2
  - Involve minimal level of actions of naïve users. This requires the solution is automatic and runs in the backgrounds

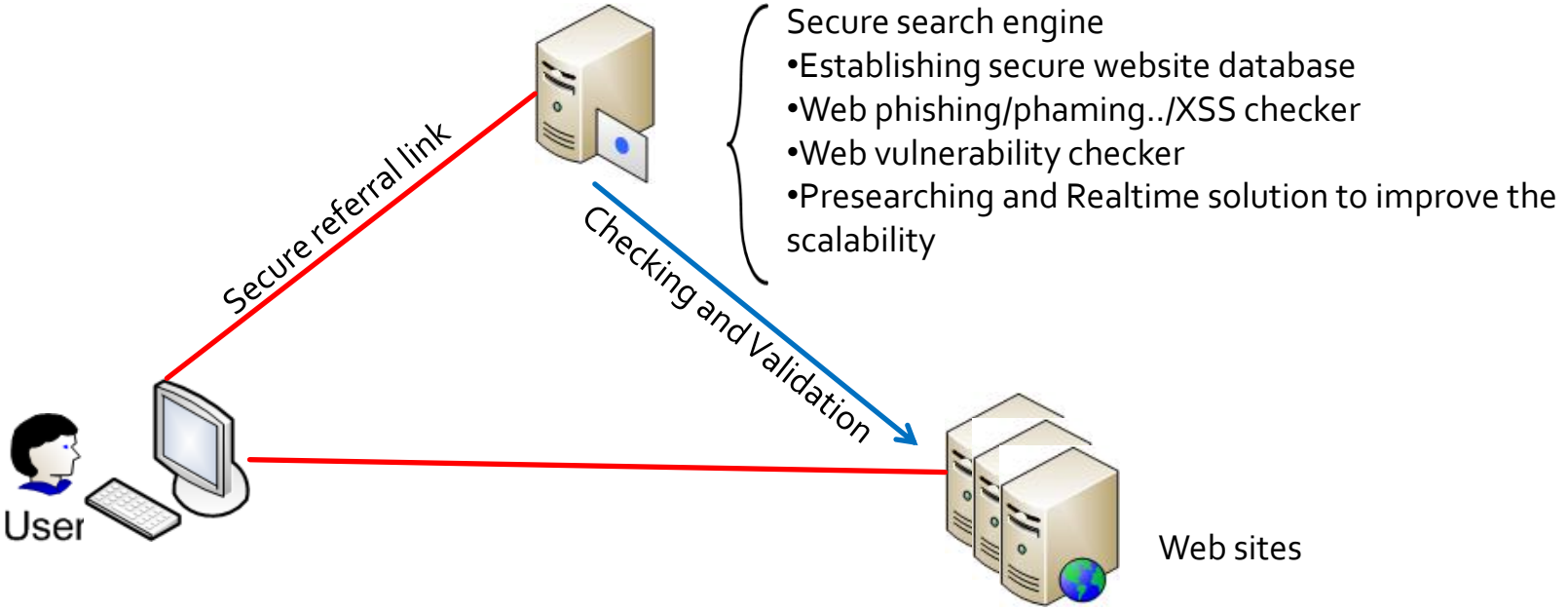


Proposed Solutions

- We propose to use Secure Search Engine(SSE) hosted at https://securesearch.eas.asu.edu validate an https link.
- Apart from the validating the URL the search engine will also check if the web page is a phishing site or a non phishing site.
- The browser extension available at the client side would forward all the validation request to the SSE.

Secure Web Referral Service

- Secure web referral service counters web-based MITM and Phishing attacks.
  - It provides realtime trusted web ranking to end users in the background through a secure connection to a secure search engine.
  - MITM attacker cannot hijack in the secure referral connection
  - Phishing attack can be prevented through a hybrid solution using phishing repository and realtime scanning.
  - The referral service can be extended to more security vulnerability checking.



Project

- Project prototype can be found at https://www.wreferral.com