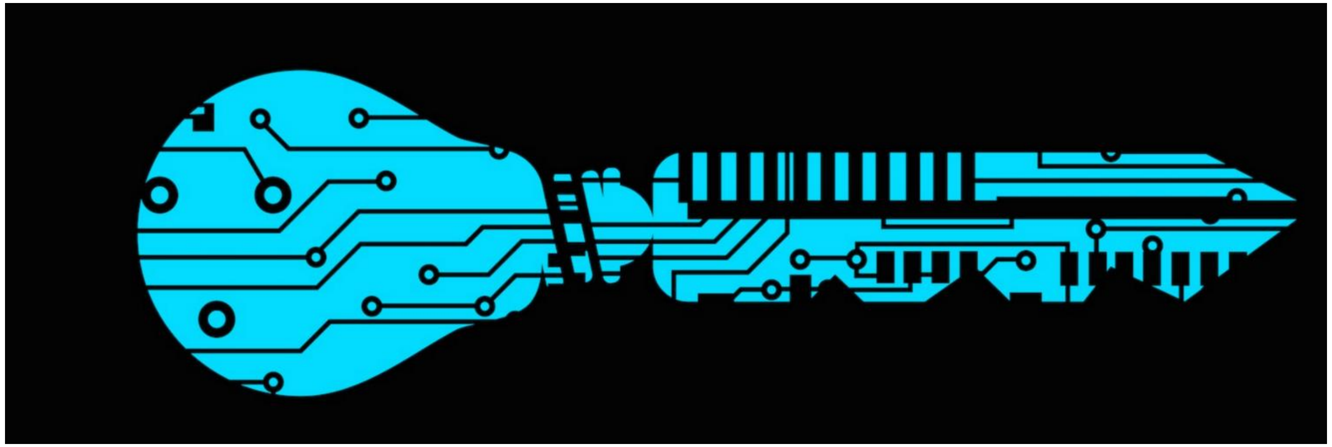
Changing the Cryptographic Key That Secures the Web

Joshua Lai

Wait? What Key?

- How do we search for information on the web?
- So how do we know that our searches are secure?

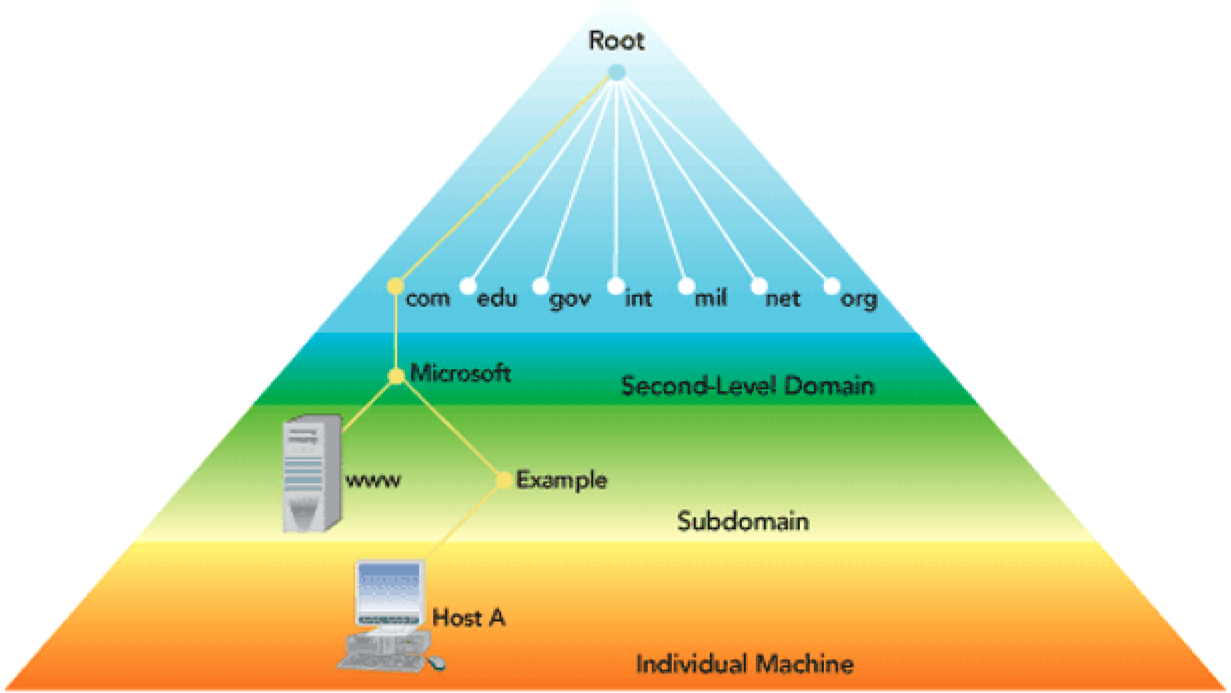


History

- When the web was first released, the DNS was not configured with the ideas behind our security principles today.
- Threats and Attacks on the DNS
- So how do we protect the DNS in the first place?
- The Internet Corporation for Assigned Names and Numbers (ICANN)

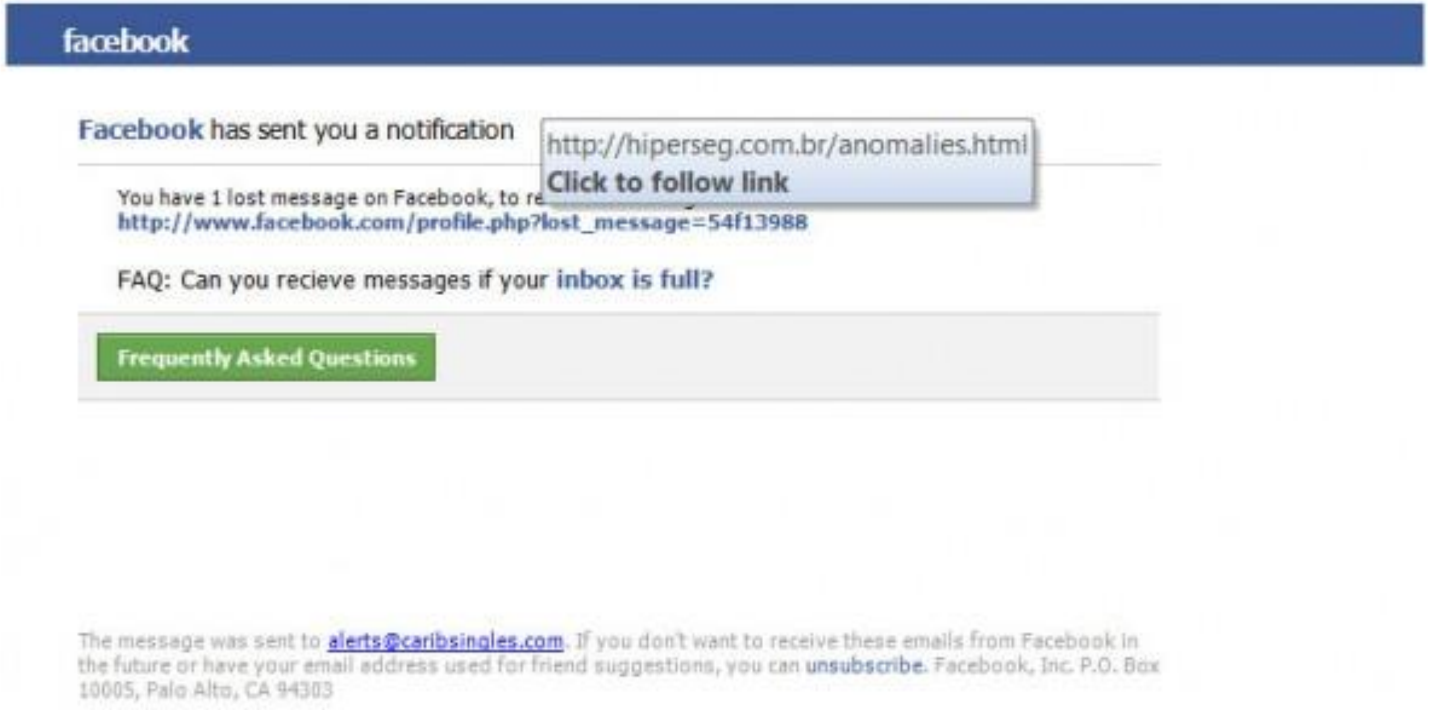
How does it work?

- Key (part of DNS Security Extensions) creates the first link in a long chain of cryptographic trust and protects the DNS root zone
- Processes and checks DNS data that comes in to ensure that it is correct
- Any piece of incorrect data will return an error
- If anyone holds this key, they can control much of the traffic
- Note: Keys do not encrypt data



Why Change?

- One of the biggest security issue is DNS cache poisoning / DNS spoofing
  - Forcing the DNS to return incorrect IP address and diverting traffic to different location
- Good cryptographic hygiene like changing your personal passwords occasionally
- Increase 1024 bits -> 2048 bits



Facebook has sent you a notification

http://hiperseg.com.br/anomalies.html
Click to follow link

You have 1 lost message on Facebook, to re
http://www.facebook.com/profile.php?lost_message=54f13988

FAQ: Can you recieve messages if your inbox is full?

The message was sent to alerts@caribsingles.com. If you don't want to receive these emails from Facebook in the future or have your email address used for friend suggestions, you can unsubscribe. Facebook, Inc. P.O. Box 10005, Palo Alto, CA 94303

So how does this apply to you?

- Heightened protection for your sake when you are looking up documentation for this class
- Continue browsing like you always do
  - Just be cautious of where you are going
- Know that at anytime, the key can be compromised

Sources

- Cox, Joseph. “The Cryptographic Key That Secures the Web Is Being Changed for the First Time.” *MOTHERBOARD*, www.motherboard.vice.com/read/the-encryption-key-that-secures-the-web-is-being-changed-for-the-first-time.