SECURITY

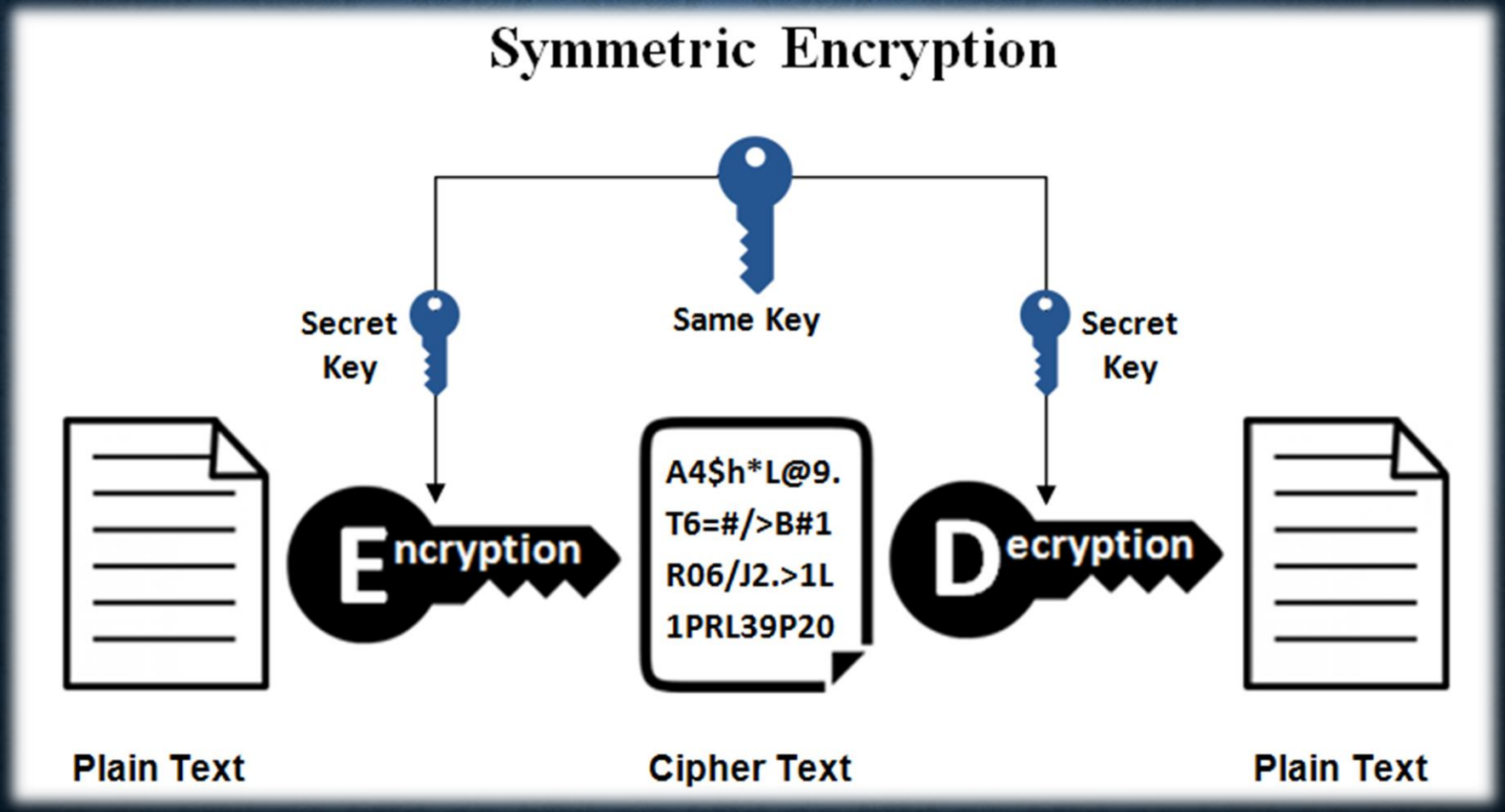
Encryption, SSL, Private Routing, and DDOs Attacks

COS216
AVINASH SINGH
DEPARTMENT OF COMPUTER SCIENCE
UNIVERSITY OF PRETORIA

SYMMETRIC ENCRYPTION

- Symmetric encryption algorithms use 1 key to do both the encryption of the plaintext, as well as the later decryption of the ciphertext
- The key/password can be used by anyone, so it is important to keep it secret
- Typically used to encrypt files or hard drives
- Common algorithms: AES, TwoFish, BlowFish, Serpent, SkipJack

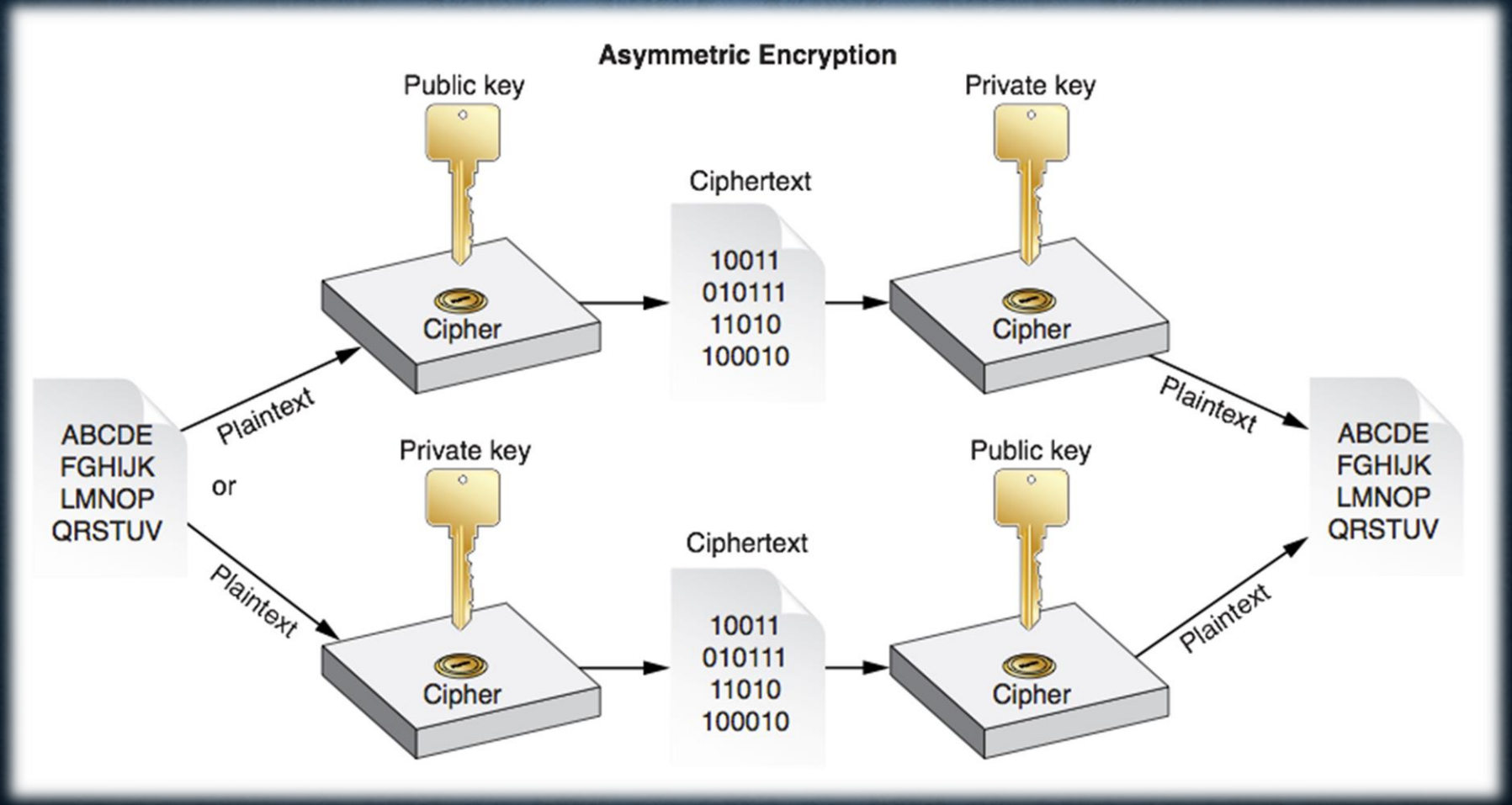
SYMMETRIC ENCRYPTION



ASYMMETRIC ENCRYPTION

- Asymmetric encryption uses a private and public key
  - The public key can be openly shared on the internet
  - The private key has to be kept safe
- If you send a message to Professor X:
  - Encrypt the message with Professor X's public key and your private key
  - Professor X will decrypt your message with his private key and your public key
- Used for SSL certificates, online banking, and email encryption
- Common algorithms include: RSA, ECC, DSA
- Often mathematically proven to be uncrackable (except for brute force)

ASYMMETRIC ENCRYPTION



SSL CERTIFICATES

- SSL certificates are used for encryption between client and server
- TLS is the improved version of SSL, and works very similar
- Uses both asymmetric (typically RSA) and symmetric (typically AES) encryption
- If and SSL certificate is installed on a server
  - Access the website via HTTPS
  - Check that the certificate is validated, green key/lock next to URL in browser

SSL CERTIFICATES

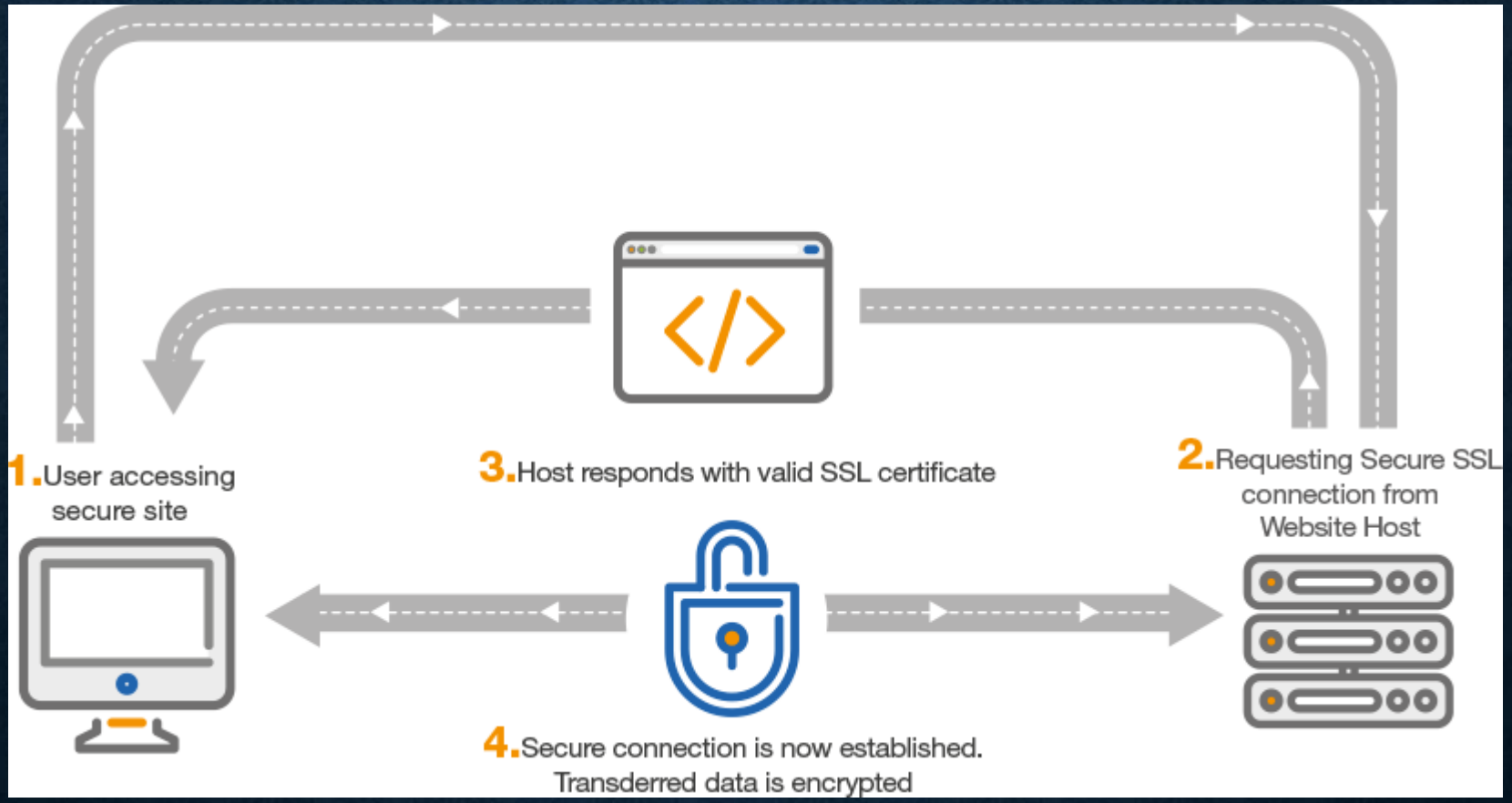
- SSL certificates must be verified by a certificate authority
  - Validates that the certificate is valid and belongs to a specific site
  - Often comes with insurance, so if you purchase something on a website and your money gets stolen, you can submit a request to the authority and get your money back if something went wrong with the certificate
- Certificates can be "self signed"
  - Is not verified by a certificate authority
  - Will still encrypt communication, but not show the green lock in the address bar
  - Will show a notification to the user that the certificate is self signed and "not secure"

SSL CERTIFICATES

- Since you need a third-party certificate authority for the validation, you have to purchase (pay for) a certificate
  - VeriSign, Thawte, Comodo, Symantex, GoDaddy, DigiCert, etc

- Recently a project has started to create and verify certificates for free
  - Already built into many hosting packages
  - Company is called: Let's Encrypt (https://letsencrypt.org)

SSL CERTIFICATES



ONLINE PRIVACY

- Every time you send a request (eg: open a website), your IP address is submitted in the HTTP header
  - Required, since the the response has to be send back to that IP address
- By default, servers log all incoming requests (access log)
  - Stores the IP address, request URL, time, and your browser details
  - Most websites do logging, since it is the default setting in webservers (eg: Apache)
  - Some countries require companies by law to store logs for a certain period of time
- Hence almost every website you ever visited knows you

ONLINE PRIVACY

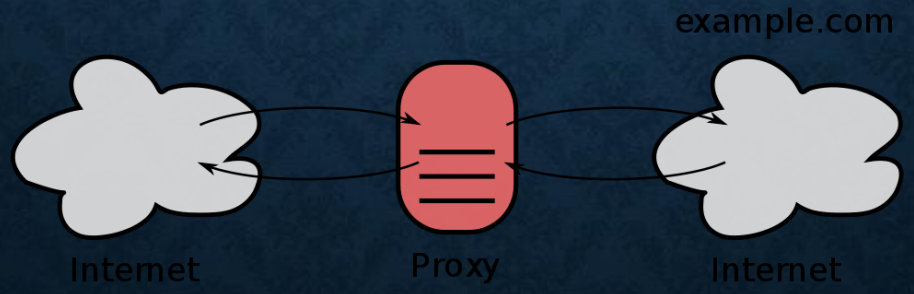
- A simple IP address is enough to track you down
- Many free geolocation services can be used free of charge
  - Used to lookup your IP address and get a rough location
  - Depending on the country, the location is accurate by a few kilometers
  - One of many: https://www.iplocation.net

ONLINE PRIVACY

- In order to get your true address
  - A court order has to be filed in your country
  - Court order forces ISP (eg: Telkom) to hand out your details
  - ISPs keep track of which customer uses which IP and at which given time (even dynamic IPs)

PROXIES

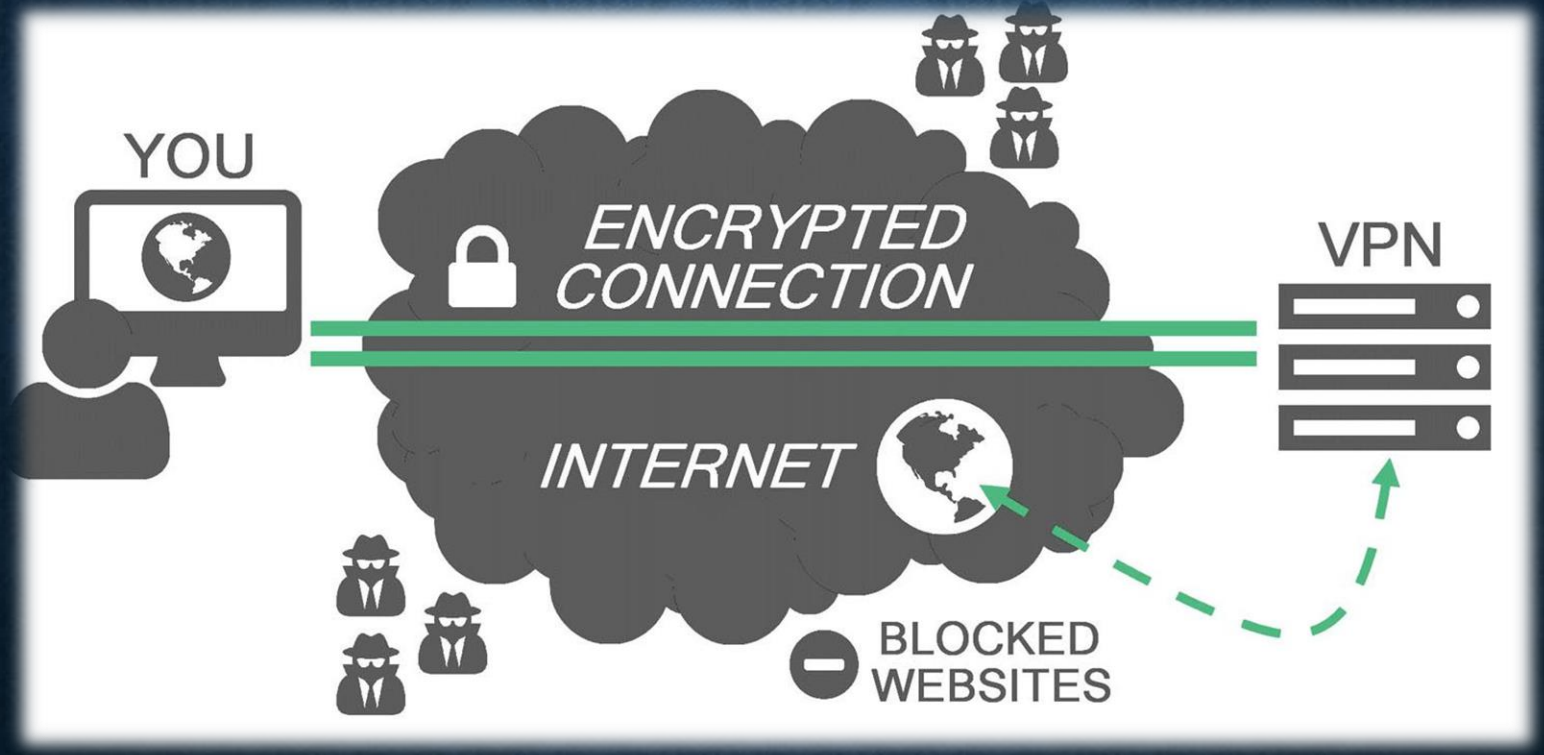
- Proxies are intermediate servers
- Example, instead of sending your request directly to Google, you send it to a proxy server which then forwards it to Google or your behalf
- Different kinds of proxies exists, some are anonymous, but forward your IP address with every request
- Often used by companies to filter requests and/or do authentication
  - Example: University of Pretoria has a proxy server, you have to log in before you can access the website



VIRTUAL PRIVATE NETWORKS

- Virtual Private Networks (VPN) were originally created to create private/**encrypted** connections between computers of a company in different geographic locations
  - Example: Bank branch in Cape Town wants to securely communicate with the branch in Pretoria
- Most VPNs these days are user by individuals to stay anonymous online
- Works similar to a proxy, but your **IP address** is kept private
  - Every website you access will log/track the VPN server's IP address and not yours
  - You still have to trust the VPN company not to release your details

VIRTUAL PRIVATE NETWORKS



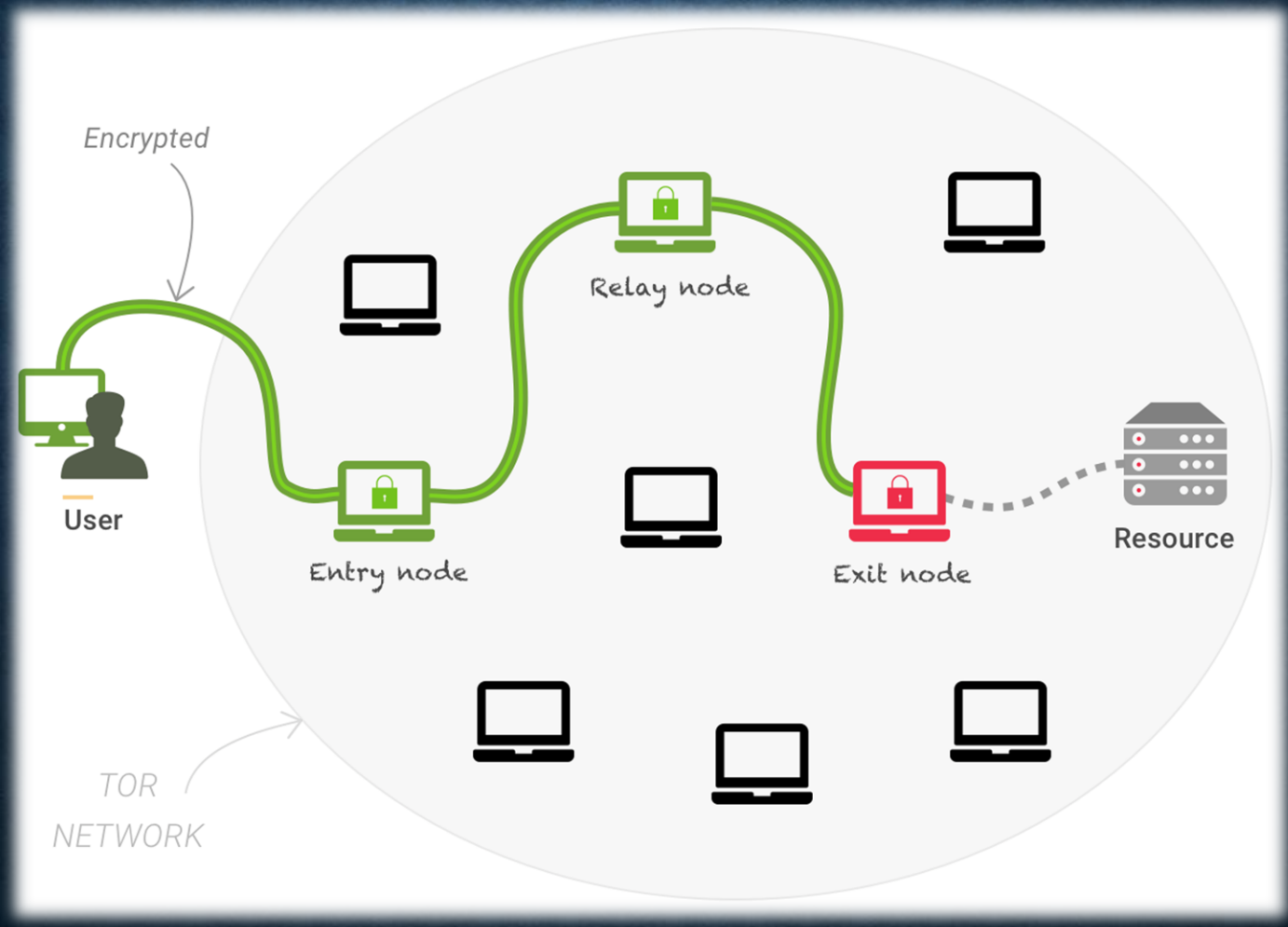
ONION ROUTING

- Onion routing is similar to proxies/VPNs, except that
  - Request are relayed via different intermediate machines instead of only one
  - Each relay has it's own encryption layer (like different layer's of an onion)
  - Is typically slower, but more secure
- Various onion networks exist, such as Tor (developed by the US military), I2P, Freenet
- Not completely anonymous , still subject to some attacks that can reveal your identity

ONION ROUTING

- To use Tor, you have to installed the Tor software and browser
  - The Tor browser is a fork of Firefox
  - The Brave browser has built-in Tor support (check the private tab menu)
- Tor addresses have the TLD .onion
- By default Tor uses 3 hops
  - Hence your request is relayed via 3 different computers/node
  - Each node has its own layer of encryption
  - Each node can only decrypt its own layer
  - Each node only knows about the node immediately before and after it, but not about the other nodes in the chain
  - Nodes are selected randomly

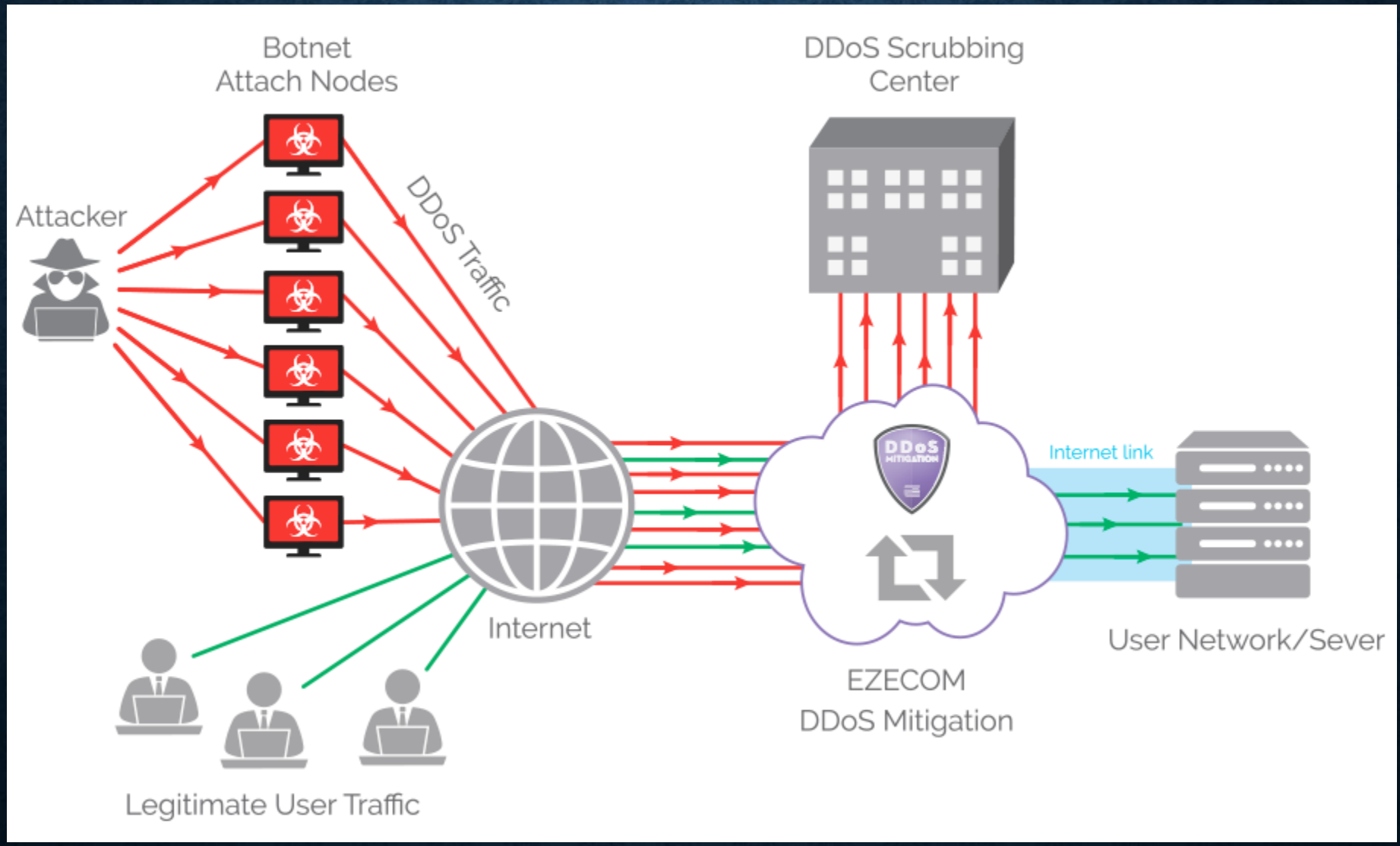
ONION ROUTING



DDOS ATTACKS

- Distributed Denial of Service (DDoS)
- Most common attacks on servers
  - Send many requests to a server in a very short time
  - Server's CPU, memory, disk, and/or connection gets overloaded
  - All incoming requests are queued while the server processes them
  - Server becomes very slow or might even crash
  - Hence, website becomes inaccessible to normal users
- To make so many request at a time
  - Many people have to participate (eg: Anonymous hacking group)
  - Botnet of many computers (eg: many computers infected by a virus)

DDOS ATTACKS



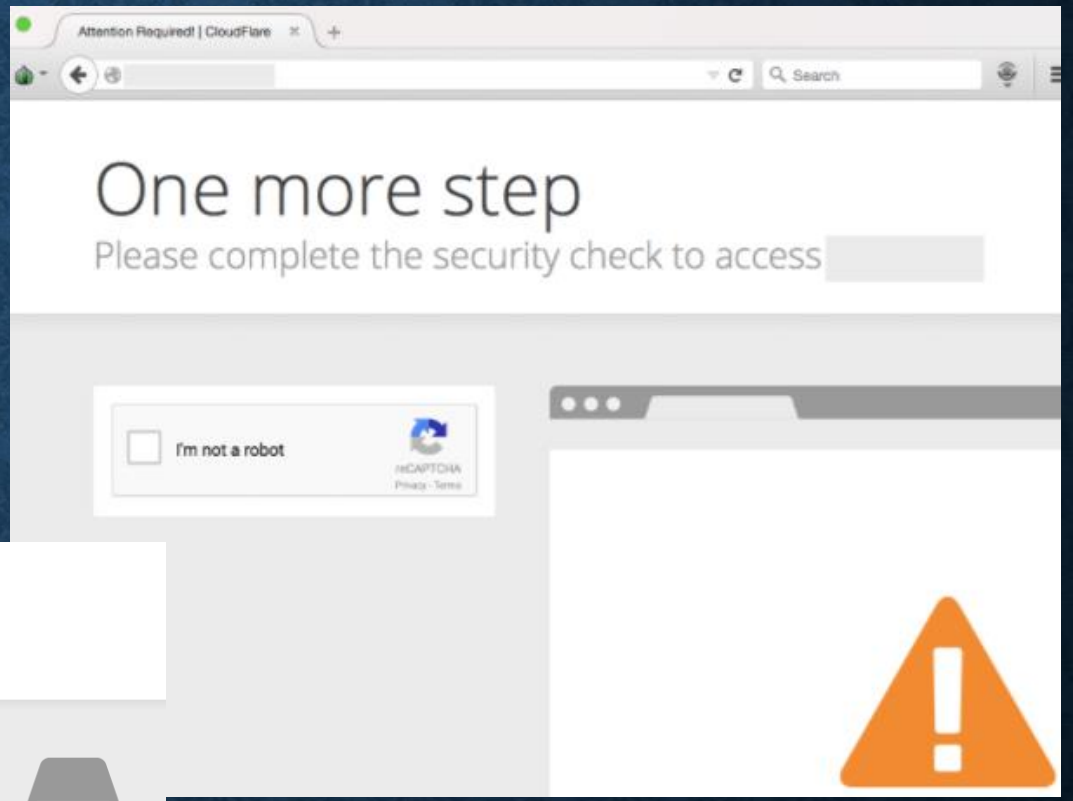
DDOS ATTACKS

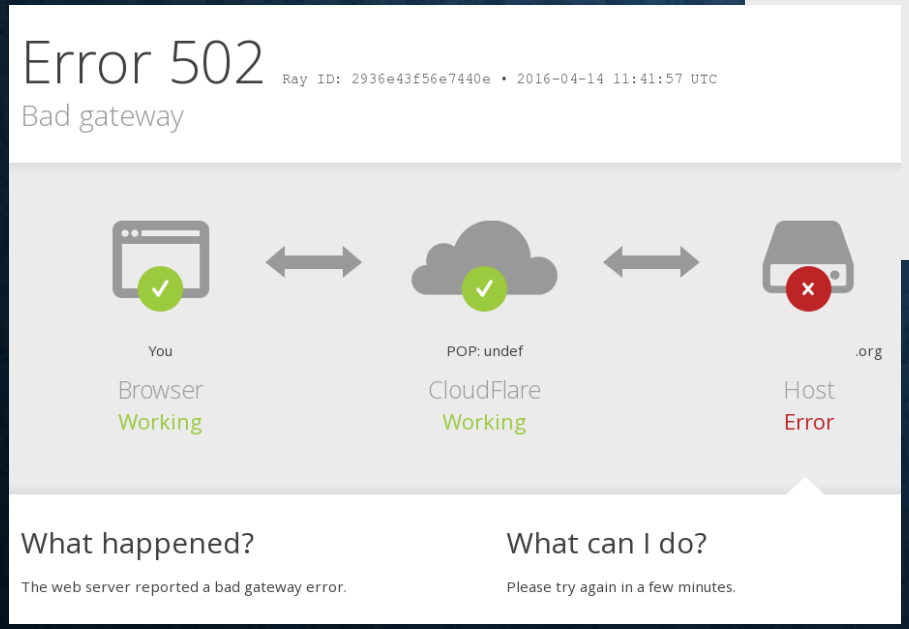
- DDoS attacks only work if the are a lot of bots sending request and the server cannot handle the load
  - A lot more difficult to DDoS attack eg Google, since they have proper servers than can easily handle millions of incoming requests at the same time

- Certain companies like CloudFlare now offer paid/free services
  - Places CloudFlare server between clients and your server
  - Hence DDoS attacks will end up on CloudFlare's server on not yours
  - CloudFlare servers are specifically build to handle DDoS attacks

CLOUDFLARE

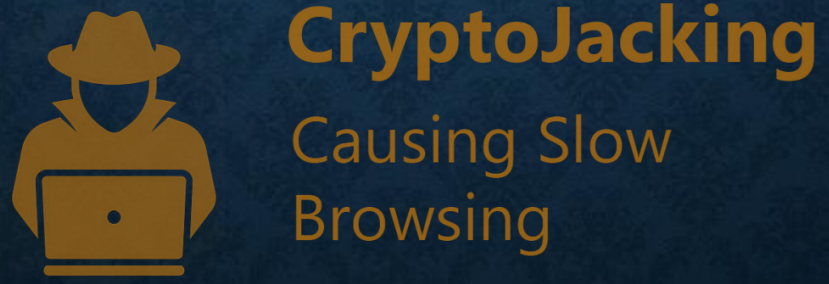
DDOS ATTACKS





CRYPTO JACKING

- New kind of "attack"
- Add JavaScript to a website that mines crypto currencies while the website is opened by a user in the browser
- Many dodgy websites do it, but also many commercial companies
- Google Ads were recently "infected" with crypto jacking scripts
- Can be used in a non-malicious manner by a company to replace advertising on the website with crypto mining to generate an income for the website



SOME VIDEOS

- Onion Routing: https://www.youtube.com/watch?v=QRYzre4bf7I
- WannaCry: https://www.youtube.com/watch?v=88jkB1V6N9w

SECURITY

Encryption, SSL, Private Routing, and DDOs Attacks