NETWORK SECURITY
INTERNET PROTOCOLS AND APPLICATIONS

Félix Cuadrado, Steve Uhlig

felix.cuadrado@qmul.ac.uk, steve.uhlig@qmul.ac.uk

Queen Mary University of London

School of Electronic Engineering and Computer Science

Queen Mary University of London

Contents

- **Network Security**
- Security Attacks
- Encryption, Certificates and Signatures

Computer Security

What is security?

Protecting **assets** against **threats**

Network threats: “attacks focused on attacking a network or the users on the network by manipulating network protocols, ranging from the data-link layer to the application layer”

Simon Hansman, Ray Hunt, "A taxonomy of network and computer attacks". In Computers & Security (2004)

Network security is protecting assets that are network-based from threats

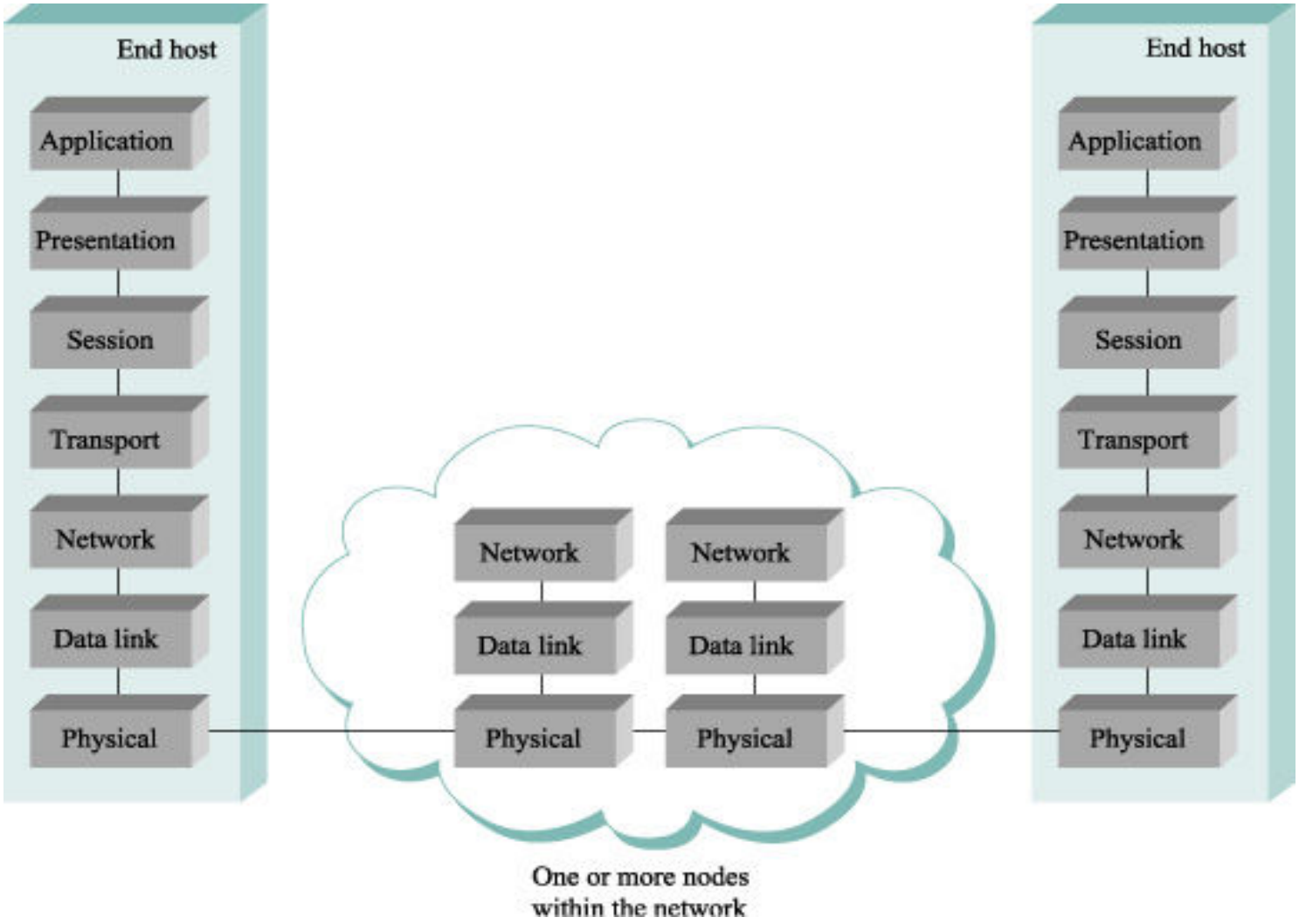
Examples of security threats

- Using a network to steal personal data
- Disabling a network to prevent people accessing a service
- Using a network to monitor traffic and interactions
- Using a network to pretend to be somebody you're not
- Using a network to modify an incoming message altering partially its contents
- Using a network to take control of a remote machine

Computer System Security Properties

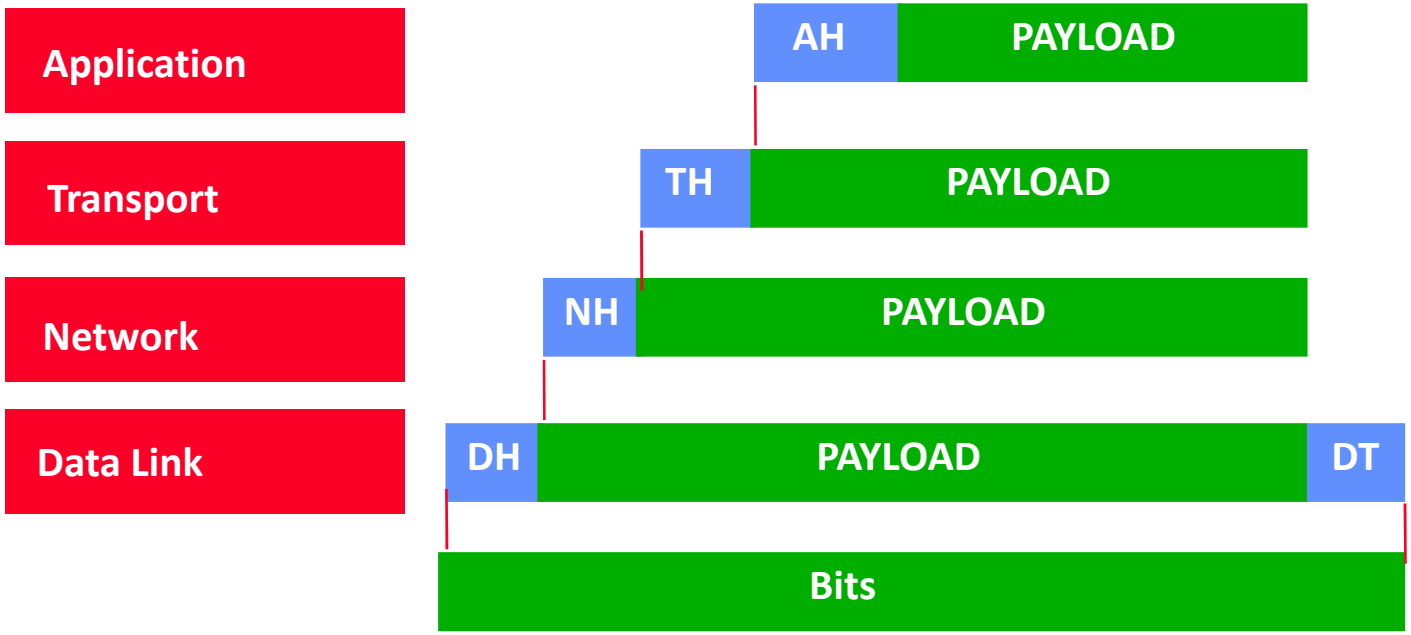
- Identity
  - Authentication: Hosts can determine the identity of the message sender
  - Authorization: Hosts can decide the operations that each authenticated user can execute in the system
- Confidentiality
  - Only the intended message recipient can access it
- Integrity
  - Any modification of the original message can be detected
- Availability
  - The system will be available whenever is needed

Open System Interconnection



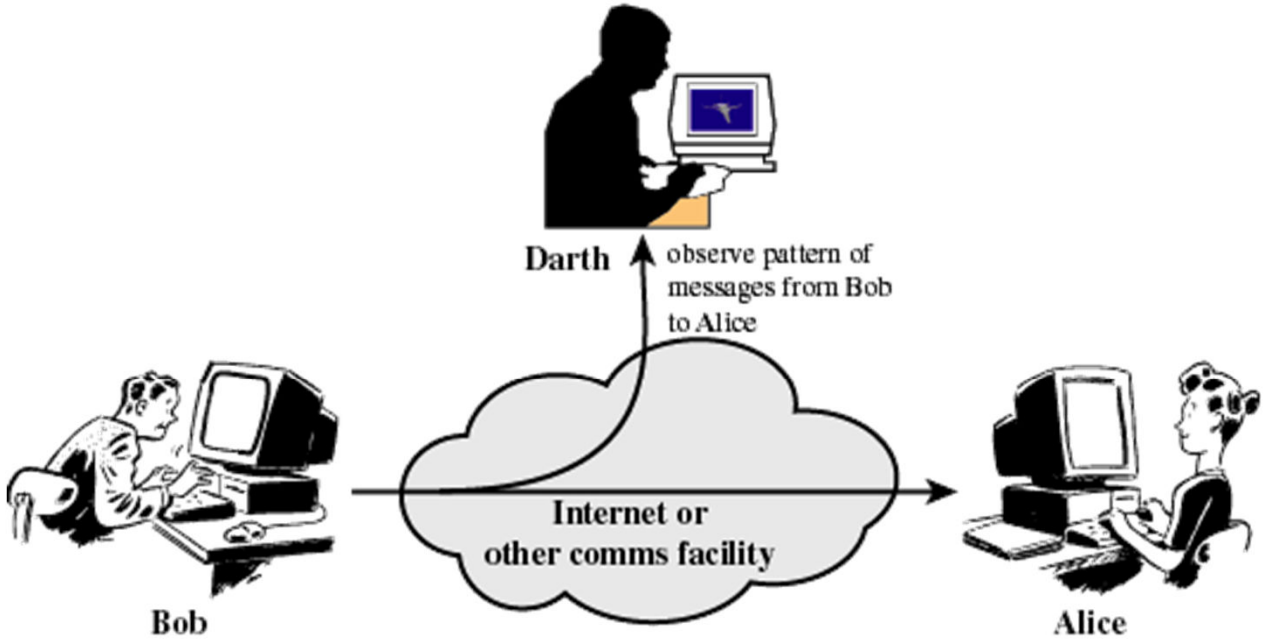
Network messages

- Each layer and protocol
  - Exposes **information**
  - Exposes **functionality**
- Seemingly secure functionality at layer 2 could enable attacks at layer 3
- Sophisticated attacks often exploit multiple layers...



Passive Attacks

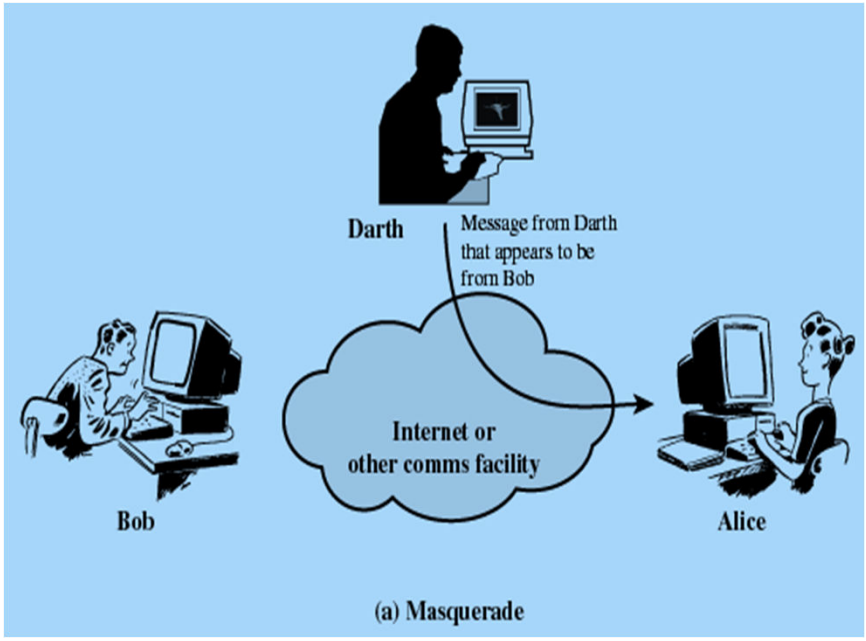
- Release of message contents - a telephone conversation, an electronic mail message, a transferred file, etc.
- Traffic analysis - encryption can mask the contents but message size, transmission frequency, location and id of communicating hosts can still be extracted

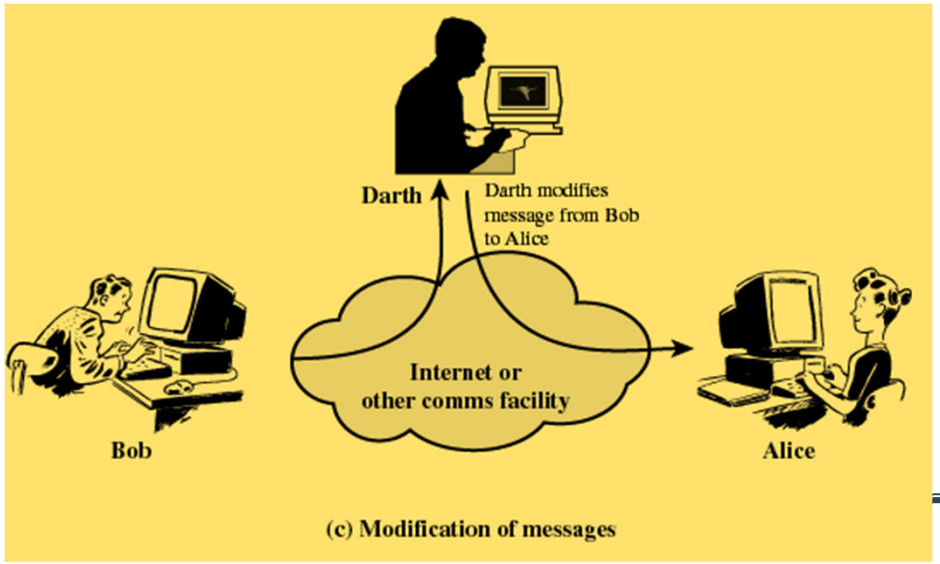


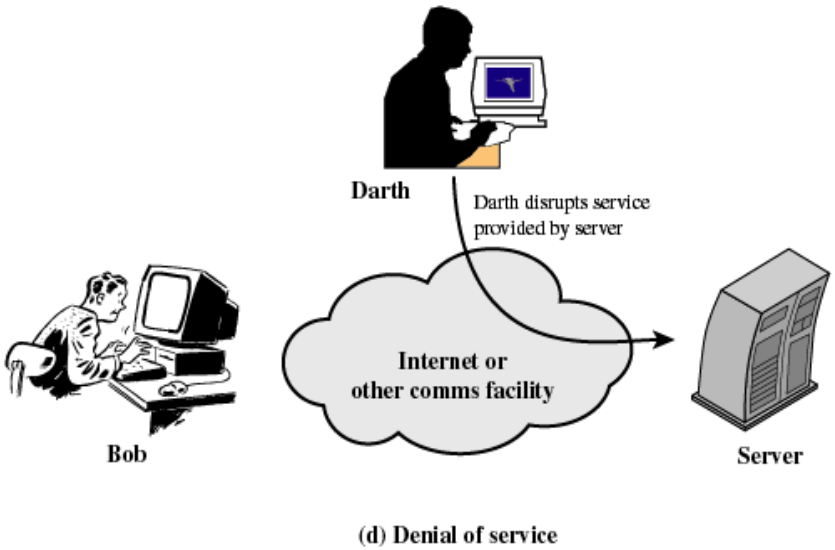
(b) Traffic analysis

Active Attacks

- ***Replay*** : passive capture of a data unit and its retransmission to produce an unauthorized effect
- ***Masquerade*** : one entity pretends to be a different entity (e.g. try to login as someone else)
- ***Modification of messages*** some portion of a legitimate message is altered, or messages are delayed or reordered
- ***Denial of service*** prevents or inhibits the normal use or management of communications facilities (Disable or overload with messages)







Queen Mary University of London

Contents

- Network Security
- **Security Attacks**
- Encryption, Certificates and Signatures

Application layer vulnerabilities

What could happen?

Information exposed

- Anything and everything!
- Browsing behaviour, usernames, interests

Functionality exposed

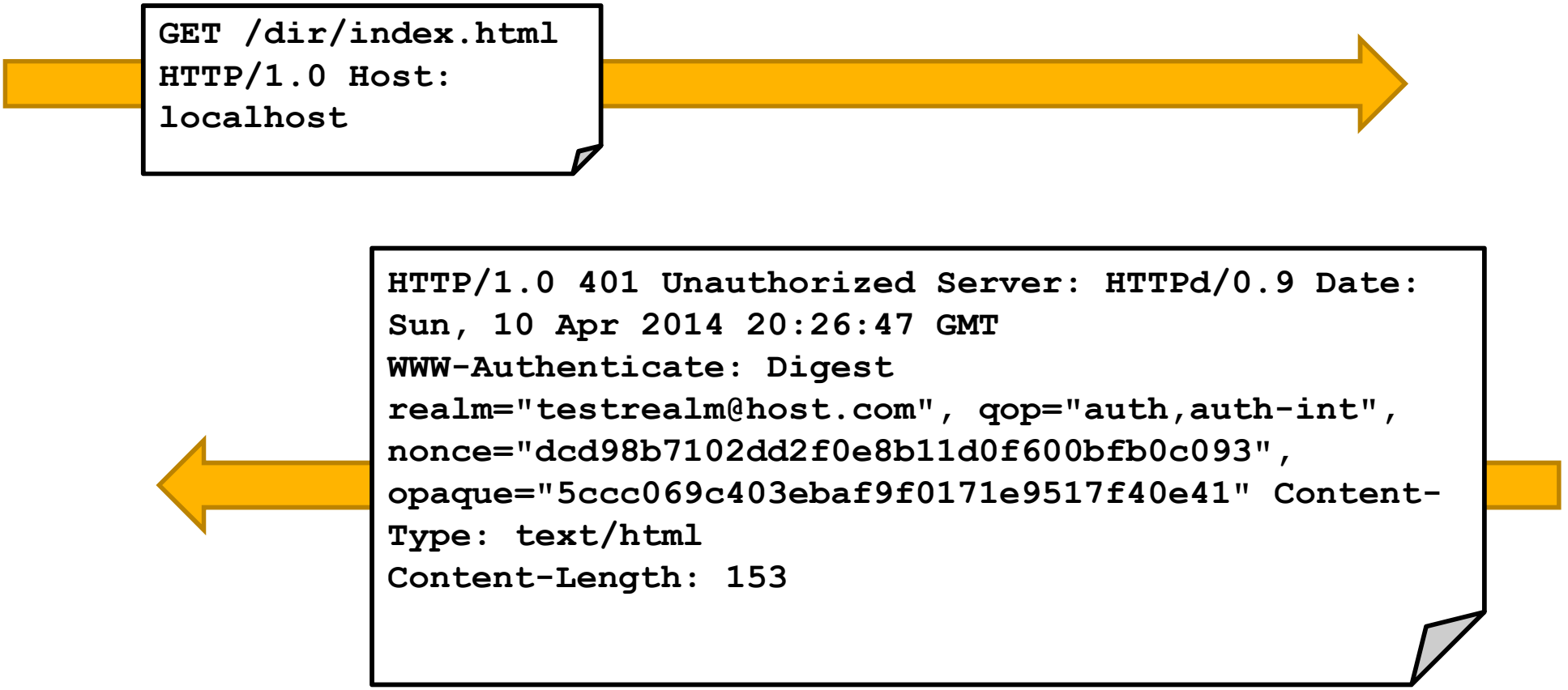
- Anything and everything!
- Sending messages, retrieving web pages etc.

What attacks could happen?

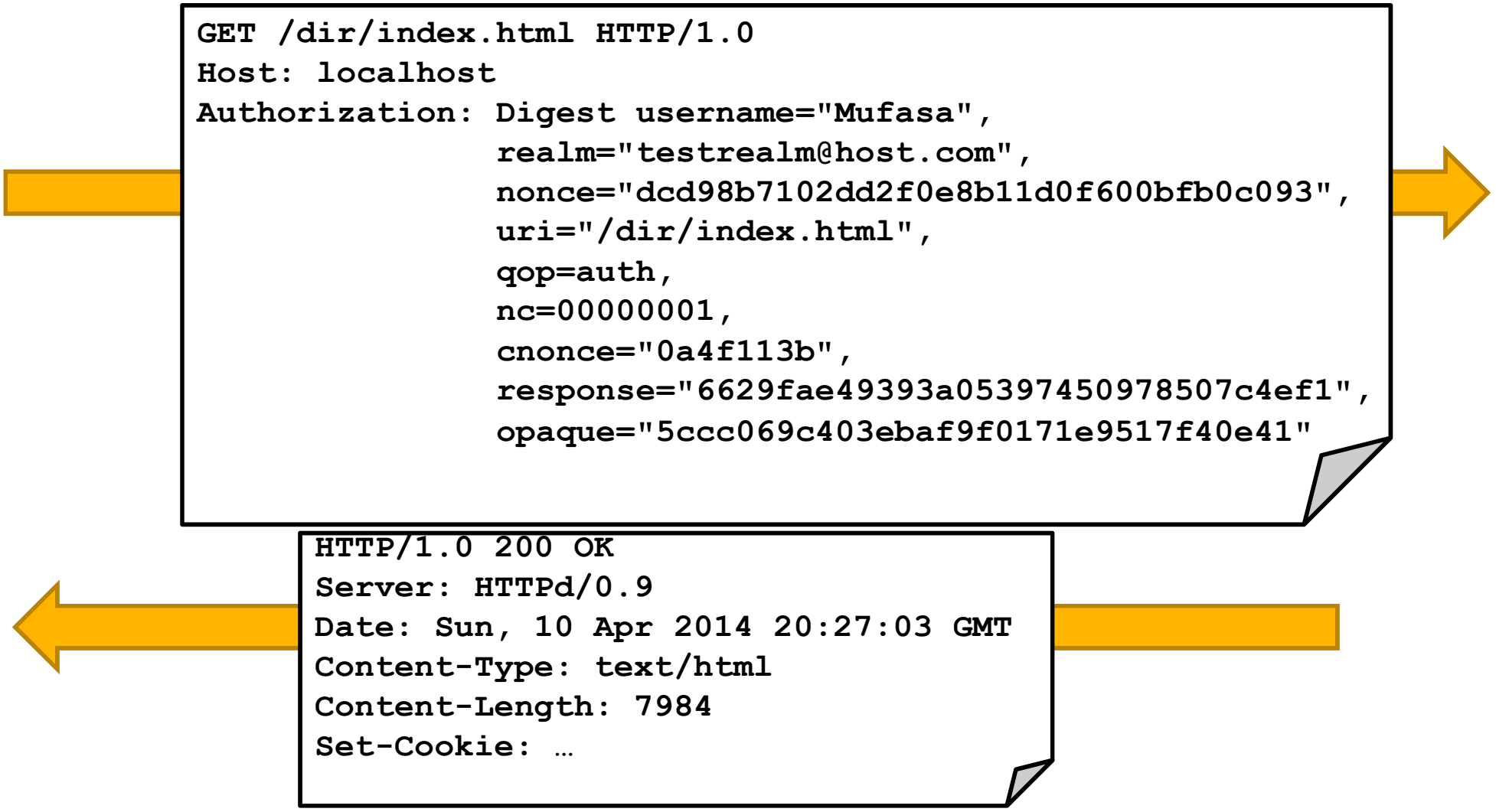
HTTP Authentication

- HTTP has multiple methods for user authentication
- 401 response code for unauthorized requests
- Most secure one is DIGEST
  - Server sends a nonce to be included in hashing
  - Client hashes user, password, domain, request and nonce
  - Server can check identity by recomputing MD5 hash
  - Client passwords can be stored in a hashed form in the server
- Session cookies can be used after authentication

Unauthorized Access to HTTP Server



HTTP Digest Authentication

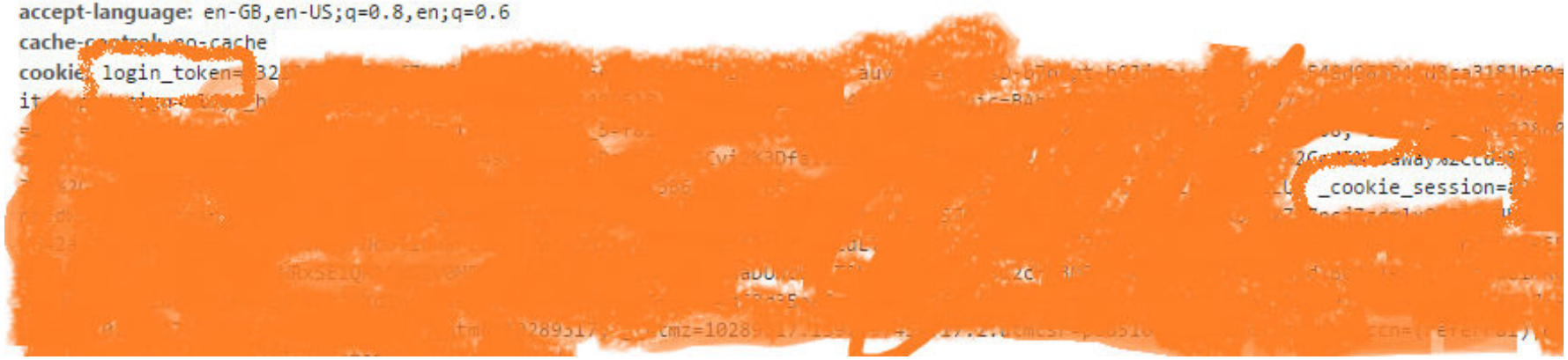


Limitations of pure HTTP Authentication

- Messages are sent in plain text
  - Usernames are visible
  - Cookies contain potentially sensible information
    - Session sniffing, man-in-the-middle attacks

HTTP attacks

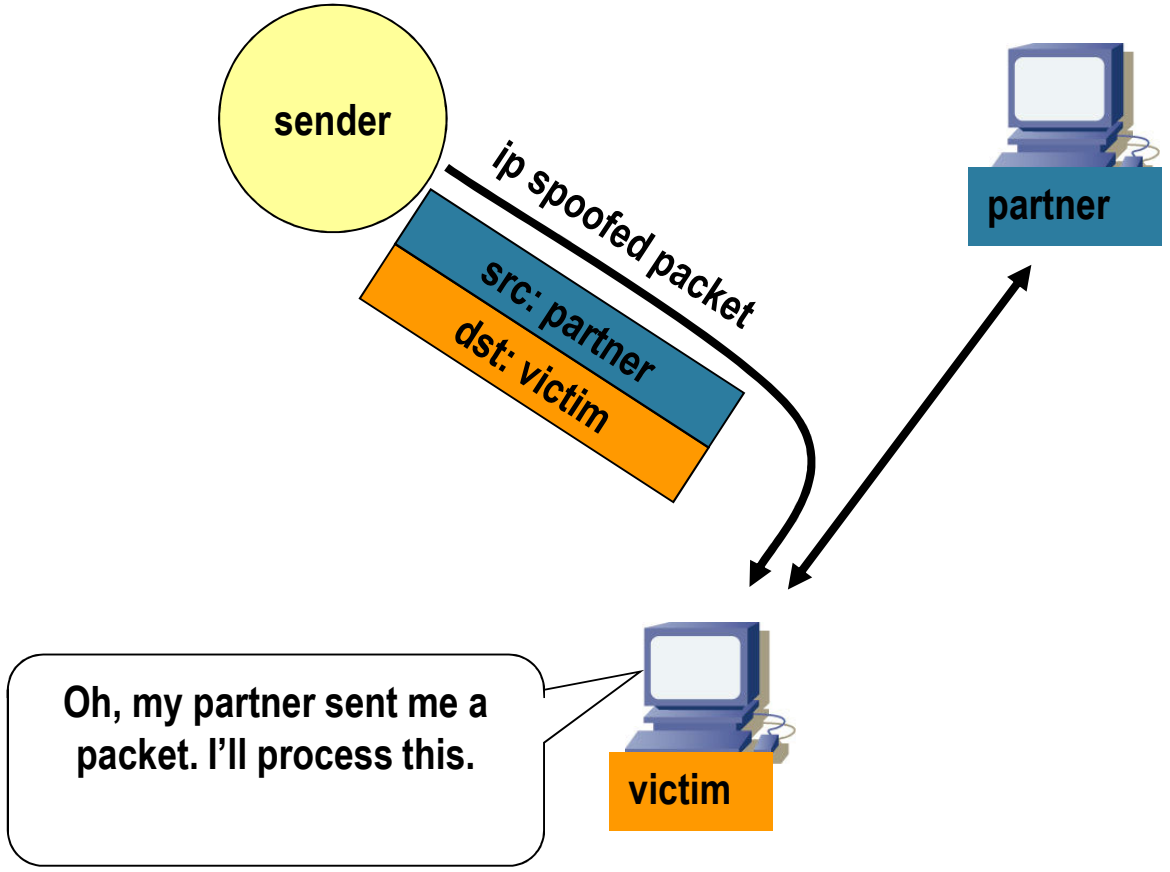
Remote Address: 54.195.140.6:443
Request URL: https://qmul.academia.edu/GarethTyson
Request Method: GET
Status Code: 200 OK
Request Headers
:host: qmul.academia.edu
:method: GET
:path: /GarethTyson
:scheme: https
:version: HTTP/1.1
accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
accept-encoding: gzip,deflate
accept-language: en-GB,en-US;q=0.8,en;q=0.6
cache-control: no-cache
cookie: login_token=



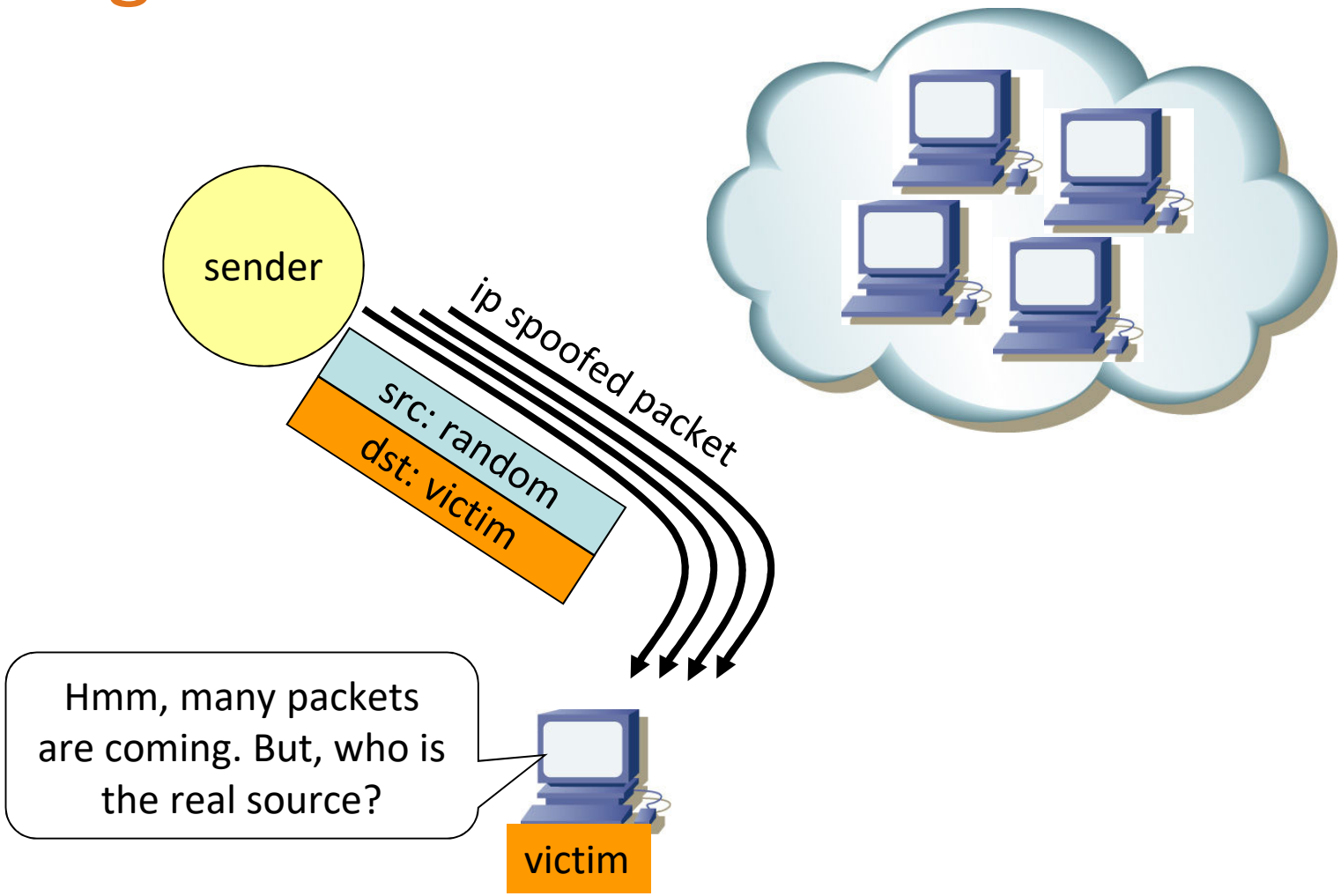
IP spoofing

- IP packets whose source is not the IP address in the source IP field
- Purposes:
  - Impersonation, e.g., session hijack or reset, man in the middle
  - Hiding, e.g., DDoS/flooding attack
  - Reflection, e.g., DNS reflection/amplification attack

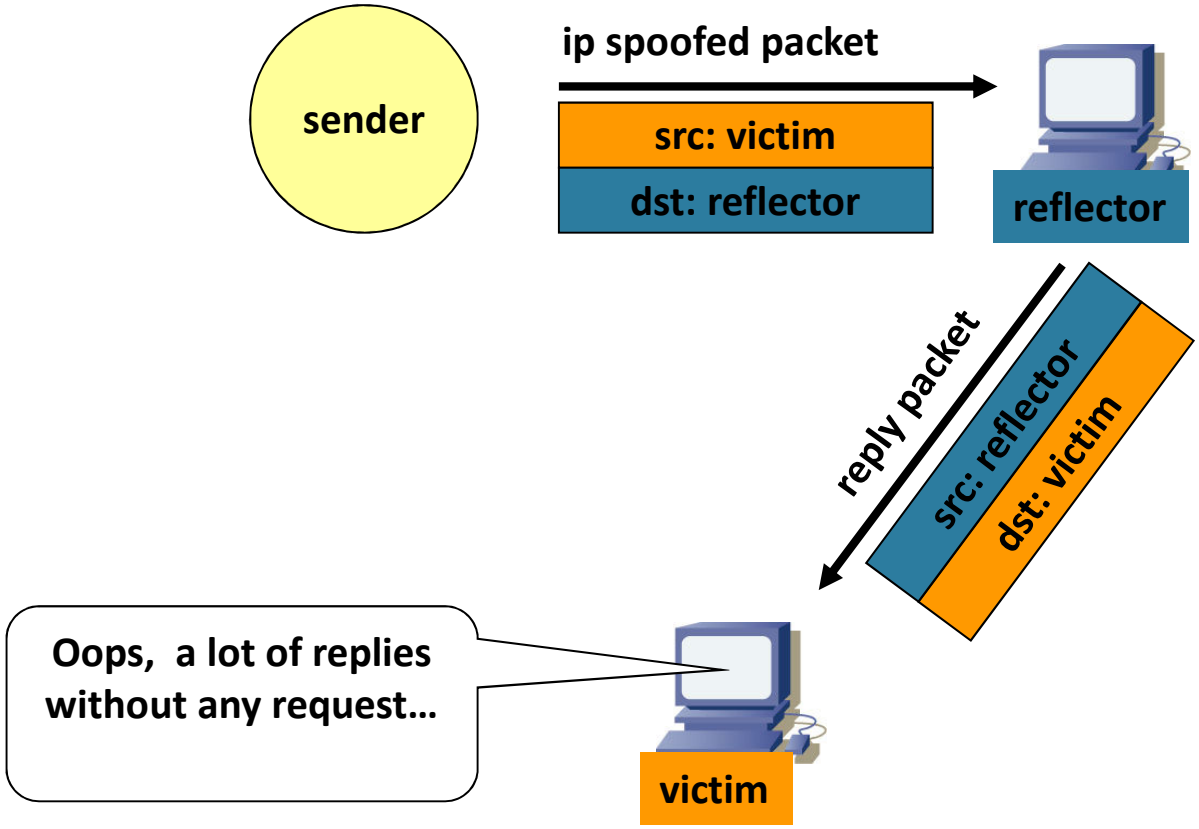
Impersonation



Hiding


sender
ip spoofed packet
src: random
dst: victim
Hmm, many packets are coming. But, who is the real source?
victim

Reflection

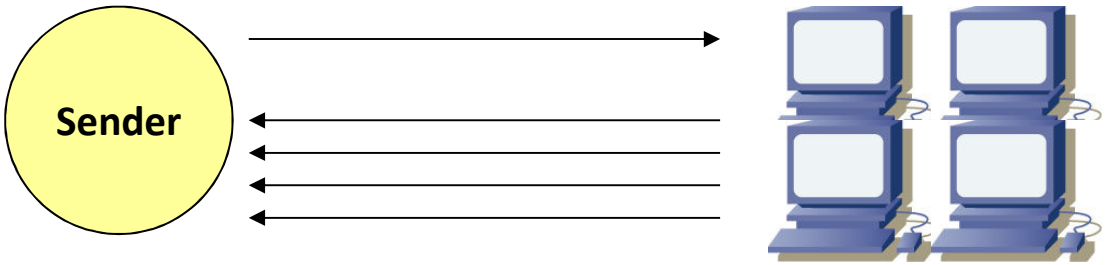

sender
ip spoofed packet
src: victim
dst: reflector
reflector
reply packet
src: reflector
dst: victim
Oops, a lot of replies without any request…
victim

Reflection/amplification attacks

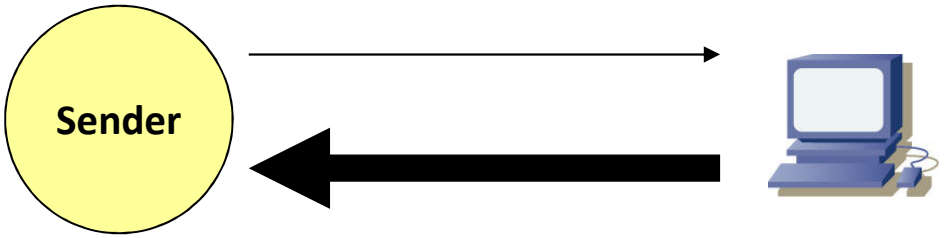
- Smurf attacks
  - ICMP echo (ping)
  - IP spoofing (reflection)
  - Amplification (multiple replies)
- DNS amplification attacks
  - DNS query
  - IP spoofing(reflection)
  - Amplification (larger reply/multiple replies)

Amplification

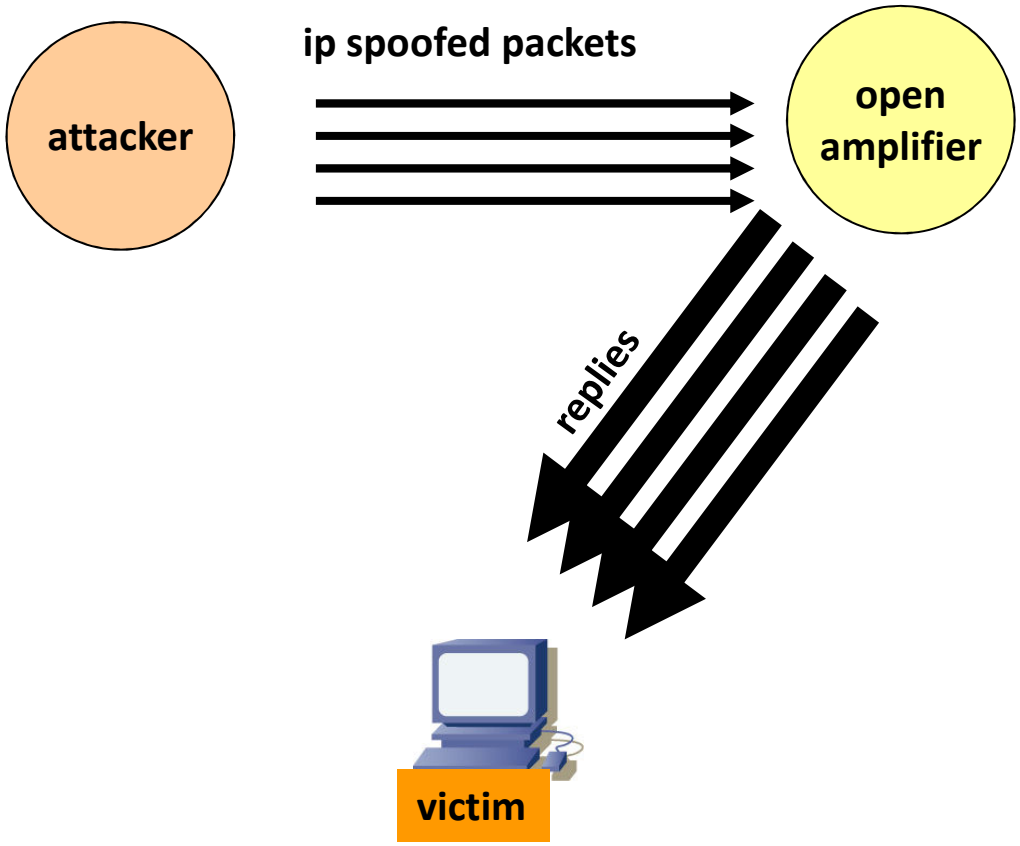
1. **multiple replies**



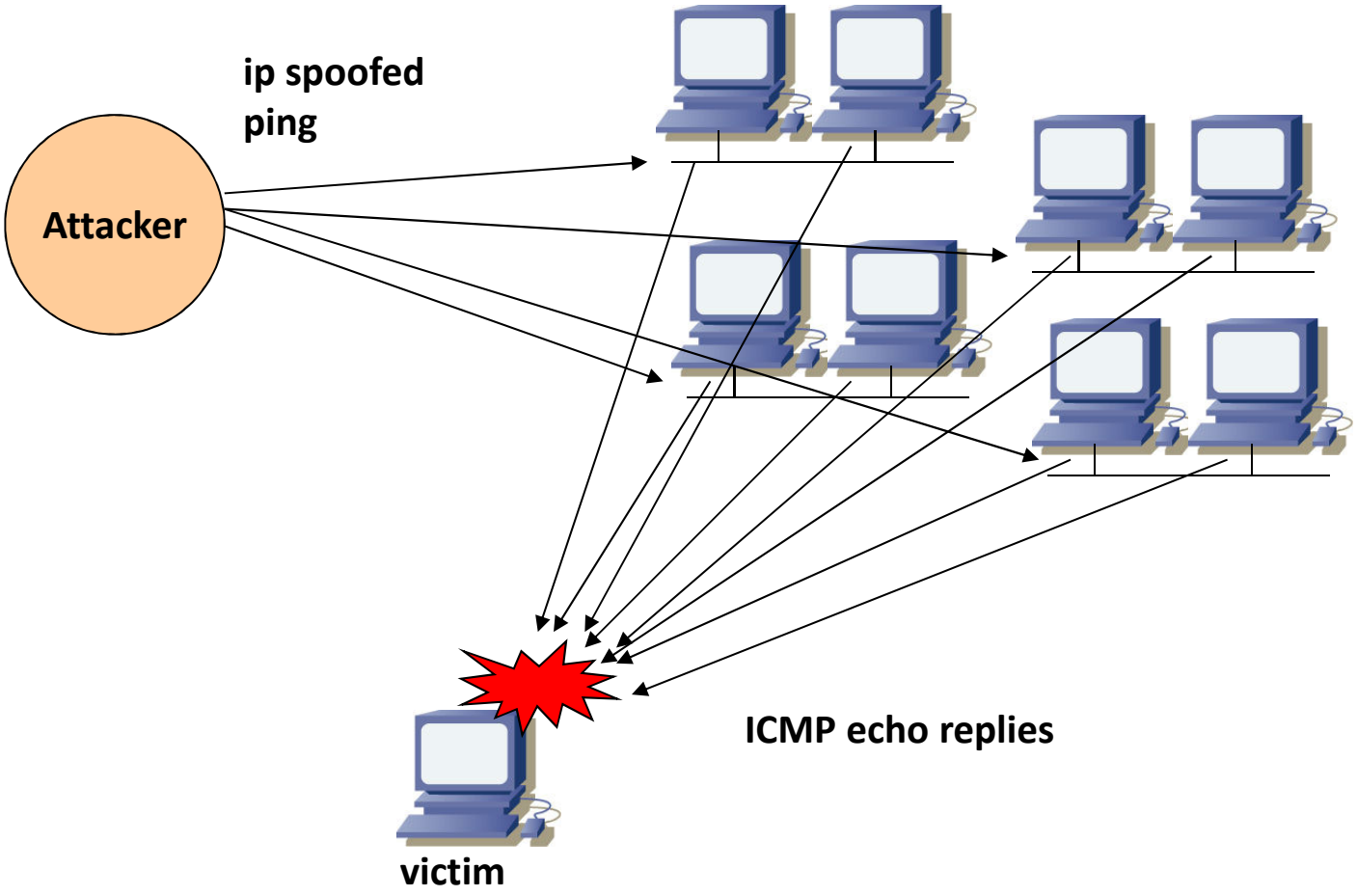
2. **larger reply**



Reflection attack



Smurf attack



Smurf attack

KASPERSKY lab | United States | Free Virus Scan | Free Trials | Sea

PRODUCTS & SERVICES | STORE | INTERNET SECURITY CENTER | DOWNLOADS | SUPPORT

SECURITY FOR HOME | SECURITY FOR BUSINESS

Home → Internet Security Center → Definitions → What is Social Engineering?

Internet Security Center

- Internet Safety
- Internet Security Threats
- Internet Security Infographics
- **Internet Security Definitions**

  All Definitions

What is a Smurf Attack? ((\ˈsmərf\ \ə-ˈtak\))

SECURITY DEFINITION

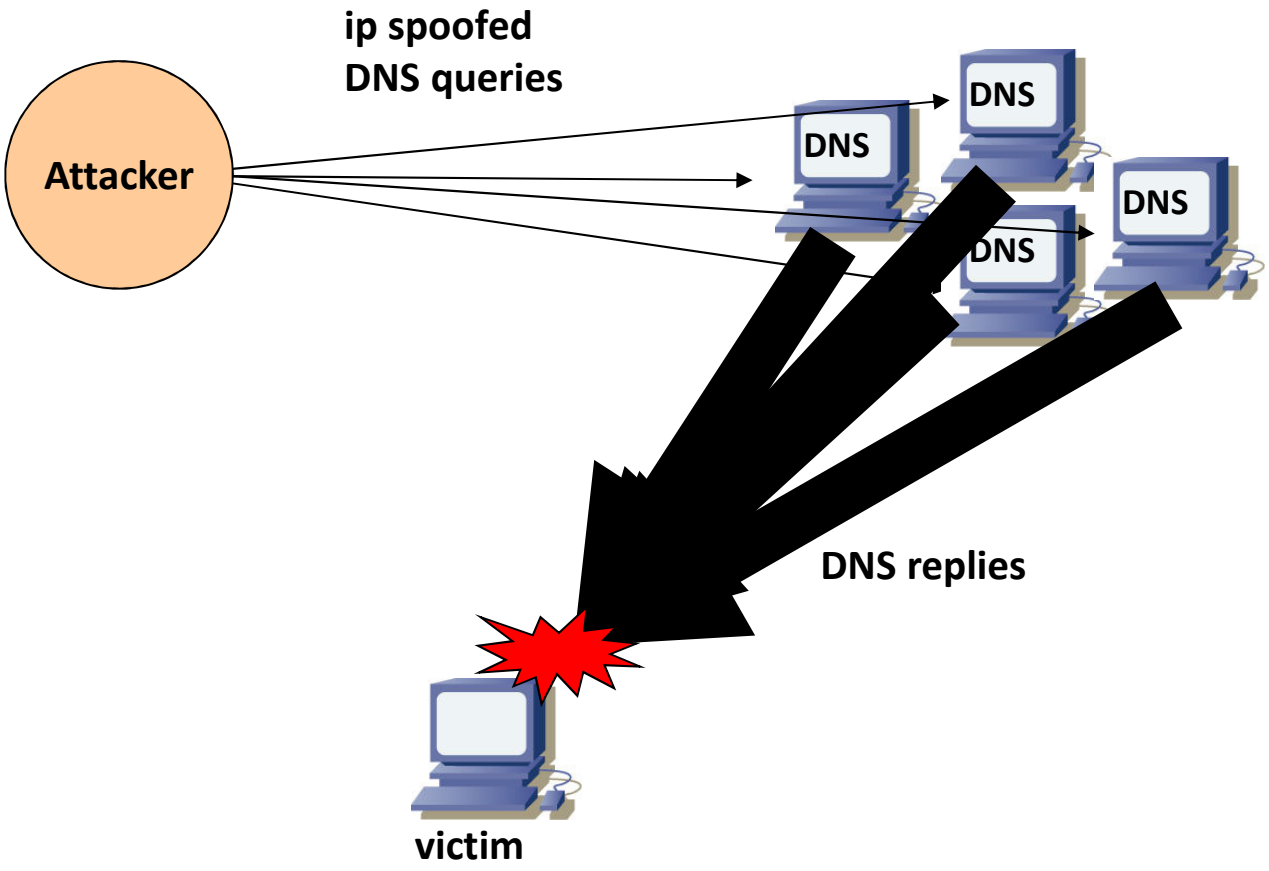
A Smurf attack is a form of a distributed denial of service (DDoS) attack that renders computer networks inoperable. The Smurf program accomplishes this by exploiting vulnerabilities of the Internet Protocol (IP) and Internet Control Message Protocols (ICMP).

The steps in a Smurf attack are as follows:

- First, the malware creates a network packet attached to a false IP address — a technique known as "spoofing."
- Inside the packet is an ICMP ping message, asking network nodes that receive the packet to send back a reply
- These replies, or "echoes," are then sent back to network IP addresses again, setting up an infinite loop.

When combined with IP broadcasting — which sends the malicious packet to every IP address in a network — the Smurf attack can quickly cause a complete denial of service.

DNS reflection/amplification attack



DNS reflection/amplification attack

Deep Inside a DNS Amplification DDoS Attack

30 Oct 2012 by Matthew Prince.

A few weeks ago I wrote about DNS Amplification Attacks. These attacks are some of the largest, as measured by the number of Gigabits per second (Gbps), that we see directed toward our network. For the last three weeks, one persistent attacker has been sending at least 20Gbps twenty-four hours a day as an attack against one of our customers.

CloudFlare blog

Contact our team

US callers
1 (888) 99-FLARE
UK callers
+44 (0)20 3514 6970
International callers
+1 (650) 319-8930

Full feature list and plan types

CloudFlare provides performance and security for any website. More than 2 million websites use CloudFlare.

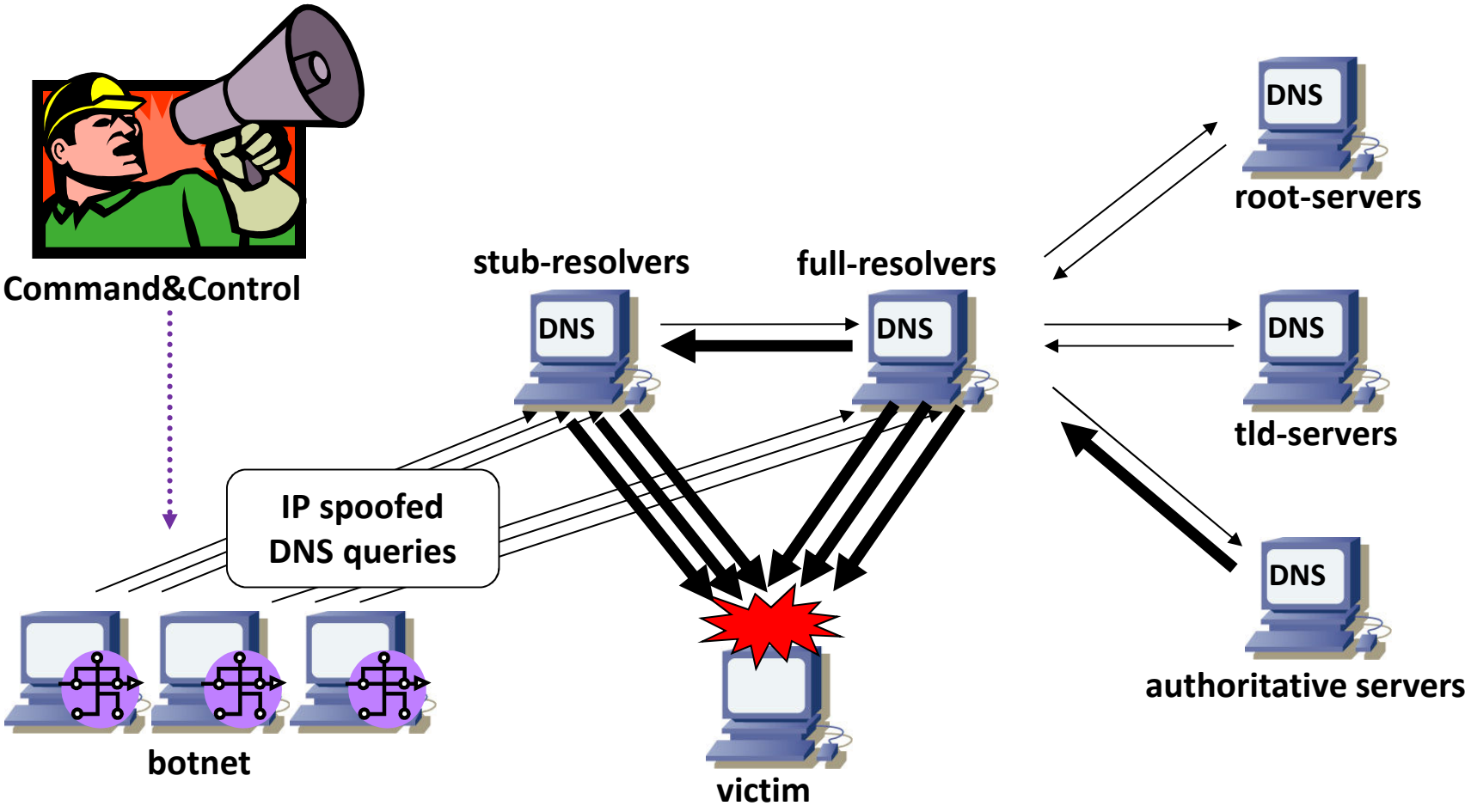
There is no hardware or software. CloudFlare works at the DNS level. It takes only 5 minutes to sign up. To learn more, please visit our website

CloudFlare features

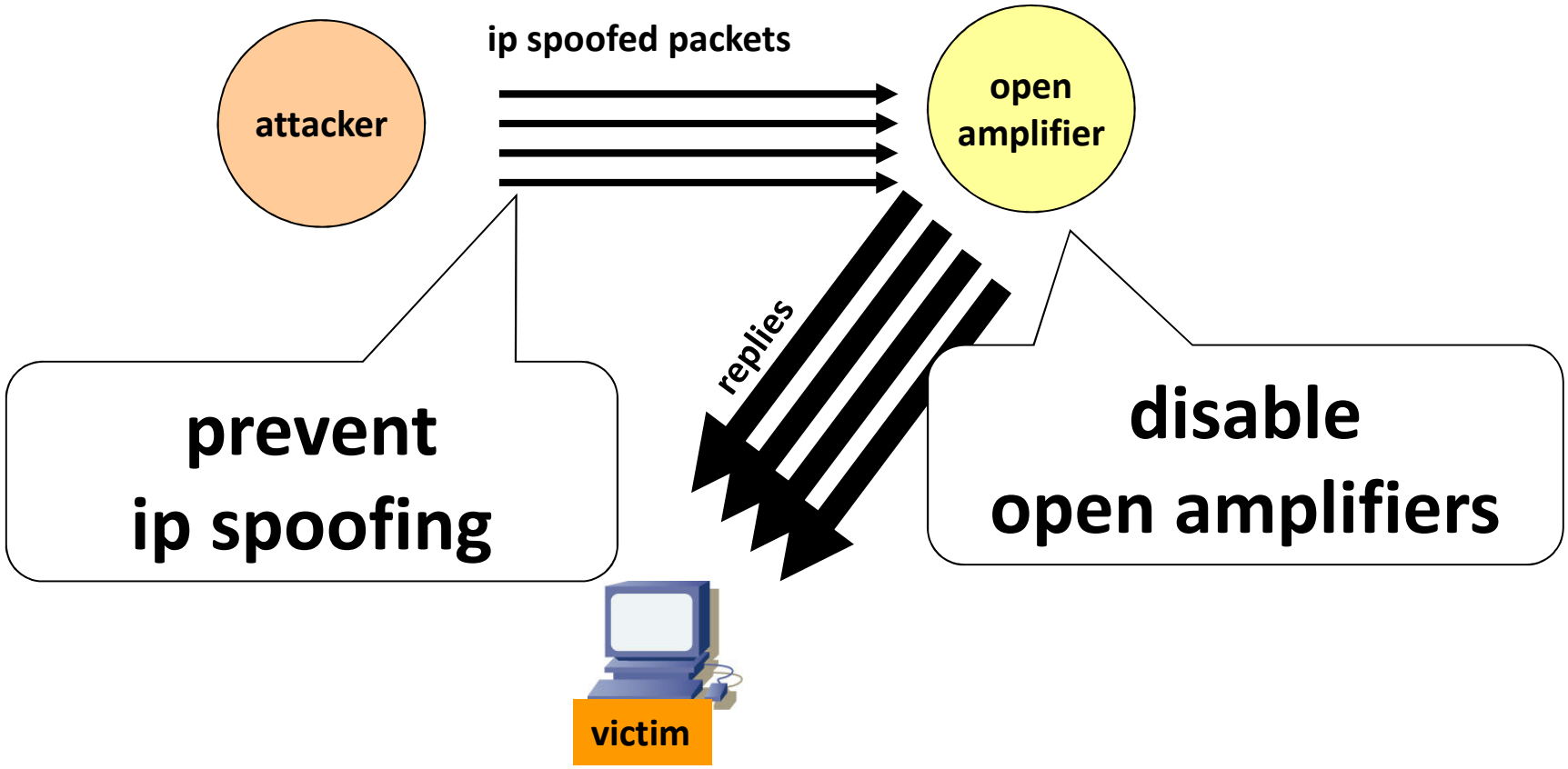
Overview

CDN

DNS amplification attack: details



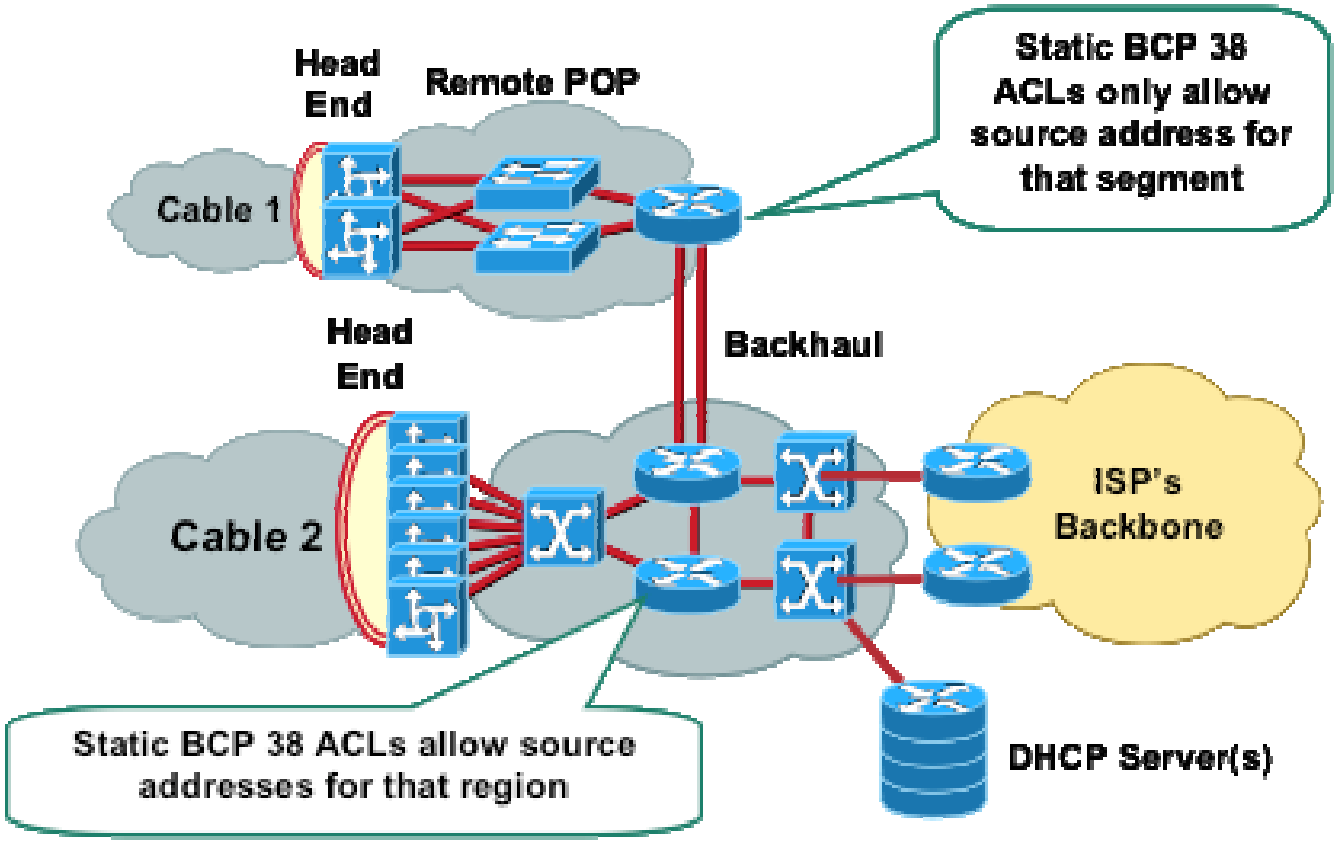
Solutions for reflection/amplification attacks



Solutions for reflection/amplification attacks

- Prevent IP spoofing
  - Source address validation, e.g., BCP38 & BCP84
- Disable open amplifier
  - E.g., open recursive DNS servers
    - DNS system should accept queries from everyone, but resolvers should be only usable by “customers”

BCP38


Head End
Remote POP
Static BCP 38 ACLs only allow source address for that segment
Cable 1
Head End
Backhaul
Cable 2
ISP's Backbone
Static BCP 38 ACLs allow source addresses for that region
DHCP Server(s)

Queen Mary University of London

Contents

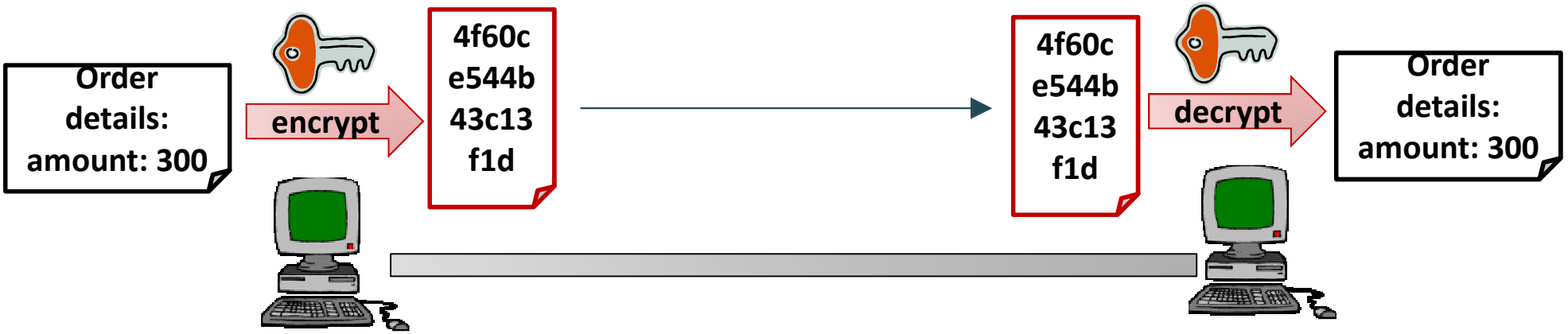
- Network Security
- Security Attacks
- **Encryption, Certificates and Signatures**

Base Security Primitives

- Encryption: encodes messages with a key. The key is required to retrieve the original message
  - Helps with confidentiality
  - Two main types of algorithms: symmetrical and asymmetrical
- Hashing: creates a digest of the message.

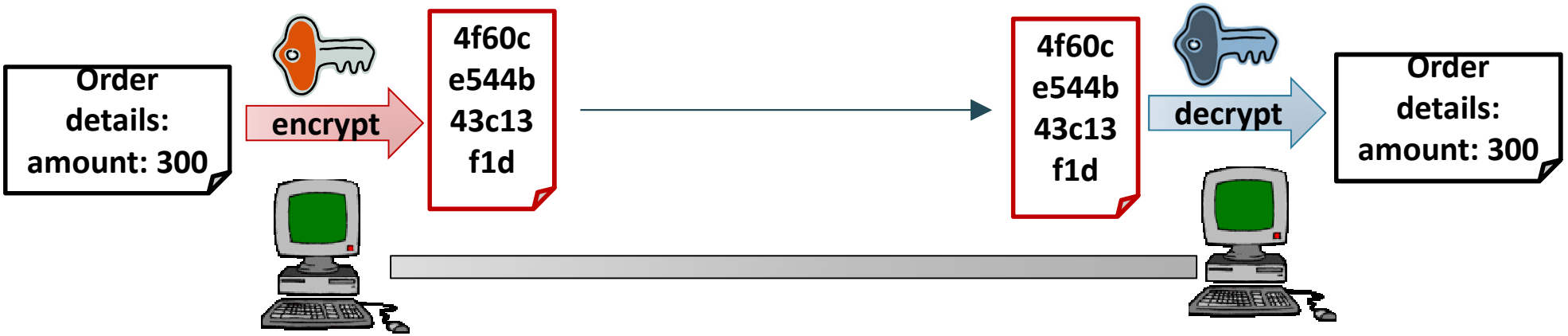
Symmetric cryptography

- AKA single key, or shared secret key encryption
  - Same key for encryption and decryption
  - Examples: RC4, DES, triple-DES
- Efficient to compute
  - Works with high volume of information



Asymmetric cryptography

- AKA as dual key, public key cryptography
  - Different keys for encrypting and decrypting
  - Example RSA,DSA
- Expensive computation
  - Limited amount of information



Management of keys

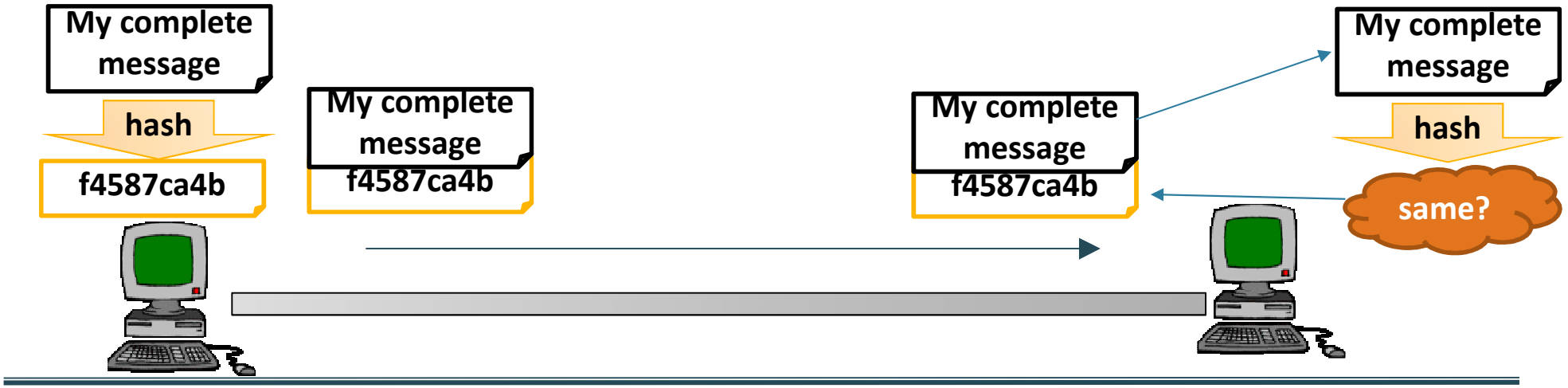
- Symmetric cryptography needs to have the same key shared by both sender/receiver
  - How can the key be exchanged?
- Asymmetric cryptography needs the receiver to have a key to decrypt the sent message
  - But different to the one used to encrypt it
  - Easier to manage… but less efficient
- Approach: use asymmetric encryption to share a symmetric key

Key management

- In asymmetric encryption algorithms a pair of keys is generated at the same time
  - The private key is NEVER SHARED with anyone else
  - The public key can be publicly advertised
- Certificates contain
  - public key
  - identity associated with public key
  - digital signature on certificate contents (by trusted 3rd party)
- Examples: X.509v3 certs, PGP certs

Message hashing

- Takes original data (any length) and computes fixed-length hash code
  - different data means different hash code
  - can't recover data from hash code
  - Examples: MD5 (128-bit hash code), SHA-1 (160-bit hash code)
- Allows to check the original message has been



Digital signatures

- A digital signature is an encrypted hash of a message
  1. compute hash code from original data
  2. encrypt hash code using signer's *private* key
- Receiver can verify digital signature
  1. decrypt hash code using signer's *public* key
  2. compute second copy of hash code from copy of original data
  3. two copies of hash code should match
- Digital signatures allow to verify both message integrity and identity of the sender
  - No match means data was altered *or* signer is imposter *or* using wrong public key

What Can SSL Do?

- SSL: Secure Sockets Layer
- SSL uses TCP/IP on behalf of the higher-level protocols
- Allows an SSL-enabled server to authenticate itself to an SSL-enabled client
- Allows the client to authenticate itself to the server
- Allows both machines to establish an encrypted connection.

Queen Mary
University of London

Security Properties provided by SSL

- Server authentication
- Client authentication (optional)
- Encrypted SSL connection for confidentiality
- Integrity.

Security Certificates

A certificate has the following content:

1. The certificate issuer's name
2. The entity for whom the certificate is being issued (aka the subject)
3. The public key of the subject
4. Some time stamps

How does SSL Work?

- The SSL protocol uses RSA public key cryptography for Internet Security
- Public key encryption uses a pair of asymmetric keys for encryption and decryption
- Each pair of keys consists of a public key and a private key. The public key is made public by distributing it widely; the private key is always kept secret
- Data encrypted with the public key can be decrypted only with the private key, and vice versa