

DNS and DNS Rebinding in IoT

Frank Walsh

Context: Local Home Networks



Growing number of devices connecting to home WiFi networks

Phones, laptops, TVs, smart devices



Some devices offer limited security/authentication:

Trust other devices on network

Assumption that router firewall will protect from external threat

Push to bring IoT products to market can reduce attention to security.



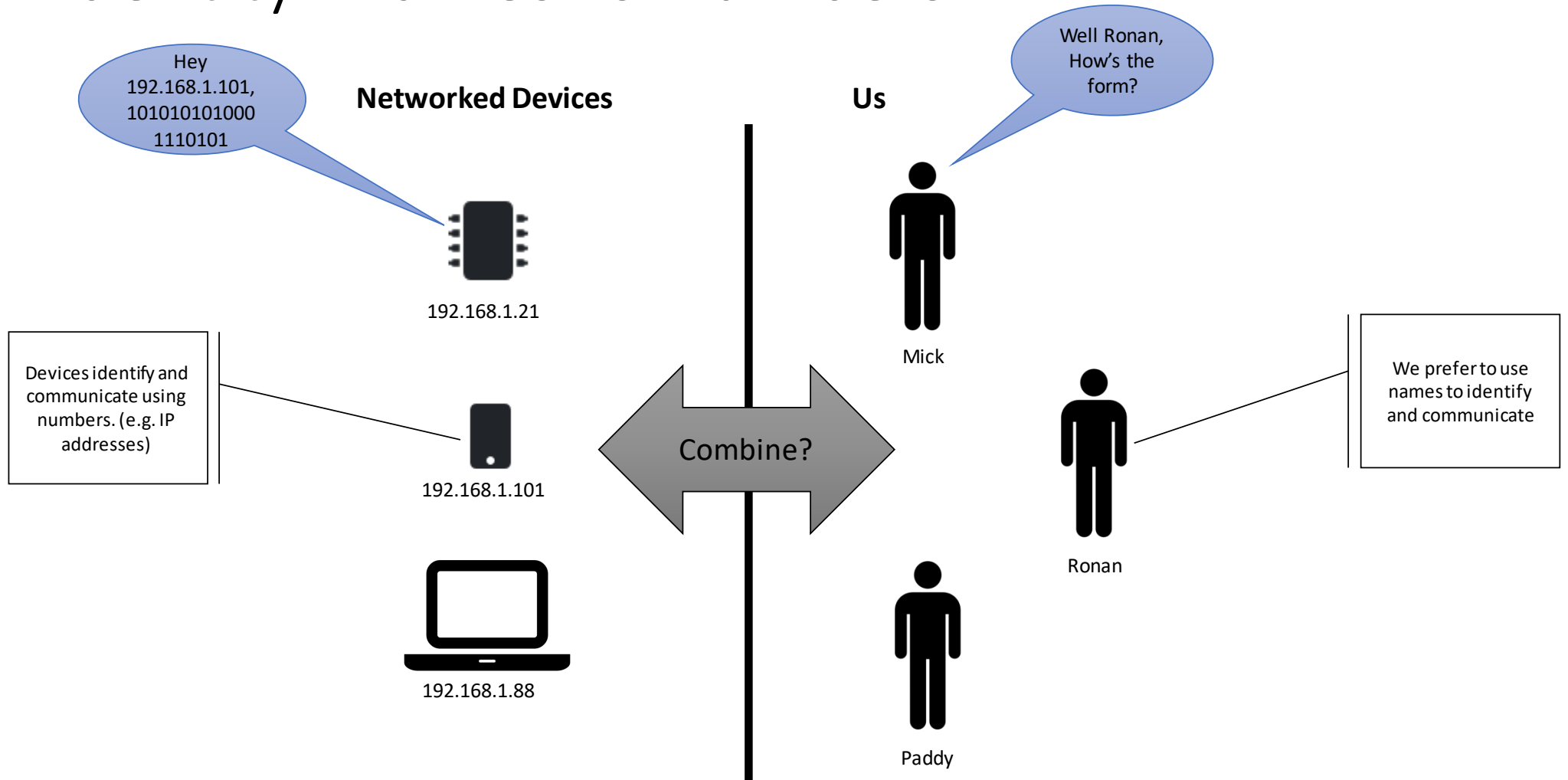
Assumption that “local home networks” are safe.



Internal smart devices are potentially vulnerable to “**DNS Rebinding attack**”

So how does DNS work....

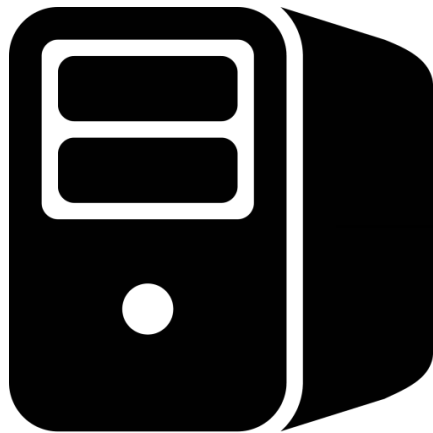
Identity: Names vs Numbers



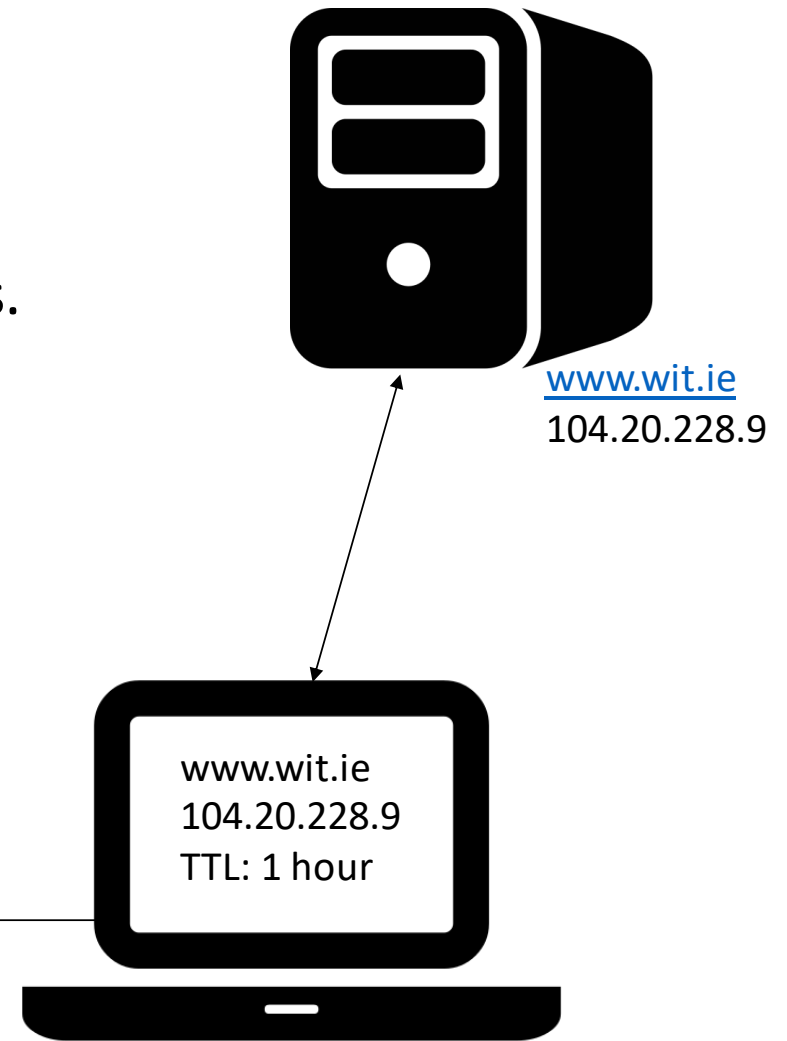
Domain Name System(DNS)

- DNS resolves Domain Names to IP addresses.
- Analogy: Phone book

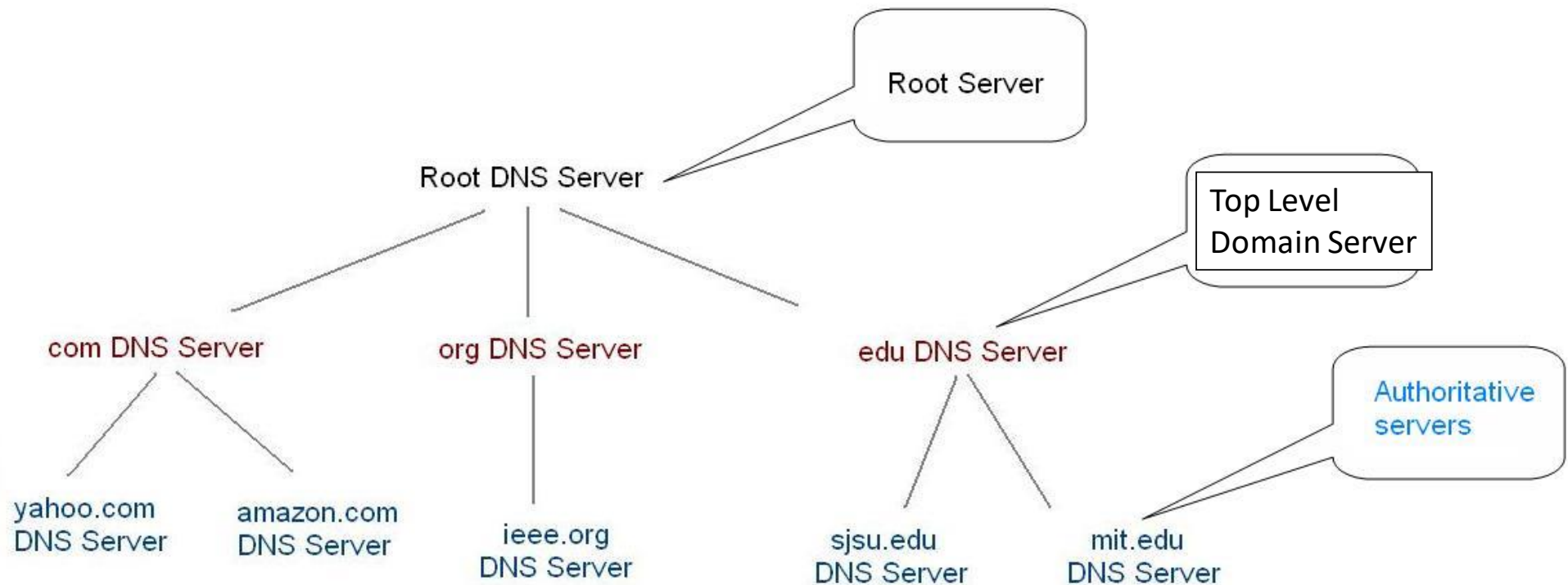
Domain Name	IP
www.wit.ie	104.20.228.9
www.google.ie	145.12.45.76
www.aib.ie	115.66.66.66



DNS Server

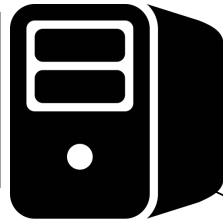


DNS Server Hierarchy



Domain Name System(DNS)

- 13 sets around the world
- Each has unique IP address



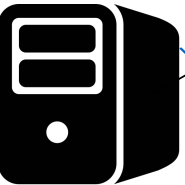
Root Server

TLD: 105.23.65.34



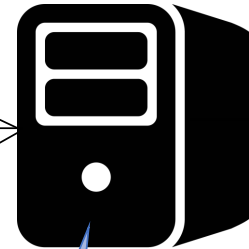
Top Level Domain Server

ANS: 105.23.65.34



Authoritative Name Server

www.wit.ie: 104.20.228.9



Resolver
(usually ISP assigned)

1. Root, I need IP address for www.wit.ie

2. TLD, I need IP address for www.wit.ie

3. ANS, I need IP address for www.wit.ie



www.wit.ie



www.wit.ie
104.20.228.9



- Address info for top level domains (.com .net .ie .org)

- Responsible for knowing everything about a domain