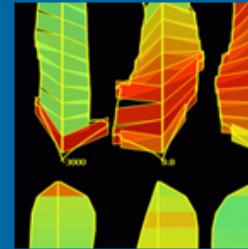
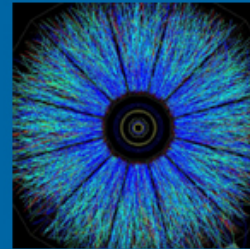
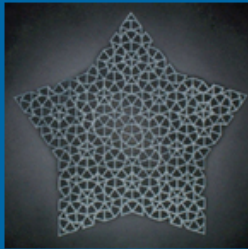




Swansea University  
Prifysgol Abertawe

# CS-130

## DNS Security and HTTPS: Patching up the Holes in the System



# NordVPN and TorGuard VPN Breaches: What You Need to Know

BY MAX EDDY 23 OCT 2019, 4:48 P.M.

*NordVPN and TorGuard VPN have suffered security breaches. Here's what happened and what it means for you (and our VPN reviews).*



After the disclosure of major security breaches at **NordVPN** and **TorGuard VPN**, we are lowering the score of NordVPN, formerly a five-star, Editors' Choice VPN service. It is now a four-star service, and will keep its Editors' Choice

award, for now. TorGuard will retain its four-star rating. I'll explain why—along with what happened—below.

The story starts months ago on the anonymous message board, 8chan, where a user bragged about having compromised NordVPN, TorGuard VPN, and a service we have not reviewed called VikingVPN. The brags went unnoticed for months until October 20th, when a Twitter storm brought the accusations against the companies into the light. That's when I found out about the incident.

## FEATURED ON PCMAG



**Best UK Broadband Deals**  
Find the best for you.



**Best VPN Services for 2019**  
A VPN, or virtual private network, is one of the smartest ways ...



**The Best VPN Deals for October 2019**

Here are the best VPN deals in October 2019: PureVPN for £2.00/month, ...

## BECOME A FAN OF PCMAG



TechRadar is supported by its audience. When you purchase through links on our site, we may earn an affiliate commission. [Learn more](#)

Home > News > VPN

# Court throws out Torguard's lawsuit against NordVPN

By Desire Athow May 29, 2019 VPN

Updated: Accusations of DDoS and much more



Image credit: Shutterstock  
(Image credit: Shutterstock)

*Editor's note: The US District Court in Orlando decided to dismiss the case against NordVPN brought by Torguard on June 10.*



**Free to Access, Read and Share**  
Build Your First Website eBook

In association with GoDaddy

Techradar Pro has teamed up with GoDaddy to produce a website-hosting tips eBook, looking at how to plan your website, picking the right domain name and great ways to promote your website.



**READ MORE TODAY ►**

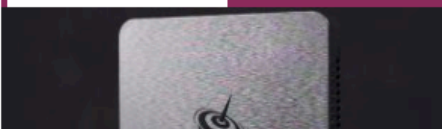
Have a read and let us know what you think. The aim is to inform and provide insight to those interested in building their first real website.

techradar.pro

Advertisement

MOST POPULAR

MOST SHARED



**1 This PC is so cheap you're kind of getting it free with Windows 10**

# Learning goals

---

How does DNS work?

Why are we moving away from DNS and what is the alternative?

What is a certification authority and how does signing work?

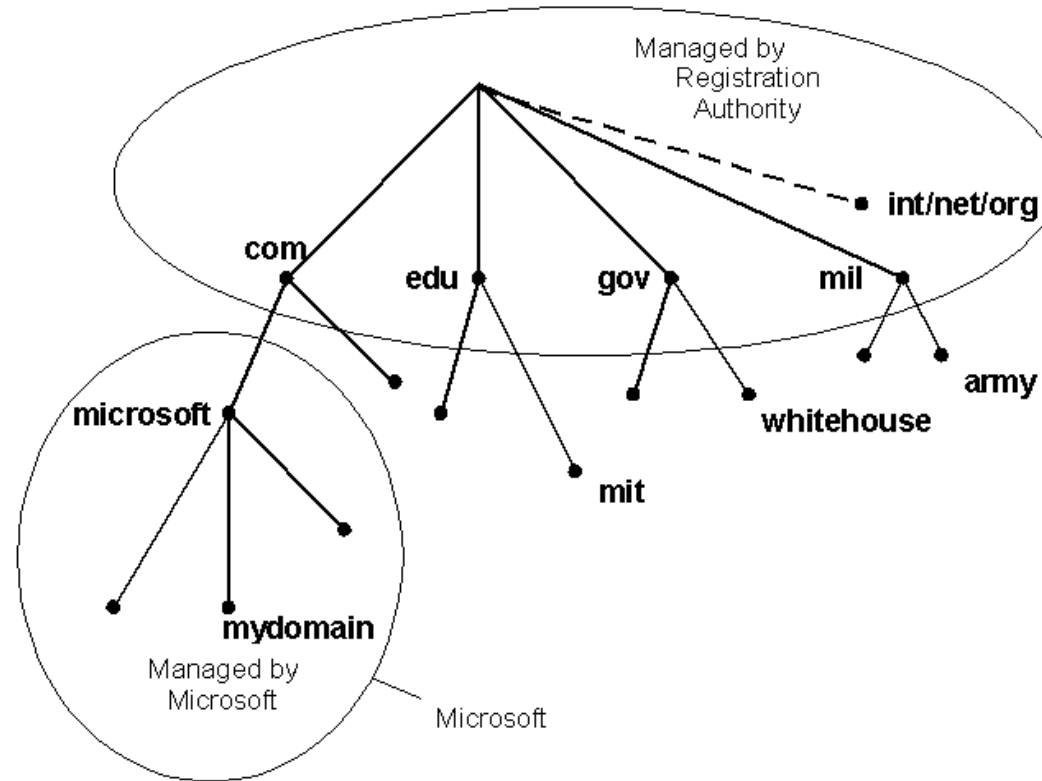
---

# How did we say Pharming attacks worked?

# DNS One more Time

Lets look at that model  
of the DNS servers  
again

*What's wrong with this  
model?*





# DNS Flaws and ???

---

There's no security or verification when connecting to a DNS server!

- This means that if you are on an unknown network (say public WiFi) and you visit a website you have no way of knowing if it's real because you might be the victim of Pharming using a ????

??? will prevent this from happening

- But ??? would make the fix unworkable as ??? demands that ISPs ??????????
  - This ?????? can't happen if DNS requests are properly secured

# DNS Flaws and SOPA

---

There's no security or verification when connecting to a DNS server!

- This means that if you are on an unknown network (say public WiFi) and you visit a website you have no way of knowing if it's real because you might be the victim of Pharming using a Man in The Middle Attack

DNS Secure (DNSSEC) will prevent this from happening

- But SOPA would make the fix unworkable as SOPA demands that ISPs redirect you if you visit a page they don't like!
  - This redirect can't happen if DNS requests are properly secured



# Mitigation: More Than One Root Server

---

ICANN does not have a monopoly over DNS root servers

- IP addresses obviously need consistent approach but mapping names to numbers can be done by anyone
- This means that ICANN is prevented from acting unilaterally

Alternative roots generally operate much more cooperatively

- Google DNS also uses DNSSEC, not all ISPs do
- Other protests against SOPA included blackout of services in 2012

# How to Switch to OpenDNS or Google DNS to Speed Up Web Browsing



Your local internet service provider probably doesn't have the fastest DNS servers, and that can slow down your browsing, since your browser needs to look up the IP address of every web site you try to view. Here is how to switch to either OpenDNS or Google DNS for faster browsing times.

This should work in Windows 7, 8, or 10 the same way.

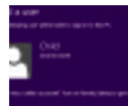
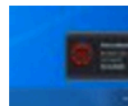
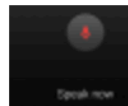
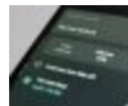
## Switching to a Better DNS Provider

The first thing we need to do is right-click on the network status notification icon and choose to Open

DID YOU

Sting sin  
single M  
clearly a  
singing '  
falsetto.

BEST OF



# One final problem...

---

We now know that DNS links a web domain to an IP address

- And we know who hands out IP address

But how do we know than someone hasn't bought an address to scam us and how do we communicate with them securely?

- IP law makes it potentially illegal which is good, as does property or contract law if they are selling goods or services
  - But that's a bit late if they are planning to take the money and run

*So what assurances can we get that a person or company is legitimately linked to their domain and how do we talk to them safely?*

# Trusted Third Parties

---

The final element of online security is the use of **Certificate Authorities** to verify that the ownership of a website is strongly linked to a company or an individual

Certificate Authorities are a set of companies that issue digital certificates that tie people or organisations to a web domain

- Passports, banking details, contracts and more can be used to verify identity much like registering a business

This system supports HTTP over SSL (or HTTPS as you know it from your browser's URL bar)

- This is another form of Public Key Encryption



# Public Key/Private Key Signing

---

1. Your browser and the website have a Key Pair
2. The websites Public Key is encrypted with the CA's Private Key
3. Very, very usefully, this can only be decrypted successfully by the CA's Public Key effectively "signing" it
4. This guarantees that a message encrypted by it can only be read by the site you want to send it to

The websites trust that most major browsers include certificate authorities public keys for validation


- This forms what we call a *Public Key Infrastructure*

# Who Are Certificate Authorities?

---


Rank	Issuer	Usage	Market share
1	Comodo	6.1%	41.0%
2	Symantec	5%	30.2%
3	GoDaddy	2.2%	13.3%
4	GlobalSign	1.7%	10.4%
5	DigiCert	0.5%	3.1%
6	StartCom	0.4%	2.2%
7	Entrust	0.1%	0.8%
8	Verizon	0.1%	0.7%
9	Trustwave	0.1%	0.6%
10	Secom	0.1%	0.6%



 <https://www.amazon.co.uk>

Click to go back, hold to see history

**amazon**.co.uk Try Prime

All 

**amazonstudent**  
in association with

Hello, S  
**Your Account**


Shop by Department ▾ S's Amazon Today's Deals Gift Cards & Top Up Sell

# Start your 30-day free trial and get FREE One-Day Delivery

**amazonPrime**

SL Hi, S On Order 0 items Amazon Prime Join Prime > Audible Membership 1 free audiobook > Customer Si 2007

Related to items you've viewed [See more](#)



Elements Console Sources Network Timeline **Security** >> 5




### Overview

Main Origin  
Reload to view details

Secure Origins

- https://www.amazon.co.uk
- https://fls-eu.amazon.com

### Security Overview

This page is secure (valid HTTPS).

- Valid Certificate**  
The connection to this site is using a valid, trusted server certificate.  
[View certificate](#)
- Secure TLS connection**  
The connection to this site is using a strong protocol version and cipher suite.
- Secure Resources**  
All resources on this page are served securely.

 **DigiCert, Inc. [US]** | <https://www.digicert.com/>

# The Flaw in the System: The DigiNotar Hack

---

DigiNotar were a Dutch CA with full Certificate Signing privileges

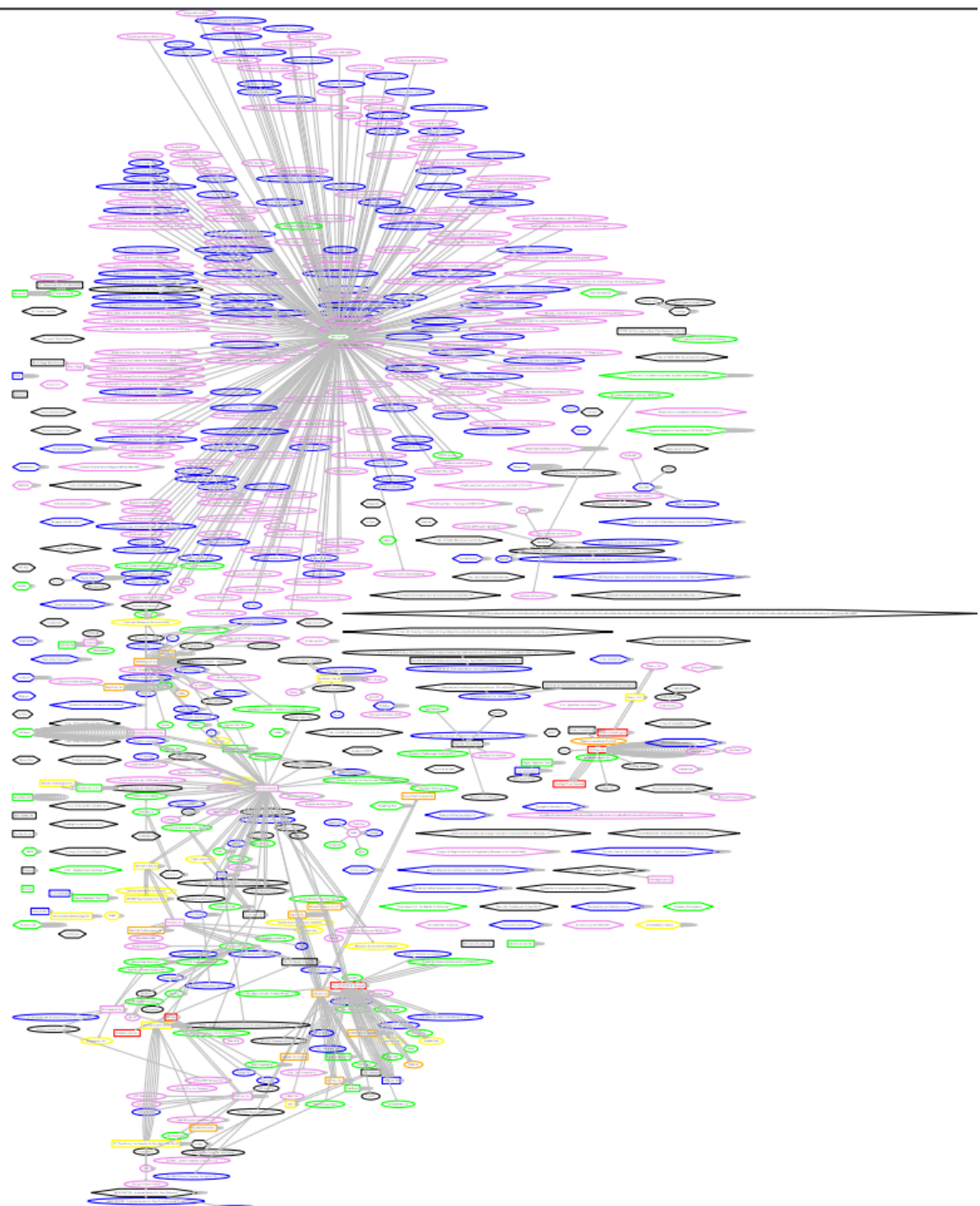
In 2011, DigiNotar were hacked due to a combination of out of date security software, lax security practices and poor network design

- As a result, their private key was stolen meaning that the thieves could sign their own fake security certificates

The hack was exploited in two ways

- Used to run a man-in-the-middle intercept attack on (primarily) Iranian email accounts affecting 300,000 users
- Attempted to verify and upload code to Google's android system but fortunately this failed

Highlights a weakness of the current security arrangements we have..



# Wider Reading and Activities

---

**Required: visit <https://haveibeenpwned.com/>**

- To see if any of your personal information might have been compromised in the past

**YouTube: This Video Is Sponsored By  VPN**

- A breakdown of what a VPN does and does not do

**Podcast: The Vergecast: Amber Baldet on what blockchain technology can do for us beyond encryption**

- Interview with the CEO of Clovyr, a Blockchain development ecosystem

**Podcast: Reset: Quantum Supremacy, WTF?**

- A quick look into what Google's recent claim to have achieved quantum supremacy really means

# Learning goals revisited

---

How does DNS work?

Why are we moving away from DNS and what is the alternative?

What is a certification authority and how does signing work?

# Learning goals revisited

---

## How does DNS work?

DNS is a networked, hierarchical lookup that resolves an IP address which is vital

## Why are we moving away from DNS and what is the alternative?

DNS is vulnerable to Man In The Middle attacks so we are moving towards using DNSSEC

## What is a certification authority and how does signing work?

A group delegated trust ultimately by the US government to test the identity of people and confirm they are the owner of a public key by encrypting it with their private key