# Security and Authentication in IP

Encryption is just a small part in making a system secure as there are many other factors

# Security and Authentication in IP

Encryption is just a small part in making a system secure as there are many other factors

Human factors are very important: we mustn't forget social engineering attacks

# Security and Authentication in IP

Encryption is just a small part in making a system secure as there are many other factors

Human factors are very important: we mustn’t forget social engineering attacks

Also, there is no point in having a military-grade encryption system if you have an easily-guessable password

# Security and Authentication in IP

There are actually two problems to address:

- Secrecy
- Authentication

# Security and Authentication in IP

There are actually two problems to address:

- Secrecy
- Authentication

Secrecy is familiar, but authentication is more fundamental

# Security and Authentication in IP

Secrecy is

> *make sure that this data is not readable by anyone other than the recipient*

# Security and Authentication in IP

Secrecy is

> *make sure that this data is not readable by anyone other than the recipient*

Authentication is

> *make sure the recipient is who I think they are*

# Security and Authentication in IP

There is no point sending a strongly encrypted message only to find you sent it to the wrong person

# Security and Authentication in IP

There is no point sending a strongly encrypted message only to find you sent it to the wrong person

Perhaps you are buying over the Web and you want to send your credit card details to Acme Widget Company

# Security and Authentication in IP

There is no point sending a strongly encrypted message only to find you sent it to the wrong person

Perhaps you are buying over the Web and you want to send your credit card details to Acme Widget Company

So you negotiate a military-grade encryption key with them and send the details, happy in the knowledge that no-one else can read them

# Security and Authentication in IP

There is no point sending a strongly encrypted message only to find you sent it to the wrong person

Perhaps you are buying over the Web and you want to send your credit card details to Acme Widget Company

So you negotiate a military-grade encryption key with them and send the details, happy in the knowledge that no-one else can read them

Later you discover the Web page was a fake and your details are now in the hands of criminals

# Security and Authentication in IP

There is no point sending a strongly encrypted message only to find you sent it to the wrong person

Perhaps you are buying over the Web and you want to send your credit card details to Acme Widget Company

So you negotiate a military-grade encryption key with them and send the details, happy in the knowledge that no-one else can read them

Later you discover the Web page was a fake and your details are now in the hands of criminals

You must have some way of determining if someone is *who they say they are*: this is authentication

# Security and Authentication in IP

In the real world we use documents like passports and driving licences to identify people

# Security and Authentication in IP

In the real world we use documents like passports and driving licences to identify people

In the Internet world we do the same, except now the documents are chunks of mathematical data

# Security and Authentication in IP

In the real world we use documents like passports and driving licences to identify people

In the Internet world we do the same, except now the documents are chunks of mathematical data

For details go to a crypto course!

# Aside

If we were doing things properly, we should also talk about *authorisation* at this point

# Aside

If we were doing things properly, we should also talk about *authorisation* at this point

After authentication there is the question of whether this entity is allowed access to some resource

# Aside

If we were doing things properly, we should also talk about *authorisation* at this point

After authentication there is the question of whether this entity is allowed access to some resource

For example, in WPA-PSK, a correct password is usually taken as authorisation; in WPA-Enterprise the server will have a list of allowed users+passwords

# Security and Authentication in IP

We have already considered a link layer security: WPA

# Security and Authentication in IP

We have already considered a link layer security: WPA

We now look at a few others, including IPSec (network layer), PPTP and L2TP (link layer), SSL/TLS (transport layer)

# Security and Authentication in IP

We have already considered a link layer security: WPA

We now look at a few others, including IPSec (network layer), PPTP and L2TP (link layer), SSL/TLS (transport layer)

In the normal way of blurring layers when thinking about functionality, PPTP and L2TP are regarded as link layer, even though they layer over IP

# Security and Authentication in IP

## IPSec

IPSec can be used to set up secure point-to-point links (see VPNs, later), but can also be used to secure and authenticate individual connections when the other end supports it: *opportunistic encryption*

# Security and Authentication in IP

## IPSec

IPSec can be used to set up secure point-to-point links (see VPNs, later), but can also be used to secure and authenticate individual connections when the other end supports it: *opportunistic encryption*

IPSec consists of several protocols and defines several IP optional header fields

# Security and Authentication in IP

## IPSec

Secrecy is implemented by *Encapsulating Security Payload* (ESP)

# Security and Authentication in IP

## IPSec

Secrecy is implemented by *Encapsulating Security Payload* (ESP)

Authentication by *Authentication Header* (AH)

# Security and Authentication in IP

## IPSec

Secrecy is implemented by *Encapsulating Security Payload* (ESP)

Authentication by *Authentication Header* (AH)

Keys are managed by *Internet Key Exchange* (IKE) which itself uses the *Internet Security Association and Key Management Protocol* (ISAKMP)

# Security and Authentication in IP

## IPSec

IPSec authenticates connections, not users

# Security and Authentication in IP

## IPSec

IPSec authenticates connections, not users

You do not use it to login, but to ensure the remote host really is Acme Widgets before you send data (money) to them

# Security and Authentication in IP

## IPSec

IPSec authenticates connections, not users

You do not use it to login, but to ensure the remote host really is Acme Widgets before you send data (money) to them

Both ESP and AH require a secret shared key to work

# Security and Authentication in IP

## IPSec

This key can be

- pre-agreed (*manual keying*)
- negotiated by IKE

# Security and Authentication in IP

## IPSec

This key can be

- pre-agreed (*manual keying*)
- negotiated by IKE

IKE can itself use a pre-agreed key to deliver the ESP/AH key, or use a public-key certificate mechanism

# Security and Authentication in IP

## IPSec

Normally there is one IKE process per host and it manages all exchanges for that host

# Security and Authentication in IP

## IPSec

Normally there is one IKE process per host and it manages all exchanges for that host

When a new IPSec/IP connection is started an IKE exchange will take place before the IPSec can continue

# Security and Authentication in IP

## IPSec

Normally there is one IKE process per host and it manages all exchanges for that host

When a new IPSec/IP connection is started an IKE exchange will take place before the IPSec can continue

This may take some time: even enough to cause a TCP timeout on slow machines

# IPSec

# Security and Authentication in IP

## IPSec

IPSec

- is directly inside the IP layer (optional headers), so UDP and TCP are easily layered transparently on top

# Security and Authentication in IP

## IPSec

IPSec

- is directly inside the IP layer (optional headers), so UDP and TCP are easily layered transparently on top
- clearly only applies to IP

IPSec

- is directly inside the IP layer (optional headers), so UDP and TCP are easily layered transparently on top
- clearly only applies to IP
- AH does authentication, while ESP does secrecy and authentication. Pure authentication is OK if you do not need secrecy, but pure secrecy is open to impersonation attacks without some authentication

# Security and Authentication in IP

## IPSec

- ESP has a trailer as well as a header: this can contain padding to hide the length of the original packet

# Security and Authentication in IP

## IPSec

- ESP has a trailer as well as a header: this can contain padding to hide the length of the original packet
- ESP only authenticates the payload, while AH authenticates all the packet, excepting the mutable fields (TTL etc.) that change en route

# Security and Authentication in IP

## IPSec

- ESP has a trailer as well as a header: this can contain padding to hide the length of the original packet
- ESP only authenticates the payload, while AH authenticates all the packet, excepting the mutable fields (TTL etc.) that change en route
- applies to both IPv4 and IPv6

# Security and Authentication in IP

## IPSec

Problems:

# Security and Authentication in IP

## IPSec

Problems:

- initial connection overhead is high

# Security and Authentication in IP

## IPSec

Problems:

- initial connection overhead is high
- IPSec is tricky to set up and manage

# Security and Authentication in IP

## IPSec

Problems:

- initial connection overhead is high
- IPSec is tricky to set up and manage
- It works at the OS host level, and so needs a competent administrator

# Security and Authentication in IP

## IPSec

Problems:

- initial connection overhead is high
- IPSec is tricky to set up and manage
- It works at the OS host level, and so needs a competent administrator
- and also does not have the flexibility that (say) SSL/TLS has, allowing each application to be managed independently

# Security and Authentication in IP

## IPSec

The general view of IPSec is that it is slow: though this view was formed some years ago when computers were much slower than now

# Security and Authentication in IP

## IPSec

The general view of IPSec is that it is slow: though this view was formed some years ago when computers were much slower than now

In fact, after the connection setup, IPSec is not that bad in terms of speed

# Security and Authentication in IP

## IPSec

The general view of IPSec is that it is slow: though this view was formed some years ago when computers were much slower than now

In fact, after the connection setup, IPSec is not that bad in terms of speed

But the configuration question remains

# Security and Authentication in IP

## IPSec

The general view of IPSec is that it is slow: though this view was formed some years ago when computers were much slower than now

In fact, after the connection setup, IPSec is not that bad in terms of speed

But the configuration question remains

**Exercise** The University uses IPsec: investigate

# Security and Authentication in IP

## IPSec

A new alternative to IPSec that is growing in popularity is *WireGuard*

# Security and Authentication in IP

## IPSec

A new alternative to IPSec that is growing in popularity is *WireGuard*

It is (primarily) a point-to-point connection that is high performance, using modern design and algorithms in a small, auditable, codebase (about 1% the size of the IPSec code)

# Security and Authentication in IP

## IPSec

A new alternative to IPSec that is growing in popularity is *WireGuard*

It is (primarily) a point-to-point connection that is high performance, using modern design and algorithms in a small, auditable, codebase (about 1% the size of the IPSec code)

It layers over UDP to provide an encrypted, authenticated network layer

# Security and Authentication in IP

## IPSec

A new alternative to IPSec that is growing in popularity is *WireGuard*

It is (primarily) a point-to-point connection that is high performance, using modern design and algorithms in a small, auditable, codebase (about 1% the size of the IPSec code)

It layers over UDP to provide an encrypted, authenticated network layer

It is very easy to set up

# Security and Authentication in IP

## IPSec

A new alternative to IPSec that is growing in popularity is *WireGuard*

It is (primarily) a point-to-point connection that is high performance, using modern design and algorithms in a small, auditable, codebase (about 1% the size of the IPSec code)

It layers over UDP to provide an encrypted, authenticated network layer

It is very easy to set up

**Exercise** Read about WireGuard

# Security and Authentication in IP

## VPNs

Some systems are based around creating a *Virtual Private Networks* (VPN)

# Security and Authentication in IP

## VPNs

Some systems are based around creating a *Virtual Private Networks* (VPN)

A VPN allows a machine to appear to be on another network by means of tunnelling

# Security and Authentication in IP

## VPNs

Some systems are based around creating a *Virtual Private Networks* (VPN)

A VPN allows a machine to appear to be on another network by means of tunnelling

Recall tunnelling: where one protocol is layered over another so the lower protocol can transport the upper protocol transparently over a network that might not normally carry the upper protocol

# Security and Authentication in IP

## VPNs

Some systems are based around creating a *Virtual Private Networks* (VPN)

A VPN allows a machine to appear to be on another network by means of tunnelling

Recall tunnelling: where one protocol is layered over another so the lower protocol can transport the upper protocol transparently over a network that might not normally carry the upper protocol

VPNs are *private* as they add encryption of the data in the tunnel to provide security

# Security and Authentication in IP

## VPNs

Traffic from the host travels through the tunnel to the network, where it can be routed as if it had originated there

# Security and Authentication in IP

## VPNs

Traffic from the host travels through the tunnel to the network, where it can be routed as if it had originated there

This allows the host to use the services on the network as if it were local to that network

# Security and Authentication in IP

## VPNs

Traffic from the host travels through the tunnel to the network, where it can be routed as if it had originated there

This allows the host to use the services on the network as if it were local to that network

This is good for *teleworkers*

# Security and Authentication in IP

## VPNs

Traffic from the host travels through the tunnel to the network, where it can be routed as if it had originated there

This allows the host to use the services on the network as if it were local to that network

This is good for *teleworkers*

For example, IPSec and WireGuard are VPNs

In overview a VPN:

# Security and Authentication in IP

## VPNs

In overview a VPN:

- is software that creates a new virtual network interface

# Security and Authentication in IP

## VPNs

In overview a VPN:

- is software that creates a new virtual network interface
- when packets need to use the VPN they are routed out on that interface

# Security and Authentication in IP

## VPNs

In overview a VPN:

- is software that creates a new virtual network interface
- when packets need to use the VPN they are routed out on that interface
- the packets are encrypted (in the kernel or in user level software)

# Security and Authentication in IP

## VPNs

In overview a VPN:

- is software that creates a new virtual network interface
- when packets need to use the VPN they are routed out on that interface
- the packets are encrypted (in the kernel or in user level software)
- this data is now sent out over a real interface, e.g., using UDP

# Security and Authentication in IP

## VPNs

At the receiving end:

# Security and Authentication in IP

## VPNs

At the receiving end:

- data arrives in (UDP probably) packets on a real interface

# Security and Authentication in IP

## VPNs

At the receiving end:

- data arrives in (UDP probably) packets on a real interface
- it is decrypted and presented as packets on the virtual VPN interface

# Security and Authentication in IP

## VPNs

At the receiving end:

- data arrives in (UDP probably) packets on a real interface
- it is decrypted and presented as packets on the virtual VPN interface
- which are read by the server application

# Security and Authentication in IP

## VPNs

At the receiving end:

- data arrives in (UDP probably) packets on a real interface
- it is decrypted and presented as packets on the virtual VPN interface
- which are read by the server application

As far as the client and server are concerned, they are operating as normal, sending and receiving packing on a normal interface

# Security and Authentication in IP

## VPNs

There are two common setups for VPNs that treat data from the client in different ways

There are two common setups for VPNs that treat data from the client in different ways

- where *all* client traffic goes out through the VPN, and the server end of the VPN routes it onwards as appropriate

# Security and Authentication in IP

## VPNs

There are two common setups for VPNs that treat data from the client in different ways

- where *all* client traffic goes out through the VPN, and the server end of the VPN routes it onwards as appropriate
- where only traffic destined for the server's network goes through the VPN. Other traffic from the source goes directly to its destination in the normal way. This is sometimes called a *split tunnel*

# Security and Authentication in IP

## VPNs

```
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
...
default         home.gateway.ho 0.0.0.0         UG    0      0        0 wlan0
cs.bath.ac.uk   172.16.0.1      255.255.255.240 UG    2      0        0 tun0
fire.cs.bath.ac home.gateway.ho 255.255.255.255 UGH   0      0        0 wlan0
...
```

# Security and Authentication in IP

## VPNs

```
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
...
default         home.gateway.ho 0.0.0.0         UG    0      0        0 wlan0
cs.bath.ac.uk   172.16.0.1      255.255.255.240 UG    2      0        0 tun0
fire.cs.bath.ac home.gateway.ho 255.255.255.255 UGH   0      0        0 wlan0
...
```

A packet destined for the CS network goes through (virtual) interface `tun0`, which actually sends packets to the VPN software on the local machine;

# Security and Authentication in IP

## VPNs

```
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
...
default         home.gateway.ho 0.0.0.0         UG    0      0        0 wlan0
cs.bath.ac.uk   172.16.0.1      255.255.255.240 UG    2      0        0 tun0
fire.cs.bath.ac home.gateway.ho 255.255.255.255 UGH   0      0        0 wlan0
...
```

This is encrypted and encapsulated in a packet with destination `fire` on the CS network;

# Security and Authentication in IP

## VPNs

```
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
...
default         home.gateway.ho 0.0.0.0         UG    0      0        0 wlan0
cs.bath.ac.uk   172.16.0.1      255.255.255.240 UG    2      0        0 tun0
fire.cs.bath.ac home.gateway.ho 255.255.255.255 UGH   0      0        0 wlan0
...
```

And port number that of the VPN software on the remote server;

# Security and Authentication in IP

## VPNs

```
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
...
default         home.gateway.ho 0.0.0.0         UG    0      0        0 wlan0
cs.bath.ac.uk   172.16.0.1      255.255.255.240 UG    2      0        0 tun0
fire.cs.bath.ac home.gateway.ho 255.255.255.255 UGH   0      0        0 wlan0
...
```

This packet then goes through the host (`H`) route to CS through the real interface `wlan0`;

# Security and Authentication in IP

## VPNs

```
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
...
default         home.gateway.ho 0.0.0.0         UG    0      0        0 wlan0
cs.bath.ac.uk   172.16.0.1      255.255.255.240 UG    2      0        0 tun0
fire.cs.bath.ac home.gateway.ho 255.255.255.255 UGH   0      0        0 wlan0
...
```

The routes are checked longest mask first, to prevent an infinite loop!

# Security and Authentication in IP

## VPNs

```
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
...
default         home.gateway.ho 0.0.0.0         UG    0      0        0 wlan0
cs.bath.ac.uk   172.16.0.1      255.255.255.240 UG    2      0        0 tun0
fire.cs.bath.ac home.gateway.ho 255.255.255.255 UGH   0      0        0 wlan0
...
```

The VPN software on the remote server gets the packet and deencapsulates it;

# Security and Authentication in IP

## VPNs

```
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
...
default         home.gateway.ho 0.0.0.0         UG    0      0        0 wlan0
cs.bath.ac.uk   172.16.0.1      255.255.255.240 UG    2      0        0 tun0
fire.cs.bath.ac home.gateway.ho 255.255.255.255 UGH   0      0        0 wlan0
...
```

It rewrites the source address on the packet to its own address so that replies come back to it (c.f., NAT);

# Security and Authentication in IP

## VPNs

```
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
...
default         home.gateway.ho 0.0.0.0         UG    0      0        0 wlan0
cs.bath.ac.uk   172.16.0.1      255.255.255.240 UG    2      0        0 tun0
fire.cs.bath.ac home.gateway.ho 255.255.255.255 UGH   0      0        0 wlan0
...
```

The remote host forwards the packet to the destination which is on its local network;

# Security and Authentication in IP

## VPNs

```
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
...
default         home.gateway.ho 0.0.0.0         UG    0      0        0 wlan0
cs.bath.ac.uk   172.16.0.1      255.255.255.240 UG    2      0        0 tun0
fire.cs.bath.ac home.gateway.ho 255.255.255.255 UGH   0      0        0 wlan0
...
```

Symmetrically, it will encrypt, encapsulate and return any replies back through the tunnel;

# Security and Authentication in IP

## VPNs

```
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
...
default         home.gateway.ho 0.0.0.0         UG    0      0        0 wlan0
cs.bath.ac.uk   172.16.0.1      255.255.255.240 UG    2      0        0 tun0
fire.cs.bath.ac home.gateway.ho 255.255.255.255 UGH   0      0        0 wlan0
...
```

Locally, all other (default) traffic goes out through the normal interface, not the VPN

# Security and Authentication in IP

## VPNs

```
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
...
default         172.16.0.1      0.0.0.0         UG    0      0        0 tun0
cs.bath.ac.uk   172.16.0.1      255.255.255.240 UG    2      0        0 tun0
fire.cs.bath.ac home.gateway.ho 255.255.255.255 UGH   0      0        0 wlan0
...
```

In comparison, the other setup;

# Security and Authentication in IP

## VPNs

```
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
...
default         172.16.0.1      0.0.0.0         UG    0      0        0 tun0
cs.bath.ac.uk   172.16.0.1      255.255.255.240 UG    2      0        0 tun0
fire.cs.bath.ac home.gateway.ho 255.255.255.255 UGH   0      0        0 wlan0
...
```

Here all default traffic goes through interface `tun0`;

# Security and Authentication in IP

## VPNs

```
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
...
default         172.16.0.1      0.0.0.0         UG    0      0        0 tun0
cs.bath.ac.uk   172.16.0.1      255.255.255.240 UG    2      0        0 tun0
fire.cs.bath.ac home.gateway.ho 255.255.255.255 UGH   0      0        0 wlan0
...
```

This is encapsulated in the same way;

# Security and Authentication in IP

## VPNs

```
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
...
default         172.16.0.1      0.0.0.0         UG    0      0        0 tun0
cs.bath.ac.uk   172.16.0.1      255.255.255.240 UG    2      0        0 tun0
fire.cs.bath.ac home.gateway.ho 255.255.255.255 UGH   0      0        0 wlan0
...
```

And routed through the tunnel via the real interface;

# Security and Authentication in IP

## VPNs

```
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
...
default         172.16.0.1      0.0.0.0         UG    0      0        0 tun0
cs.bath.ac.uk   172.16.0.1      255.255.255.240 UG    2      0        0 tun0
fire.cs.bath.ac home.gateway.ho 255.255.255.255 UGH   0      0        0 wlan0
...
```

The VPN software on the remote network gets the packet, deencapsulates it, rewrites its source address and forwards it to the destination which now might be anywhere, not just on its local network;

# Security and Authentication in IP

## VPNs

```
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
...
default         172.16.0.1      0.0.0.0         UG    0      0        0 tun0
cs.bath.ac.uk   172.16.0.1      255.255.255.240 UG    2      0        0 tun0
fire.cs.bath.ac home.gateway.ho 255.255.255.255 UGH   0      0        0 wlan0
...
```

Returning packets are sent back through the VPN as before

In the first setup you get secure access to the work network, but to the rest of the world you are at home (and not secure)

In the first setup you get secure access to the work network, but to the rest of the world you are at home (and not secure)

The second makes you to appear to everyone to be at work as all your packets have a work IP address on them

**Exercise** Find out how to use the University's VPN from your home

**Exercise** Find out how to use the University's VPN from your home

**Exercise** The `www.newscientist.com` website reserves some content for subscribers. It uses the requesting IP address to check for access rights. The University is a subscriber. Use a VPN to get at this content from your home

# Security and Authentication in IP

## VPNs

**Exercise** Find out how to use the University's VPN from your home

**Exercise** The `www.newscientist.com` website reserves some content for subscribers. It uses the requesting IP address to check for access rights. The University is a subscriber. Use a VPN to get at this content from your home

**Exercise** Find out how (or if) your favourite VPN can be configured as a split tunnel

The *Point-to-Point Tunneling Protocol* (PPTP) was devised by Microsoft to support VPNs

# Security and Authentication in IP

## VPNs

The *Point-to-Point Tunneling Protocol* (PPTP) was devised by Microsoft to support VPNs

It

- tunnels IP over PPP over the *Generic Routing Encapsulation* protocol (GRE) over IP and sends connection control messages over a separate TCP connection
- layers only over IP

It

# Security and Authentication in IP

## VPNs

It

- can encapsulate other protocols such as IPX (Internetwork Packet Exchange, Novell) and NetBIOS/NetBEUI (Network BIOS, NetBIOS Extended User Interface, Microsoft)

# Security and Authentication in IP

## VPNs

It

- can encapsulate other protocols such as IPX (Internetwork Packet Exchange, Novell) and NetBIOS/NetBEUI (Network BIOS, NetBIOS Extended User Interface, Microsoft)
- uses PPP for authentication

# Security and Authentication in IP

## VPNs

It

- can encapsulate other protocols such as IPX (Internetwork Packet Exchange, Novell) and NetBIOS/NetBEUI (Network BIOS, NetBIOS Extended User Interface, Microsoft)
- uses PPP for authentication
- can use *Microsoft Point-to-Point Encryption* (MPPE) for privacy, combined with *Challenge-Handshake Authentication Protocol* (MS-CHAP) for authentication

# Security and Authentication in IP

## VPNs

It

- can encapsulate other protocols such as IPX (Internetwork Packet Exchange, Novell) and NetBIOS/NetBEUI (Network BIOS, NetBIOS Extended User Interface, Microsoft)
- uses PPP for authentication
- can use *Microsoft Point-to-Point Encryption* (MPPE) for privacy, combined with *Challenge-Handshake Authentication Protocol* (MS-CHAP) for authentication
- is simple to set up

# Security and Authentication in IP

## VPNs

On the other hand, PPTP is regarded as insecure as the authentication mechanism (MS-CHAP) can be broken

# Security and Authentication in IP

## VPNs

On the other hand, PPTP is regarded as insecure as the authentication mechanism (MS-CHAP) can be broken

A later version (MS-CHAPv2) fixes some, but not all of the holes

The *Layer 2 Tunneling Protocol* (L2TP) combines features of PPTP and *Layer 2 Forwarding* (L2F) developed by Cisco Systems Inc

It

It

- tunnels IP over PPP over L2TP over UDP

# Security and Authentication in IP

## VPNs

It

- tunnels IP over PPP over L2TP over UDP
- is intended to be used over ATM, Frame Relay and X.25 networks

# Security and Authentication in IP

## VPNs

It

- tunnels IP over PPP over L2TP over UDP
- is intended to be used over ATM, Frame Relay and X.25 networks
- has no native encryption and must rely on, say, IPSec for secrecy

# Security and Authentication in IP

## VPNs

It

- tunnels IP over PPP over L2TP over UDP
- is intended to be used over ATM, Frame Relay and X.25 networks
- has no native encryption and must rely on, say, IPSec for secrecy
- mainly uses PPP for authentication, but can also use ESP from IPSec

# Security and Authentication in IP

## VPNs

It

- tunnels IP over PPP over L2TP over UDP
- is intended to be used over ATM, Frame Relay and X.25 networks
- has no native encryption and must rely on, say, IPSec for secrecy
- mainly uses PPP for authentication, but can also use ESP from IPSec
- is believed to be more secure than PPTP

# Security and Authentication in IP

## VPNs

It

- tunnels IP over PPP over L2TP over UDP
- is intended to be used over ATM, Frame Relay and X.25 networks
- has no native encryption and must rely on, say, IPSec for secrecy
- mainly uses PPP for authentication, but can also use ESP from IPSec
- is believed to be more secure than PPTP
- is simple to set up

While L2TP and PPTP were popularised by Microsoft, other operating systems prefer other solutions

While L2TP and PPTP were popularised by Microsoft, other operating systems prefer other solutions

We shall talk about *OpenVPN*, later

# Security and Authentication in IP

## Tunnelling TCP

Note that all these tunnels layer over UDP, not TCP

Note that all these tunnels layer over UDP, not TCP

This is because tunnelling TCP over TCP is usually a bad idea

# Security and Authentication in IP

## Tunnelling TCP

Note that all these tunnels layer over UDP, not TCP

This is because tunnelling TCP over TCP is usually a bad idea

TCP has a large overhead to gain reliability: there's no point in paying this cost twice

# Security and Authentication in IP

## Tunnelling TCP

Note that all these tunnels layer over UDP, not TCP

This is because tunnelling TCP over TCP is usually a bad idea

TCP has a large overhead to gain reliability: there's no point in paying this cost twice

Plus, each TCP has its own idea of timeouts and retransmits and they can start to fight each other: the retransmit of one TCP will be viewed as a duplicate by the other TCP

# Security and Authentication in IP

## Tunnelling TCP

Note that all these tunnels layer over UDP, not TCP

This is because tunnelling TCP over TCP is usually a bad idea

TCP has a large overhead to gain reliability: there's no point in paying this cost twice

Plus, each TCP has its own idea of timeouts and retransmits and they can start to fight each other: the retransmit of one TCP will be viewed as a duplicate by the other TCP

Thus most VPNs tunnel over UDP

# Security and Authentication in IP

## Tunnelling TCP

**Exercise** Read about the *Secure Socket Tunneling Protocol* (SSTP) and the *TCP meltdown problem*

Generic problems of VPNs include

Generic problems of VPNs include

- there is encryption and authentication header overhead in every packet: this may cause extra packets or extra fragmentation

# Security and Authentication in IP

## VPNs

Generic problems of VPNs include

- there is encryption and authentication header overhead in every packet: this may cause extra packets or extra fragmentation
- there is overhead in the time taken to encrypt or authenticate the packets

# Security and Authentication in IP

## VPNs

- some routers or ISPs make decisions based on the type of traffic (e.g., video or HTTP): encryption hides this and makes efficient routing harder

# Security and Authentication in IP

## VPNs

- some routers or ISPs make decisions based on the type of traffic (e.g., video or HTTP): encryption hides this and makes efficient routing harder
- some ISPs like to charge more for, or manage certain kinds of traffic (e.g., bittorrent and video) and this hides the kind of traffic. So some ISPs have blanket bans on VPNs

# Security and Authentication in IP

## VPNs

- some routers or ISPs make decisions based on the type of traffic (e.g., video or HTTP): encryption hides this and makes efficient routing harder
- some ISPs like to charge more for, or manage certain kinds of traffic (e.g., bittorrent and video) and this hides the kind of traffic. So some ISPs have blanket bans on VPNs
- in VPNs speed is secondary to security, but people will not use them if they are too slow

# Security and Authentication in IP

And, as previously mentioned, any kind of security is viewed with suspicion by law enforcement agencies

# Security and Authentication in IP

And, as previously mentioned, any kind of security is viewed with suspicion by law enforcement agencies

Note that a VPN can make you appear to be in a different country

# Security and Authentication in IP

And, as previously mentioned, any kind of security is viewed with suspicion by law enforcement agencies

Note that a VPN can make you appear to be in a different country

Good for evading country-locked content (geofencing), but bad for law enforcement and people who want to track what you are doing

# Security and Authentication in IP

For example, the *Investigatory Powers Act 2016*, and its update, *The Data Retention and Acquisition Regulations 2018*, a law that can require your ISP to log every website you visit and every recipient of emails and phone calls (your *Internet Connection Records*)

# Security and Authentication in IP

Some core information is accessible, without warrant, by certain people:

- account reference
- a source and port address, a destination IP and port address
- a time/date + duration
- partial URLs (only part containing server name, no content)

# Security and Authentication in IP

Some core information is accessible, without warrant, by certain people:

- account reference
- a source and port address, a destination IP and port address
- a time/date + duration
- partial URLs (only part containing server name, no content)

So, the metadata and not the data

# Security and Authentication in IP

Some core information is accessible, without warrant, by certain people:

- account reference
- a source and port address, a destination IP and port address
- a time/date + duration
- partial URLs (only part containing server name, no content)

So, the metadata and not the data

An interception warrant is needed for more, e.g., content

# Security and Authentication in IP

The law also gives the security services new powers to hack computers and, e.g., pressure service providers not to support end-to-end encryption

# Security and Authentication in IP

The law also gives the security services new powers to hack computers and, e.g., pressure service providers not to support end-to-end encryption

This is a very contentious law, not only because it may be in contravention of EU privacy laws, and that might mean the UK cannot legally process data from the EU

# Security and Authentication in IP

The law also gives the security services new powers to hack computers and, e.g., pressure service providers not to support end-to-end encryption

This is a very contentious law, not only because it may be in contravention of EU privacy laws, and that might mean the UK cannot legally process data from the EU

**Exercise** Read the list of 50 or so authorities that can access your web history, without warrant