

# Virtual Private Mesh Network

## Decentralized VPN Application

Pau Rodriguez-Estivill

Summer Camp Garrotxa 2008

# Outline

- 1 **Introduction**
- 2 **State of Art**
  - IPsec
  - OpenVPN
  - Tinc VPN
- 3 **Internals**
  - Overview
  - Security
  - Architecture
  - Conclusions

# Outline

## 1 Introduction

## 2 State of Art

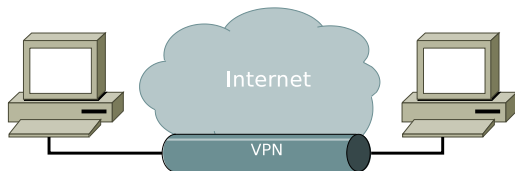
- IPsec
- OpenVPN
- Tinc VPN

## 3 Internals

- Overview
- Security
- Architecture
- Conclusions

# Internet

- **Insecure**
  - Traffic can be read by other parties
  - Traffic can be modified by other parties
  - Content can be faked (**phishing**)
- **Untrusted**
  - IPs can be spoofed
- **Divided**
  - NATs separate it in multiple private networks



- **Virtual Network**

- a tunnel with no routing hops
- own IP addressing

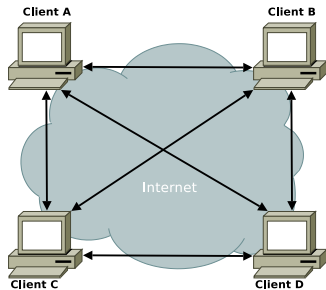
- **Private**

- exclusive for trusted parties
- traffic cannot be read by other parties

# Security

- **Encrypting** it cannot be read by other parties
- **Integrity validation** ensure it has not been modified
- **Authenticating** ensure that it is from a trusted party
- **No repudiation** other parties cannot lie
- **Anti-replay** protect against malicious replay

# Project Aims



- Add dynamically nodes to the fully connected mesh
- Authenticate nodes and IP addressing together
- Low latency and low overhead
- NAT friendly

# Outline

- 1 Introduction
- 2 State of Art**
  - IPsec
  - OpenVPN
  - Tinc VPN
- 3 Internals
  - Overview
  - Security
  - Architecture
  - Conclusions

# Outline

## 1 Introduction

## 2 State of Art

- IPsec
- OpenVPN
- Tinc VPN

## 3 Internals

- Overview
- Security
- Architecture
- Conclusions

# IPsec vs VPMN

## Pros

- Standard
- Mandatory in IPv6 implementations
- DNSSEC enable possible dynamic tunneling

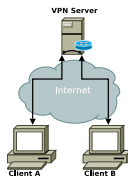
## Cons

- Different implementations are **not compatible**
- Must be supported in kernel
- Only one mode supported through NAT
- IP addressing authentication not centralized

# Outline

- 1 Introduction
- 2 **State of Art**
  - IPsec
  - **OpenVPN**
  - Tinc VPN
- 3 Internals
  - Overview
  - Security
  - Architecture
  - Conclusions

# OpenVPN vs VPMN



## Pros

- IP configurations can be pushed
- Standard encryption channel

## Cons

- Centralized, mesh alternative not easy
- IP addressing not authenticated

# Outline

## 1 Introduction

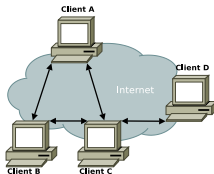
## 2 State of Art

- IPsec
- OpenVPN
- Tinc VPN

## 3 Internals

- Overview
- Security
- Architecture
- Conclusions

# Tinc VPN vs VPMN



## Pros

- Meshed Network

## Cons

- Not fully connected
- IP addressing not authenticated

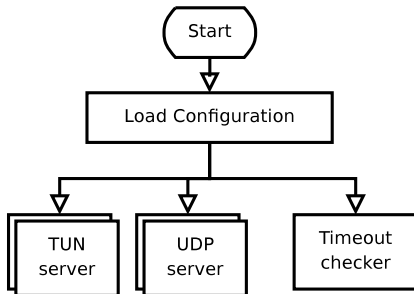
# Outline

- 1 Introduction
- 2 State of Art
  - IPsec
  - OpenVPN
  - Tinc VPN
- 3 Internals**
  - Overview
  - Security
  - Architecture
  - Conclusions

# Outline

- 1 Introduction
- 2 State of Art
  - IPsec
  - OpenVPN
  - Tinc VPN
- 3 Internals
  - Overview
  - Security
  - Architecture
  - Conclusions

# Application



- Multi-thread application
- Entirely written in C

# Outline

- 1 Introduction
- 2 State of Art
  - IPsec
  - OpenVPN
  - Tinc VPN
- 3 Internals**
  - Overview
  - Security**
  - Architecture
  - Conclusions


## Security summary

- Datagram TLS (DTLS)
- Uses CA for trusting nodes from the same network
- Certificates contain ACLs for IP addressing

### NameConstraints (x509v3)

```
nameConstraints=permitted;IP:192.168.0.0/255.255.0.0
```

## DTLS: Datagram TLS

-  RFC 4347
- All operations in UDP
  - Exchange of certificates
  - Negotiation of cryptography algorithms
  - Transport of ciphered data
- Based on TLSv1
- Cryptography mechanisms as TLS
  - Encryption
  - Integrity validation
  - Authentication
  - Anti-replay mechanism

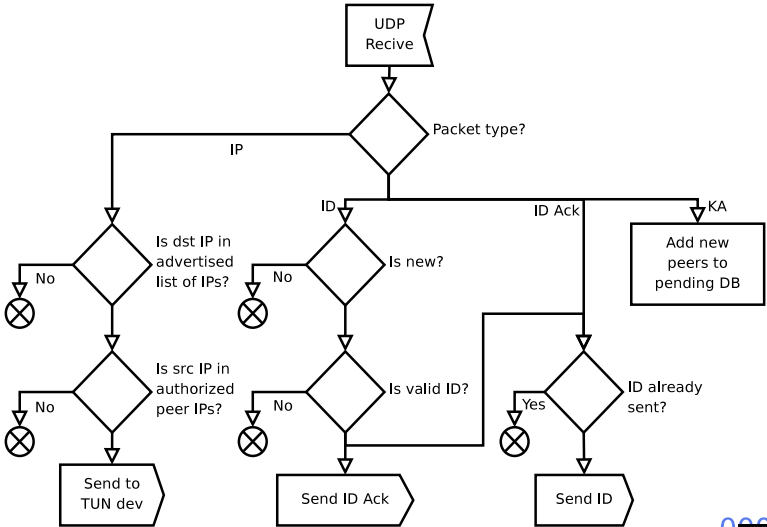
## Type of packets

- 1 Raw IP packets
- 2 Identification packets
  - IP-port pairs
  - Shared networks
- 3 Identification acknowledgment packets
- 4 Keep alive packets
  - Information of other known peers
    - All IP-port pairs
    - Shared networks

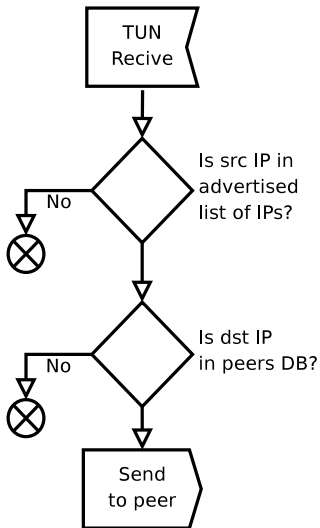
# Outline

- 1 Introduction
- 2 State of Art
  - IPsec
  - OpenVPN
  - Tinc VPN
- 3 Internals**
  - Overview
  - Security
  - Architecture**
  - Conclusions

# UDP Server Part



# TUN Server Part



# Outline

- 1 Introduction
- 2 State of Art
  - IPsec
  - OpenVPN
  - Tinc VPN
- 3 Internals
  - Overview
  - Security
  - Architecture
  - Conclusions

# Conclusions

## Pros

- Dynamic Fully Connected Mesh Network
- Authenticated IP addressing with certificates
- Standard encryption channel (**DTLS**)

## Cons

- No relay mode possible
- Fragmentation needed

## Future tasks

- Heterogeneous MTU support
- Let fragmentation be optional
- User-space NAT

## Summary

- Internet is **insecure** and **VPN** is needed
- **Server-less** architecture
- **Dynamic** Fully Connected Mesh Network
- **Authenticated IP** addressing with certificates
- Standard encryption channel (**DTLS**)

# Questions?