Chapter 53
Virtual Private Networks

- **Virtually Speaking of Real Security.**

"We use military-grade encryption. This just speaks to the need to safeguard one's password with as much care as possible."

-- Vincent Sollitto

Copyright Information

- Some rights reserved / Einige Rechte vorbehalten
- Michael Kafka, René Pfeiffer, Sebastian Mayer
  C.a.T. Consulting and Trainings, Vienna, Austria
- You may freely use, distribute and modify this work under following agreement:
- Diese Arbeit darf frei genutzt, verbreitet und bearbeitet werden unter folgenden Bedingungen:

Authors must be referenced (also for modification)
Autoren müssen genannt werden (auch bei Bearbeitung)

Only for non commercial use
Nur für nichtkommerzielle Nutzung

Derivative work under same licence
Derivative Arbeit unter selber Lizenz

creative commons http://www.creativecommons.com

DeepSec Vienna 2007
7 Layers of Insecurity

Chapter 53
Virtual Private Networks

- Agenda
  - Technologies
  - Attacks

VPN Technologies

- Various Ways of Virtual Privacy.

IP Security (IPsec)

- **Native Security for IPv4/IPv6.**

IP Security (IPsec)

- IPsec is mandatory part of IPv6
- IPsec can be used with IPv4
- Design of IPsec covers
  - Encryption
  - Integrity validation
  - Authentication
  - Protection from replay attacks

IPSec Protocols

- Authentication header (AH)
  - Connectionless integrity
  - Data origin authentication
- Encapsulating Security Payload (ESP)
  - Integrity & authentication
  - Encryption

IPSec Modes

- Transport mode
  - End-to-end
  - Encrypted payload
- Tunnel mode
  - Gateway-to-gateway
  - Encrypted payload and header

Security Association

- Connected points share parameters
  - Algorithms & keys
  - Security Association (SA)
- SA needs to be negotiated
  - Internet Key Exchange (IKE)
  - Manual keying

Internet Key Exchange (IKE)

- IKE proposed in RFCs
  - Internet Security Association and Key Management Protocol (ISAKMP)
  - Internet IP Security DOI (IPSEC DOI)
- Handles key exchange and management
  - IKE Main Mode
  - IKE Aggressive Mode

Attacks on IPsec

- Bugs in implementations
  - IPsec/IKE are very complex
  - Configuration errors likely
- Key exchange in aggressive mode
  - Sniffing exchange (few packets)
  - Brute-force the hash
- Risk: medium
- Impact: high

Point-to-Point Tunneling Protocol (PPTP)

- Early VPN Technology.

PPTP Overview

- PPTP uses two sessions
  - PPP link to peer with GRE
  - Session on 1723/TCP to manage GRE
- PPTP offers authentication
  - Microsoft® MSCHAP-v2
  - EAP-TLS
- Encryption via Microsoft® Point-to-Point Encryption (MPPE)
  - Uses RC4 with 40, 56 or 128 bit keys

PPTP Weakness

- In theory PPTP is fine
  - Bruce Schneier says so ☺
- In practice avoid MS PPTP with MS-CHAP-v2
  - Full key length not used
  - Passwords use guessable hashes
  - Control channel attacks against server
  - *Upgrade path:* use IPsec or L2TP/IPsec
- Risk: medium
- Impact: high

Layer 2 Tunneling Protocol (L2TP)

- Layer 2 VPN Support on Layer 5.

L2TP Overview

- L2TP creates a tunnel for VPN traffic
  - Uses encapsulation in UDP (port 1701)
  - Looks like layer 2, should be layer 5
- L2TP Access Concentrator (LAC)
  - Initiator of tunnel
- L2TP Network Server (LNS)
  - Waits for new tunnels
- L2TP provides no strong authentication
- L2TP provides no confidentiality

L2TP Tunnels

- L2TP provides session management
- L2TP is often combined with
  - IPSec
  - PPTP
  - Layer 2 Forwarding (L2F)
- Tunnel may hinder inspection of passenger protocol

OpenVPN™

- It's Open and yet it's Virtually Private.

OpenVPN™ Overview

- OpenVPN™ is based on OpenSSL
- Server/client in userspace
- OpenVPN™ multiplexes everything
  - Uses port 1194 (UDP or TCP)
  - Can (ab)use proxies through HTTP
- Provides authentication and encryption

OpenVPN™ Cryptography

- Static key
  - HMAC send/receive key
  - Data decrypt/encrypt
- SSL/TLS keys & certificates
- HMAC signature for all VPN packets
  - Protects SSL/TLS, no DoS, no scanning
- OpenVPN™ can authenticate TLS handshake
  - PSK or static key is used
  - Attacker can't start TLS at all

Attacks on OpenVPN™

- MITM with certificates
  - Valid but malicious certificates
  - Check certificates, use a proper CA
- OpenVPN™ servers push configs
  - Malicious server can execute code on client (OpenVPN™ 2.0.0 to 2.0.5)
- Risk: medium
- Impact: high

OpenSSH

- **Secure Shell Connections with Tunnel.**

SSH and OpenSSH

- Secure Shell replaces rsh, rlogin, telnet, rcp
- TCP tunnels possible
  - Port and X forwarding
- Integrity protection, host identification
- Lots of authentication methods
  - Passwords or keys with passphrases
  - Smart Cards, PKI, One Time Passwords
  - Kerberos

(Open)SSH Attacks

- Replay/insertion attacks with SSH v1
- MITM attacks (very difficult)
- Password guessing
- TCP/IP attacks
- Traffic analysis
- Risk: low
- Impact: medium/high

Other VPN Implementations

- **The Key is Out There.**

VPN Implementations

- CIPE
  - Crypto IP Encapsulation
- vtun
  - Supports layer 2/3 tunnel
  - Uses Blowfish 128 bit and PSK
- tinc
- Hamachi
  - Proprietary VPN tool

Chapter 53
VPN

- Summary
  - Always check implementation.
  - Use known secure algorithms.
  - Be careful when using certificates.
  - Protect and change your keys.

Thank You

- Questions?

DeepSec Vienna 2007
7 Layers of Insecurity

Chapter 53
Virtual Private Networks

- Virtually Speaking of Real Security.

"We use military-grade encryption. This just speaks to the need to safeguard one's password with as much care as possible."

-- Vincent Sollitto

DeepSec Vienna 2007
7 Layers of Insecurity

Copyright Information

- Some rights reserved / Einige Rechte vorbehalten
- Michael Kafka, René Pfeiffer, Sebastian Mayer
  C.a.T. Consulting and Trainings, Vienna, Austria
- You may freely use, distribute and modify this work under following agreement:
- Diese Arbeit darf frei genutzt, verbreitet und bearbeitet werden unter folgenden Bedingungen:

Authors must be referenced (also for modification)
Autoren müssen genannt werden (auch bei Bearbeitung)

Only for non commercial use
Nur für nichtkommerzielle Nutzung

Derivative work under same licence
Derivative Arbeit unter selber Lizenz

creative commons http://www.creativecommons.com

DeepSec Vienna 2007
7 Layers of Insecurity

© November 2007 53 - VPN 2

This presentation is published under the CreativeCommons License which can be viewed in detail on their hompage: http://creativecommons.org/licenses/by-nc-sa/2.0/at/

Read more on http://www.creativecommons.com

You are free:

to Share — to copy, distribute and transmit the work

to Remix — to adapt the work

Under the following conditions:

Attribution. You must attribute the work in the manner specified by the author or licensor (but not in any way that suggests that they endorse you or your use of the work).

Noncommercial. You may not use this work for commercial purposes.

Share Alike. If you alter, transform, or build upon this work, you may distribute the resulting work only under the same or similar license to this one.

- **For any reuse or distribution, you must make clear to others the license terms of this work. The best way to do this is with a link to this web page.**
- **Any of the above conditions can be waived if you get permission from the copyright holder.**
- **Nothing in this license impairs or restricts the author's moral rights.**

Chapter 53
Virtual Private Networks

- Agenda
  - Technologies
  - Attacks

DeepSec Vienna 2007
7 Layers of Insecurity

VPN Technologies

- Various Ways of Virtual Privacy.

DeepSec Vienna 2007
7 Layers of Insecurity

IP Security (IPsec)

- Native Security for IPv4/IPv6.

DeepSec Vienna 2007
7 Layers of Insecurity

IP Security (IPsec)

- IPsec is mandatory part of IPv6
- IPsec can be used with IPv4
- Design of IPsec covers
  - Encryption
  - Integrity validation
  - Authentication
  - Protection from replay attacks

DeepSec Vienna 2007
7 Layers of Insecurity

IPSec Protocols

- Authentication header (AH)
  - Connectionless integrity
  - Data origin authentication
- Encapsulating Security Payload (ESP)
  - Integrity & authentication
  - Encryption

DeepSec Vienna 2007
7 Layers of Insecurity

IPSec Modes

- Transport mode
  - End-to-end
  - Encrypted payload
- Tunnel mode
  - Gateway-to-gateway
  - Encrypted payload and header

DeepSec Vienna 2007
7 Layers of Insecurity

Transport is usually used to secure host-to-host connections. In IPv6 all security and authentication is shifted to the IPsec component. This is the reason why IPsec is mandatory in IPv6. Other protocols such as OSPFv6 or others don't have their own mechanisms for authentication anymore.

Security Association

- Connected points share parameters
  - Algorithms & keys
  - Security Association (SA)
- SA needs to be negotiated
  - Internet Key Exchange (IKE)
  - Manual keying

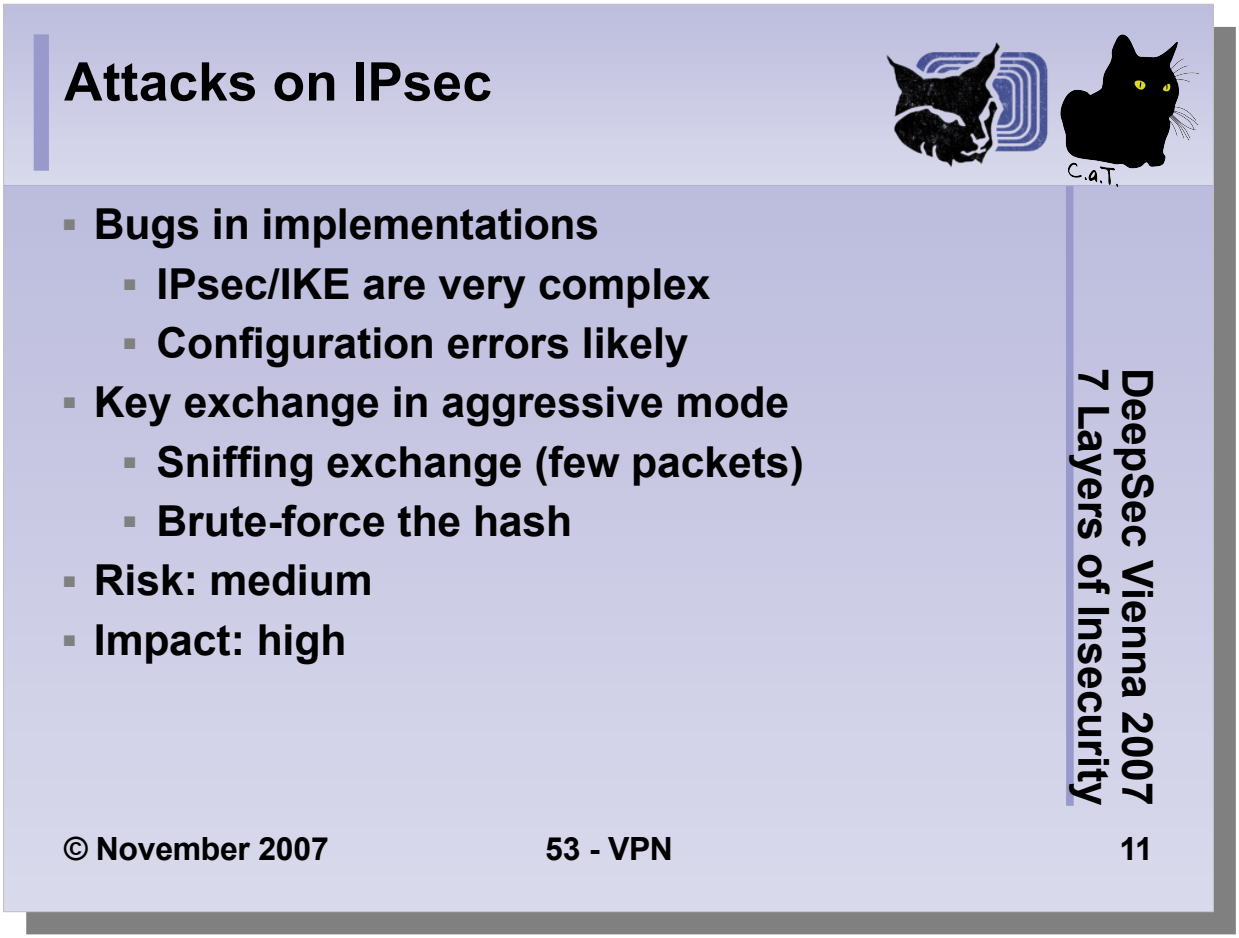
DeepSec Vienna 2007
7 Layers of Insecurity

Internet Key Exchange (IKE)

- IKE proposed in RFCs
  - Internet Security Association and Key Management Protocol (ISAKMP)
  - Internet IP Security DOI (IPSEC DOI)
- Handles key exchange and management
  - IKE Main Mode
  - IKE Aggressive Mode

DeepSec Vienna 2007
7 Layers of Insecurity

An architecture for the Internet Key Exchange Protocol



Penetration Testing IPsec VPNs

A Cryptographic Evaluation of IPsec

Cryptography in Theory and Practice: The Case of Encryption in IPsec

IPsec offers “too much” options. This can easily lead to implementation errors that may open doors for attackers. It also increases the possibility for errors in the source code of the IPSec stack. Nevertheless IPSec offers interoperability and a solid encryption with key management provided the administrators created a proper configuration.

Mitigation:

• Make sure IPsec parametersare fully defined and known to everyone dealing with administration.

• Always use encryption **and** integrity checks (make sure integrity of packets gets really checked).

• IPsec endpoints need to be inside DMZs so that decrypted traffic can still be inspected.

• Don't use the aggressive mode (also known as quick mode) if possible.

• Test the implementation of IPsec you use. Disagreement between developers and standard designers may lead to unpredicted results (see Lost in Translation: Theory and Practice in Cryptography for details).

Point-to-Point Tunneling Protocol (PPTP)

- Early VPN Technology.

DeepSec Vienna 2007
7 Layers of Insecurity

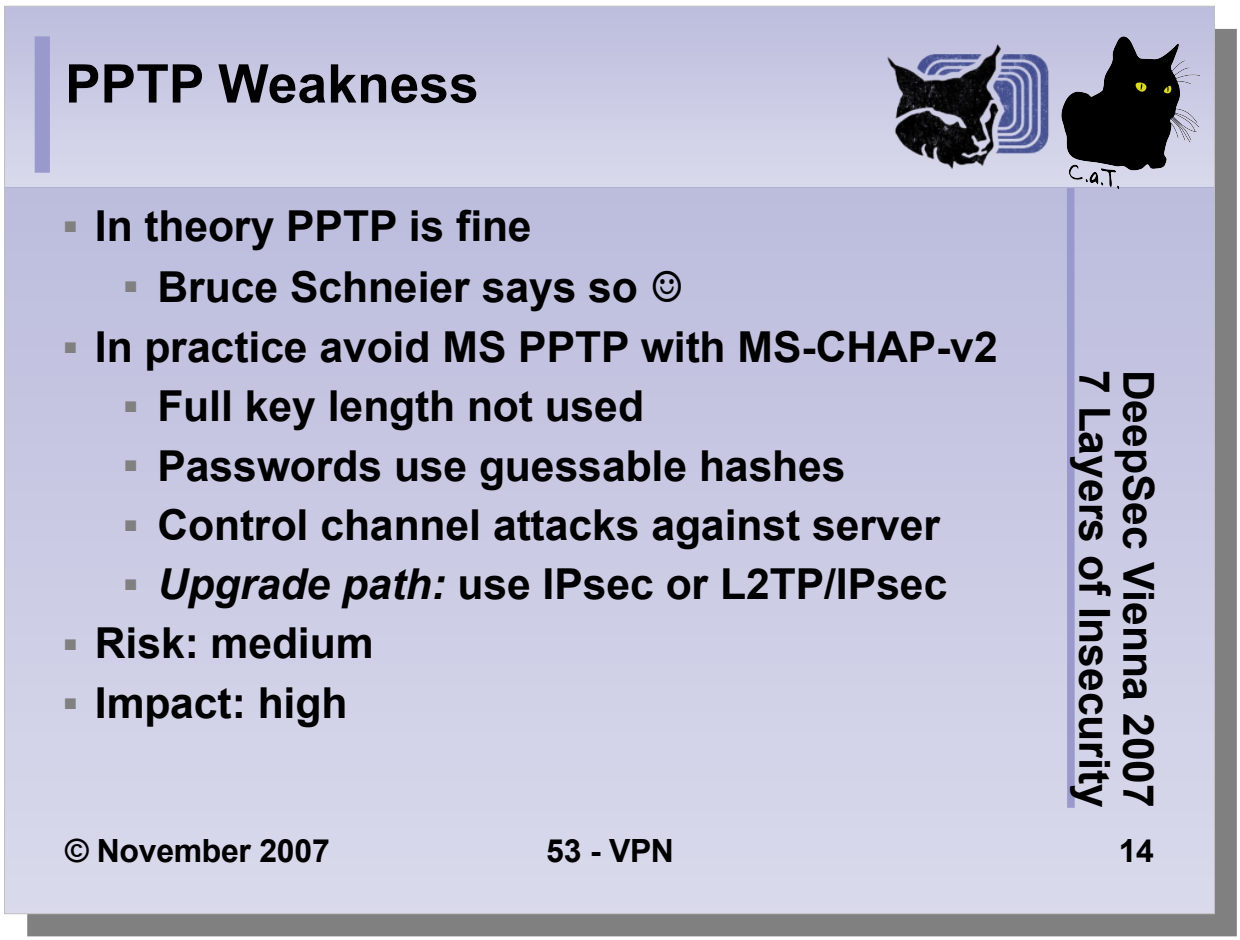
PPTP Overview

- PPTP uses two sessions
  - PPP link to peer with GRE
  - Session on 1723/TCP to manage GRE
- PPTP offers authentication
  - Microsoft® MSCHAP-v2
  - EAP-TLS
- Encryption via Microsoft® Point-to-Point Encryption (MPPE)
  - Uses RC4 with 40, 56 or 128 bit keys

DeepSec Vienna 2007
7 Layers of Insecurity

PPTP proposed in RFC 2637

FAQ on PPTP from Microsoft®



Frequently Asked Questions -- Microsoft's PPTP Implementation (Bruce Schneier's web site)

Cryptanalysis of Microsoft's PPTP Authentication Extensions (MS-CHAPv2)

Mitigation:

• Avoid Microsoft® PPTP with MS-CHAP v2.

• Use a strong password policy and change passwords periodically.

• Use IPsec or L2/TP/IPsec

Layer 2 Tunneling Protocol (L2TP)

- Layer 2 VPN Support on Layer 5.

DeepSec Vienna 2007
7 Layers of Insecurity

L2TP Overview

- L2TP creates a tunnel for VPN traffic
  - Uses encapsulation in UDP (port 1701)
  - Looks like layer 2, should be layer 5
- L2TP Access Concentrator (LAC)
  - Initiator of tunnel
- L2TP Network Server (LNS)
  - Waits for new tunnels
- L2TP provides no strong authentication
- L2TP provides no confidentiality

DeepSec Vienna 2007
7 Layers of Insecurity

© November 2007 53 - VPN 16

Layer 2 Tunnel Protocol (documentation from Cisco)
U.S. Patent 5,918,019

L2TP Tunnels

- L2TP provides session management
- L2TP is often combined with
  - IPSec
  - PPTP
  - Layer 2 Forwarding (L2F)
- Tunnel may hinder inspection of passenger protocol

DeepSec Vienna 2007
7 Layers of Insecurity

OpenVPN™

- It's Open and yet it's Virtually Private.

DeepSec Vienna 2007
7 Layers of Insecurity

OpenVPN™ Overview

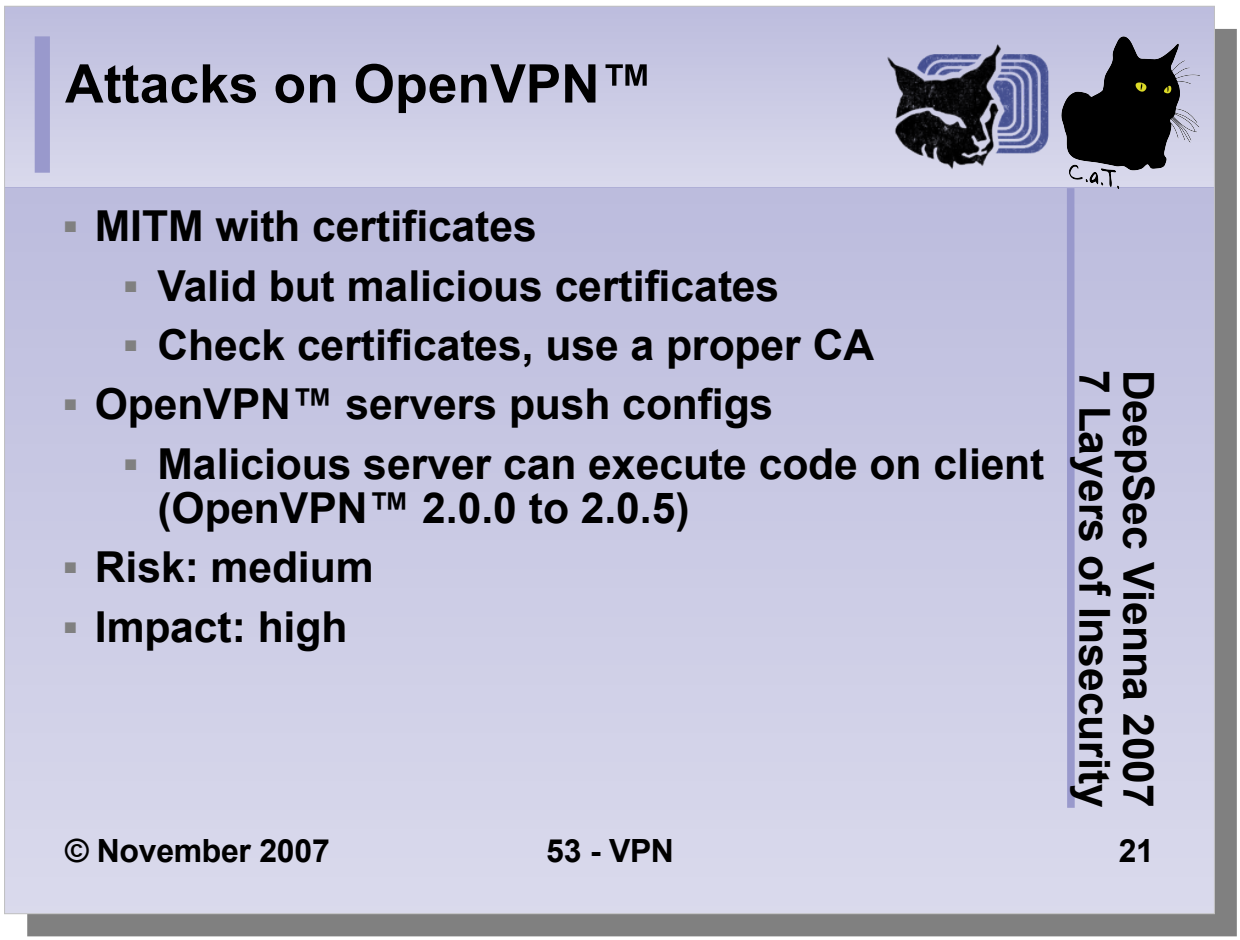
- OpenVPN™ is based on OpenSSL
- Server/client in userspace
- OpenVPN™ multiplexes everything
  - Uses port 1194 (UDP or TCP)
  - Can (ab)use proxies through HTTP
- Provides authentication and encryption

DeepSec Vienna 2007
7 Layers of Insecurity

OpenVPN™ Cryptography

- Static key
  - HMAC send/receive key
  - Data decrypt/encrypt
- SSL/TLS keys & certificates
- HMAC signature for all VPN packets
  - Protects SSL/TLS, no DoS, no scanning
- OpenVPN™ can authenticate TLS handshake
  - PSK or static key is used
  - Attacker can't start TLS at all

DeepSec Vienna 2007
7 Layers of Insecurity



Mitigation:

• Establish a proper PKI for OpenVPN™ deployment.

• Test your OpenVPN™ implementation with test tools and random data.

OpenSSH

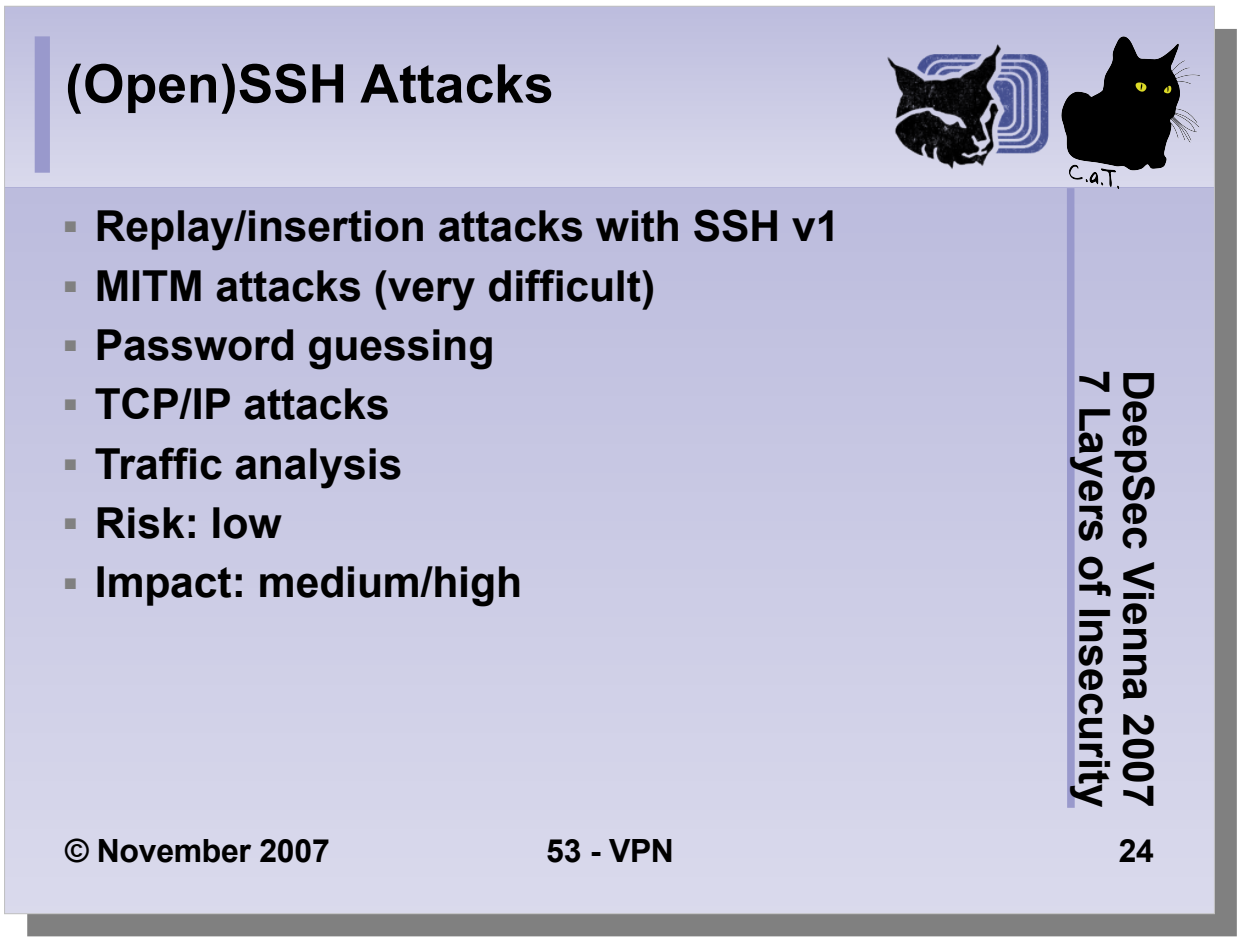
- **Secure Shell Connections with Tunnel.**

DeepSec Vienna 2007
7 Layers of Insecurity

SSH and OpenSSH

- Secure Shell replaces rsh, rlogin, telnet, rcp
- TCP tunnels possible
  - Port and X forwarding
- Integrity protection, host identification
- Lots of authentication methods
  - Passwords or keys with passphrases
  - Smart Cards, PKI, One Time Passwords
  - Kerberos

DeepSec Vienna 2007
7 Layers of Insecurity



OpenSSH knows different SSH protocols (v1, v1.5, v2, compatibility modes). SSH v1 has a weakness in its CRC-32 checksumming and may allow insertion attacks. There is also a possibility to stage a MITM attack, but this requires getting the private server host key. SSH can't do anything against TCP/IP attacks or traffic analysis (in terms of volume and addresses used).

Mitigation:

• Limit access to SSH ports (22/TCP).

• Don't allow interactive username/password logins. Use keys with passphrases instead.

Further reading:

• OpenSSH security information

• Detailed Review of SSH

Other VPN Implementations

- The Key is Out There.

DeepSec Vienna 2007
7 Layers of Insecurity

VPN Implementations

- CIPE
  - Crypto IP Encapsulation
- vtun
  - Supports layer 2/3 tunnel
  - Uses Blowfish 128 bit and PSK
- tinc
- Hamachi
  - Proprietary VPN tool

DeepSec Vienna 2007
7 Layers of Insecurity

Chapter 53
VPN

- Summary
  - Always check implementation.
  - Use known secure algorithms.
  - Be careful when using certificates.
  - Protect and change your keys.

DeepSec Vienna 2007
7 Layers of Insecurity

Thank You

- Questions?

DeepSec Vienna 2007
7 Layers of Insecurity