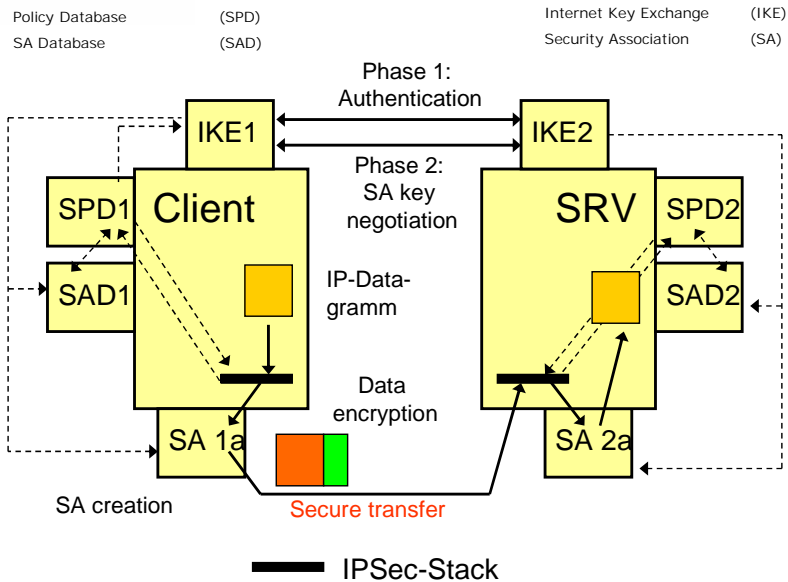


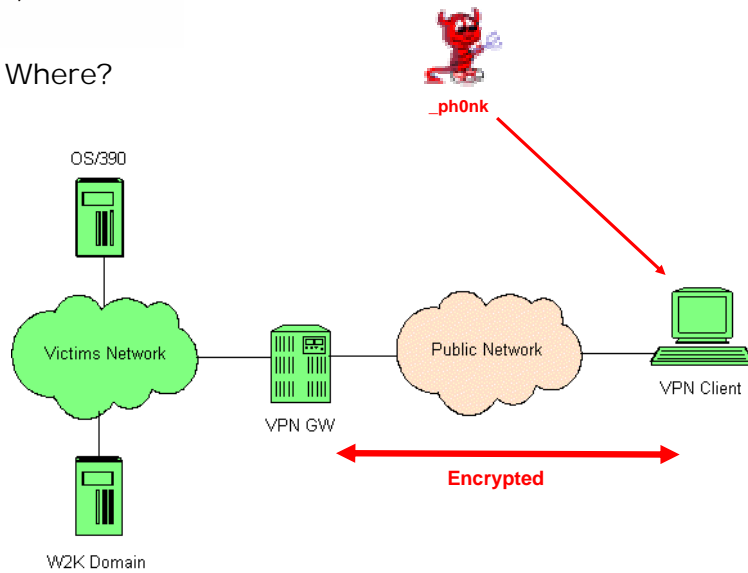
VPN Threat Analysis

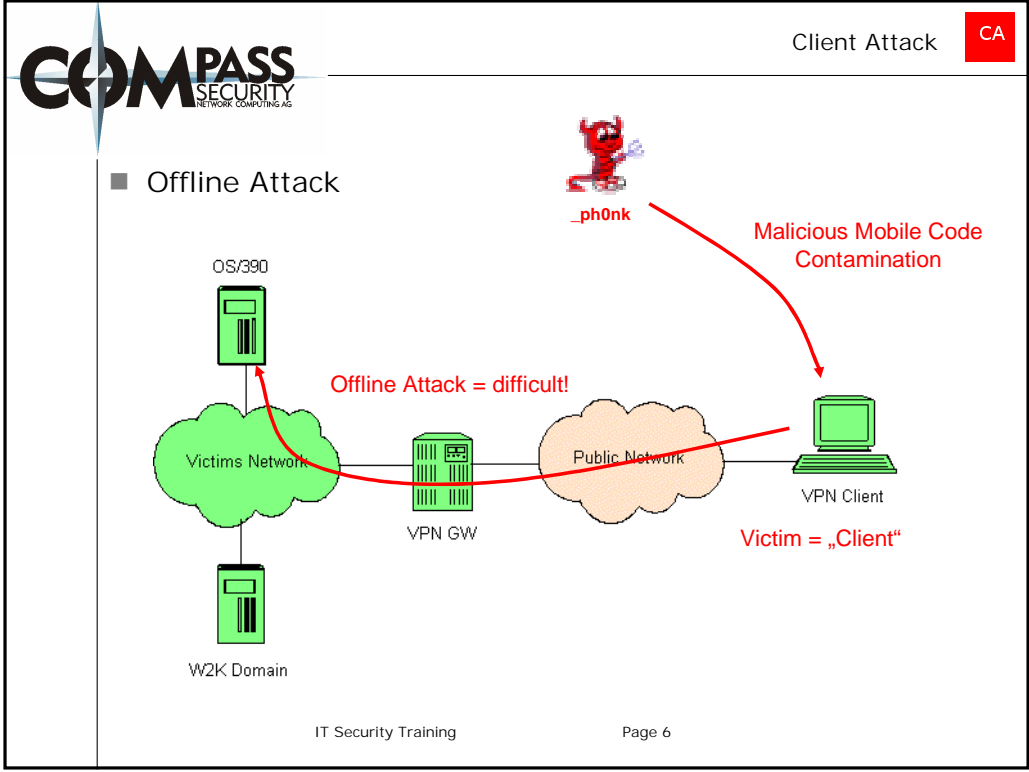
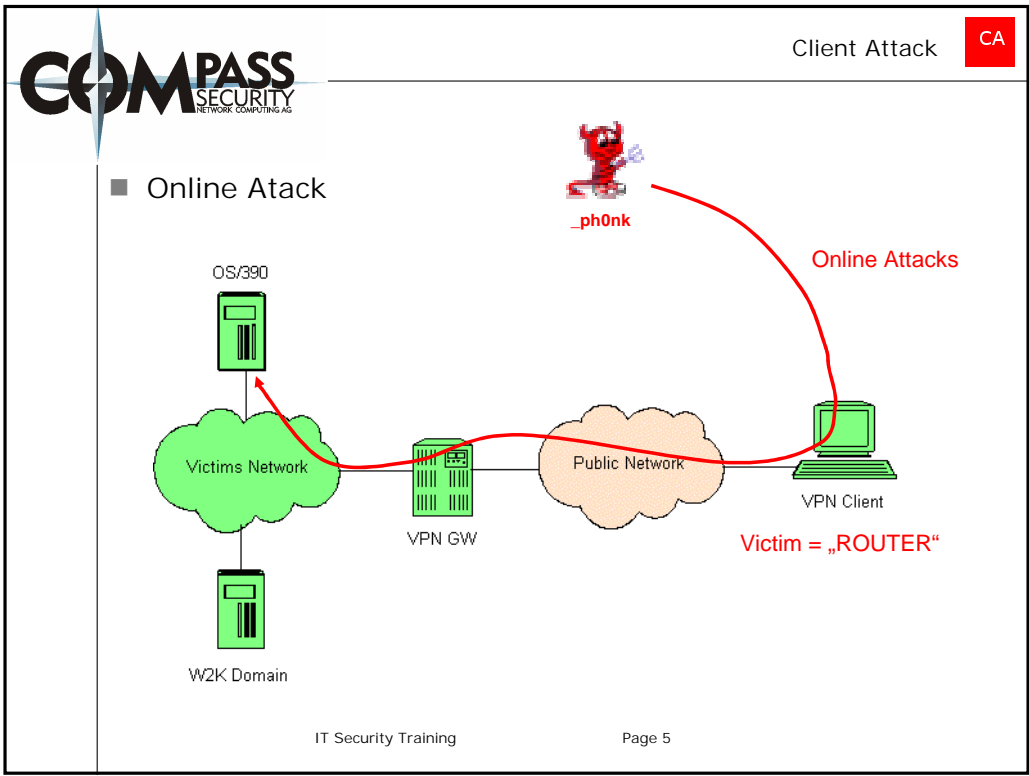
ivan.buetler@csnc.ch

- VPN
 - IPSEC
 - L2TP Layer 2 Tunneling Protocol
 - SKIP SUN Microsystems

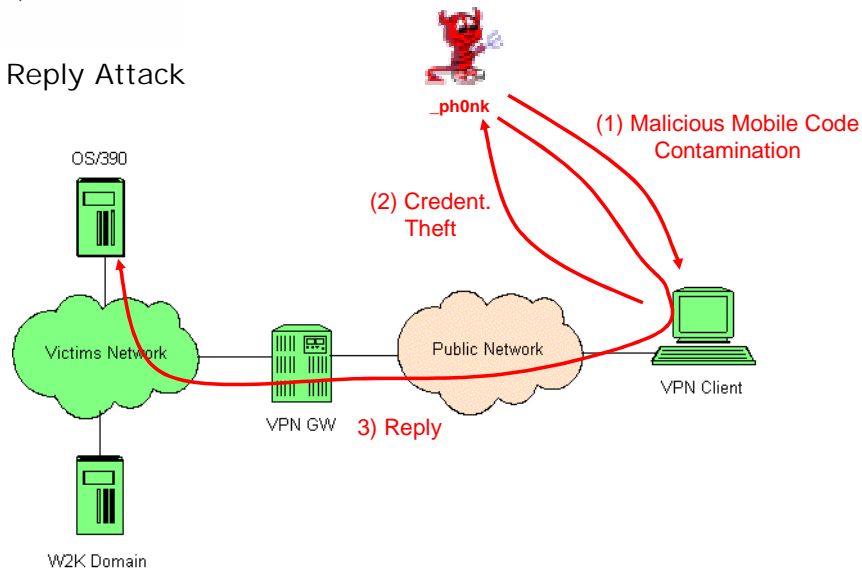


Where?





■ Reply Attack



■ HIGH Security Solution

- Hardware
 - The firm **owns** and **delivers** the VPN client
 - Home PC's are denied
- Internet Access
 - The firm becomes the clients ISP
 - The firms perimeter security mechanisms is protecting the client
 - The VPN client is "part" of the corporate network
- Policy
 - Receive the policy from the VPN gateway (authenticated download)
 - Any changes to the current local policy drops all sessions
- Policy Settings
 - While VPN down = all packets from and to VPN client are dropped
 - While VPN up = all traffic is sent to the gateway

■ MEDIUM Security Solution

- Hardware
 - The firm owns and delivers the VPN client to the managers
 - Home PC's are allowed (costs)
- Internet Access
 - Direct Internet access or via corporate network is possible
- Policy
 - Receive the policy from the VPN gateway (authenticated download)
 - Any changes to the current local policy drops all sessions
- Policy Settings
 - While VPN down = Internet LAN access allowed
 - While VPN up = Internet LAN access disabled
- Potential Attack
 - Offline Attack and Reply Attack

■ LOW Security Solution

- Hardware
 - The firm owns and delivers the VPN client to the managers
 - Home PC's are allowed (costs)
- Internet Access
 - Direct Internet access or via corporate network is possible
- Policy
 - Receive the policy from the VPN gateway (authenticated download)
 - Any changes to the current local policy drops all sessions
- Policy Settings
 - While VPN down = Internet LAN access allowed
 - While VPN up = Internet LAN access allowed
- Potential Attack
 - Online attack

- Authentication Identifier

- Definition:
 - A) Username
 - B) Password
 - C) PIN (OTP = one-time-password)
- Active Attack (keystroke sniffer installation)
 - Auth(A,B) = **high risk** = **long-term compromise possible**
 - Auth(A,B,C) = **low risk**
- Passive Attack (lost VPN client)
 - Auth(A,B) = **medium risk** = pw policy defines security level
 - Auth(A,B,C) & OTP device lost = **medium risk** = pw policy defines security level

- Recommendation

- Give your employees a VPN business computer
- Be the ISP for your employees
- Deny any LAN traffic beside VPN traffic
- Use of OTP (one-time password)
- Apply "strong" password policy for the VPN clients

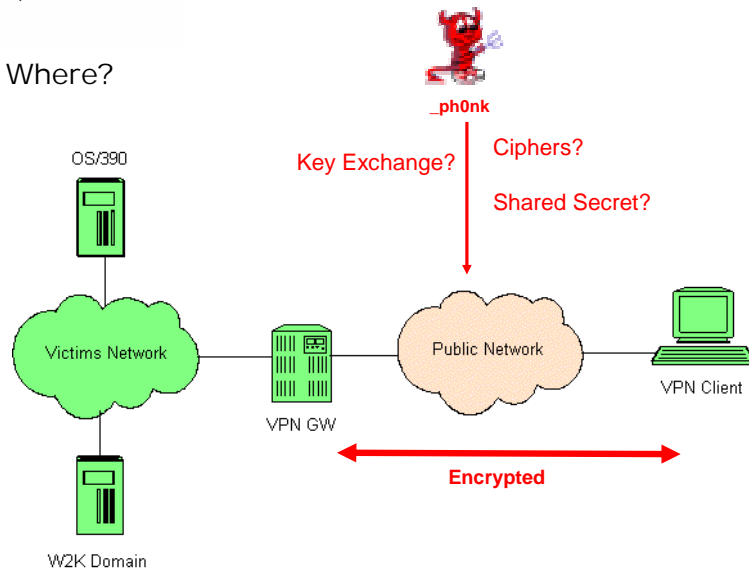
Keep in mind...

Whatever you do on the client,
the best policy can not protect
from high skilled hackers, able to
bypass TCP/IP stacks by their
own technique.

VPN clients are always a threat
because it is a bridge into the
heart of the company

Interception

■ Where?



Initial Key Exchange Problem

- Authentication in IPSEC
 - Pre-shared keys
 - Digital **Signatures** using DSA
 - Public Key **Encryption** using RSA
 - Revised Mode of Public Key **Encryption** (faster)

**IPSEC standard authenticates
"devices"**

- Hybrid Mode (Expanded IPSEC standard)
 - A method of using Authentication Schemes other than Pre-shared Secret, or a Digital Certificate
 - Legacy Systems like:
 - Token Cards – SecurID, etc.
 - LDAP
 - Radius
 - NT Domain
 - FW-1 PW
 - Kerberos

<http://www.ietf.org/internet-drafts/draft-hoffman-sla-00.txt>

■ Security Advisory

Checkpoint FW-1 VPN Security Flaw (updated)

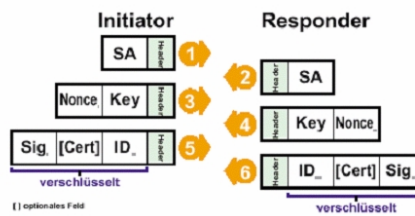
<http://www.securiteam.com/securitynews/5TP040U8AW.html>

- Username Guessing
- Username Sniffing

A real threat?

■ Cryptography

- IKE Main Mode
 - Main Mode is recommended (Identity protection)



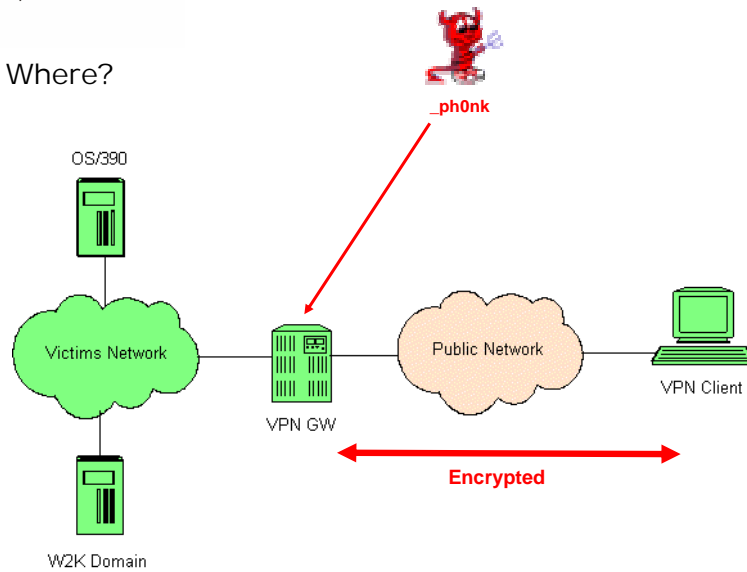
- Cryptography
 - IKE Aggressive Mode



Abb. 8. IKE Aggressive Mode.

- IKE
 - Use of "Main Mode"
 - If using Aggressive Mode
 - Certificate based authentication is recommended

■ Where?



■ Known VPN Server/GW Attacks

- DoS
 - Multiple IPSEC Implementations Do Not Adequately Validate Authentication Data (DoS) 24.10.2002
- IKE identification
- Unauthenticated topology download
- Username guessing
- Implementation
 - Cisco VPN 3000 Concentrator Vulnerabilities (5.9.2002)
„a VPN client logging in using PPTP or IPSEC user authentication succeeds by using a group name/password as login credentials“
 - PIX peer-authentication vulnerability (Nov. 2002)

- Security Actions
 - Trace bugtraq and patch
 - Alarming and alerting (IDS)
 - Username guessing
 - Faked client certificate

VPN DEMO

PPTP

1. What did Bruce Schneier and Mudge actually do?

They found security flaws in Microsoft PPTP that allow attacks to *sniff passwords* across the network, break the encryption scheme and read confidential data, and mount denial of service attacks against PPTP servers. They did not find flaws in PPTP, only in Microsoft's implementation of it.

2. How bad is PPTP?

Very.

Microsoft PPTP is very broken, and there's no real way to fix it without taking the whole thing down and starting over. This isn't just one problem, but six different problems, any one of which breaks the protocol.

3. How good is IPSEC?

N. Ferguson and B. Schneier

We perform a cryptographic review of the IPsec protocol, as described in the November 1998 RFCs. Even though the protocol is a **disappointment**--our primary complaint is with its complexity--it is the best IP security protocol available at the moment.

4. Questions

Ivan Bütler