

Sicherheitsprobleme IPsec-basierter VPNs & die technische Realisierung von SSL-basierten VPNs

**Enno Rey, erey@ernw.de
CISSP, CISA, BS 7799 Lead Auditor**



ERNW



- Gegründet Sommer 2001 durch Enno Rey
- Netzwerk-Dienstleister mit Sicherheits-Fokus
- Aktuell neun Mitarbeiter
- Schwerpunkte: Security Management, Audit/Revision, Security Research, Penetrations-Tests
- Kunden: Industrie, Banken, Behörden, Provider



Agenda



- Sicherheitsprobleme IPsec-basierter VPNs
- Darstellung der Technologie SSL-basierter VPNs
- Sicherheits-Bewertung SSL-basierter VPNs
- Diskussion



Typische Probleme IPsec-basierter VPNs ([1])



- Vernachlässigung der Sicherheit der (mobilen) Endpunkte
- Fehlendes Verständnis grundlegender IPsec-Funktionalität beim zuständigen Personal
- Großflächiger Einsatz mangelhafter Authentifizierung
- Überfrachtete Erwartungen [=> Konfiguration nach Funktionalitäts-, nicht nach Sicherheitskriterien]
- Missachtung von *Segregation of Duties*



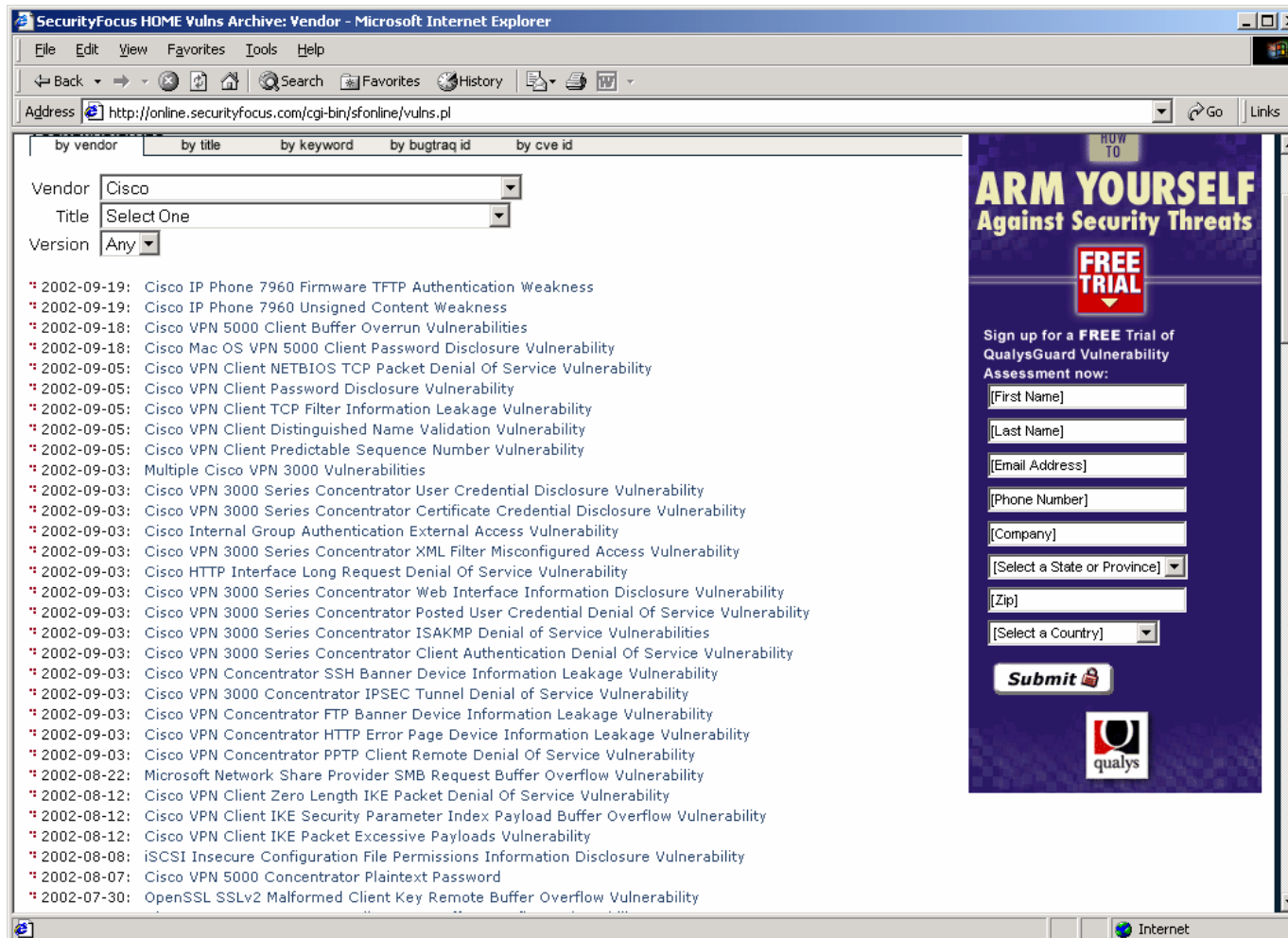
Vernachlässigung der Sicherheit der mobilen Endpunkte



- Endpunkte von VPN-Verbindungen sitzen virtuell im LAN => sie sollten auch ebenso behandelt werden
(oder: „was nützt mir x-fache Authentifizierung mit State-of-the-Art Technologie, wenn der Endpunkt über weitere aktive Netzwerkverbindungen verfügt und dort Filesharing-Tools laufen?“).
Dies ist ein organisatorisches Problem und nur bedingt mithilfe von Technologie zu lösen.
- VPN-Komponenten sind... nicht immer ausgereift...



Vernachlässigung der Sicherheit der mobilen Endpunkte



SecurityFocus HOME Vulns Archive: Vendor - Microsoft Internet Explorer

Address: http://online.securityfocus.com/cgi-bin/sfonline/vulns.pl

by vendor by title by keyword by bugtraq id by cve id

Vendor: Cisco
Title: Select One
Version: Any

- * 2002-09-19: Cisco IP Phone 7960 Firmware TFTP Authentication Weakness
- * 2002-09-19: Cisco IP Phone 7960 Unsigned Content Weakness
- * 2002-09-18: Cisco VPN 5000 Client Buffer Overrun Vulnerabilities
- * 2002-09-18: Cisco Mac OS VPN 5000 Client Password Disclosure Vulnerability
- * 2002-09-05: Cisco VPN Client NETBIOS TCP Packet Denial Of Service Vulnerability
- * 2002-09-05: Cisco VPN Client Password Disclosure Vulnerability
- * 2002-09-05: Cisco VPN Client TCP Filter Information Leakage Vulnerability
- * 2002-09-05: Cisco VPN Client Distinguished Name Validation Vulnerability
- * 2002-09-05: Cisco VPN Client Predictable Sequence Number Vulnerability
- * 2002-09-03: Multiple Cisco VPN 3000 Vulnerabilities
- * 2002-09-03: Cisco VPN 3000 Series Concentrator User Credential Disclosure Vulnerability
- * 2002-09-03: Cisco VPN 3000 Series Concentrator Certificate Credential Disclosure Vulnerability
- * 2002-09-03: Cisco Internal Group Authentication External Access Vulnerability
- * 2002-09-03: Cisco VPN 3000 Series Concentrator XML Filter Misconfigured Access Vulnerability
- * 2002-09-03: Cisco HTTP Interface Long Request Denial Of Service Vulnerability
- * 2002-09-03: Cisco VPN 3000 Series Concentrator Web Interface Information Disclosure Vulnerability
- * 2002-09-03: Cisco VPN 3000 Series Concentrator Posted User Credential Denial Of Service Vulnerability
- * 2002-09-03: Cisco VPN 3000 Series Concentrator ISAKMP Denial of Service Vulnerabilities
- * 2002-09-03: Cisco VPN 3000 Series Concentrator Client Authentication Denial Of Service Vulnerability
- * 2002-09-03: Cisco VPN Concentrator SSH Banner Device Information Leakage Vulnerability
- * 2002-09-03: Cisco VPN 3000 Concentrator IPSEC Tunnel Denial of Service Vulnerability
- * 2002-09-03: Cisco VPN Concentrator FTP Banner Device Information Leakage Vulnerability
- * 2002-09-03: Cisco VPN Concentrator HTTP Error Page Device Information Leakage Vulnerability
- * 2002-09-03: Cisco VPN Concentrator PPTP Client Remote Denial Of Service Vulnerability
- * 2002-08-22: Microsoft Network Share Provider SMB Request Buffer Overflow Vulnerability
- * 2002-08-12: Cisco VPN Client Zero Length IKE Packet Denial Of Service Vulnerability
- * 2002-08-12: Cisco VPN Client IKE Security Parameter Index Payload Buffer Overflow Vulnerability
- * 2002-08-12: Cisco VPN Client IKE Packet Excessive Payloads Vulnerability
- * 2002-08-08: iSCSI Insecure Configuration File Permissions Information Disclosure Vulnerability
- * 2002-08-07: Cisco VPN 5000 Concentrator Plaintext Password
- * 2002-07-30: OpenSSL SSLv2 Malformed Client Key Remote Buffer Overflow Vulnerability

ARM YOURSELF
Against Security Threats

FREE TRIAL

Sign up for a **FREE** Trial of QualysGuard Vulnerability Assessment now:

[First Name]
[Last Name]
[Email Address]
[Phone Number]
[Company]
[Select a State or Province]
[Zip]
[Select a Country]

Submit

qualys



Fehlendes Verständnis grundlegender IPsec-Funktionalität beim zuständigen Personal



Oder sollten wir fragen:

- Setzt jemand von Ihnen IPsec-basierte VPNs ein?
- Falls ja... was ist IKE? XAuth? Hybrid Mode?
[einiges davon verwenden Sie mit hoher Wahrscheinlichkeit]
- Können Sie mir erklären, warum der *aggressive mode* potentiell unsicherer ist als der *main mode*... oder was das überhaupt ist?
- Ist der *hybrid mode* sicherer als rein Zertifikat-basierter *main mode* ... oder warum setzen Sie dann diesen oder jenen ein?
- Sie setzen keinen von beiden ein, sondern den *aggressive Mode* mit *preshared key* [und variablen Endpunkten]? Na dann...



Eine übliche IPsec-Installation verläuft in etwa so:



[beteiligt sind Admin A und Admin B an einem Freitag gegen 19:00 Uhr]

- Admin A: Läuft's endlich?
- Admin B: Nein. Ich versteh' aber nicht, weshalb nicht.
- Admin A: Probier' doch mal den Parameter X.
- Admin B: Funktioniert auch nicht... ich könnte aber 'mal Parameter Y verwenden.
- Admin A: Wieso?
- Admin B: Weiß ich auch nicht... war nur so'ne Idee.
- Admin A: Ich teste mal... jetzt geht's!!
- Admin B: Kapierst Du, weshalb es nun funktioniert?
- Admin A: Nein, ich speicher' aber jetzt die Einstellungen [und fass es bloss nie wieder an!].
- Admin B: Na dann... schönes Wochenende!



Großflächiger Einsatz mangelhafter Authentifizierungsverfahren



- Ein möglicher Modus des IKE (der sog. *aggressive mode*) weist bei Authentifizierungsverfahren PSK (*pre-shared keys*) eine gravierende Design-Schwäche/Sicherheitslücke auf (vgl. [2]).
- Das Problem ist lange bekannt ([3]) und nur eines der Design-Probleme von IPsec (zu anderen siehe etwa [4]).
- Das Problem wird meist für mobile User durch den Einsatz Hersteller-proprietärer IPsec-Erweiterungen *verringert*.

aber...

- Auch einige dieser Verfahren haben Schwächen (bspw. MITM-Angriffe gegen XAUTH).
- Und was machen denn eigentlich die User, die nicht per Client-Software, sondern über einen DSL-Router zugreifen...
- => es gibt Design-basierte Schwächen bei IPsec



PSK Cracking

```
Take Command/32
File Edit Apps Options Utilities Help
Nikto DNSDigger NMap CMD IKE Nemesis RPC Foundstone Sysinternals Reskit Exploits NetShell
d339d63d51829b455088a790523c24dc33d6dd0d57f329d56114613d047b16
448f513639d1f43b58f518d47e19be0d6426b345
nonce_r      : 91d69fd275a63e6ae5df7b0e0f0f073638500f7c
ID_r        : 010000000a010101
HASH_r      : b39a2f234365f1186fbf8645896598e5

Header IPs 10.1.1.62.500 10.1.1.1.500:
Header IPs 10.1.1.1.500 10.1.1.62.500:
Header IPs 10.1.1.1.500 10.1.1.62.500:
Header IPs 10.1.1.1.500 10.1.1.62.500:
Header IPs 10.1.1.1.500 10.1.1.62.500:
Header IPs 10.1.1.1.500 10.1.1.62.500:
Header IPs 10.1.1.1.500 10.1.1.62.500:
Header IPs packets by

Initiator_ID - Type is IPv4: 10.1.1.62
Responder_ID - Type is IPv4: 10.1.1.1
Responder Sent MD5 HASH_R : b39a2f234365f1186fbf8645896598e5

Starting Grinder.....

Reading Dictionary File
Starting Dictionary Attack:
match with password
Calc MD5 HASH_R : b39a2f234365f1186fbf8645896598e5
Calc SKEYID : 5071dc3ae86fcae25295f3e80196da9c

root@Mozilla[c:\...\ikecrack]:|

2.11.2003 10:25:41 CPU: 20% Load: 49%
```



PSK Cracking



We Secure the Internet

CONNECT PROTECT MANAGE ACCELERATE

Home Solutions & Products How to Buy Services & Downloads Company Partners My Account

Search go

SOLUTIONS & PRODUCTS
> Enterprise
> Branch Office
> Service Provider
> Industries
> Small Business
> Home Computing
> Wireless

HIGHLIGHTS
> Platform Selection Guide
> Network Security Glossary

VPN Brute Force Attack (IKE Aggressive Mode) Public Advisory

Attack ID:	CPSA-2003-04
Last Update:	24-Apr-03
Category:	VPN brute force attack (IKE aggressive mode)
Vulnerable Systems:	VPN systems using IKE aggressive mode and Pre-shared secrets
Source:	Enno Rey Netzwerke GmbH: PSK Cracking using IKE Aggressive Mode
Description:	There is a known vulnerability for systems using Aggressive Mode with pre-shared keys (passwords). In this particular scenario, it is possible for an attacker to gather all necessary information in order to mount an off-line dictionary (brute force) attack on the pre-shared keys.
Severity:	High

IPSEC based Remote Access  be intercepted on a hostile network and manipulated while the user is unaware of such activity. While an attacker can not decrypt the VPN session itself, he can use the sniffed session to discover the Pre-shared VPN password to impersonate a trusted user and connect to the protected network, or it can mount an active Man-in-The-Middle attack on any new session.

▶ [Read the FULL ADVISORY and SOLUTION \(ID and Password Required\)](#)

[Legal Notice for SmartDefense Advisories](#)

Copyright | [Contact Us](#) | [Site Feedback](#) | [Privacy Policy](#) | [Site Map](#)



Die eierlegende Wollmilchsau



- VPNs sollen Remote-Zugriff *ermöglichen*, leicht konfigurierbar & administrierbar sein, am besten wenig kosten...
und, ach ja, auch noch sicher sein
=> oft wird schon die Konfiguration an solchen Kriterien ausgerichtet

[reale Produktiv-Konfig, Key unkenntlich]:

```
crypto isakmp key xyz address 217.227.0.0 255.255.0.0 no-xauth
```

```
crypto isakmp key xyz address 217.83.0.0 255.255.0.0 no-xauth
```

```
crypto isakmp key xyz address 80.131.0.0 255.255.0.0 no-xauth
```

!! bei kaum einem anderen Sicherheits-Instrument wird in der alltäglichen Administration so sehr *Funktionalität* fokussiert!

=> Problem im Umgang mit der Technologie



Missachtung von Segregation of Duties



Eine Firewall ist eine Firewall ist eine Firewall...

- ... und **kein** Crypto-Device
 - => beide Funktionalitäten auf einer Komponente zu vereinen, stellt ein **gravierendes Design-Problem** dar,
 - denn: Kompromittierung des VPN-Gateways ist dann = Kompromittierung der Firewall!
- => Problem im Umgang mit Technologie
- Dieser Zusammenhang sollte insbesondere bei neuen Technologien bedacht werden...



Zusammenfassung der möglichen Probleme bei IPsec



- Sicherheitsprobleme entstehen nicht durch das Übertragungsprotokoll, sondern durch die Endpunkte (sei es durch mangelhafte Implementierungen oder durch organisatorische Vernachlässigung).
- Das Protokoll in sich kann Design-Schwächen haben.
- Die Technologie wird falsch eingesetzt.
- Durch den Einsatz können neue Sicherheitslücken bestehender Komponenten auftreten.



Technologischer Überblick SSL-basierter VPNs



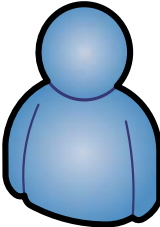
Wenn von *SSL-basierten VPNs* die Rede ist, lassen sich üblicherweise drei technologische Varianten unterscheiden:

- Var1: Das „VPN-Gateway“ fungiert als *reverse proxy* für den externen Zugriff auf Web-basierte Applikationen.
- Var2: Mittels einer Browser-basierten Applikation wird (über SSL) eine Art grafischer Remote Terminal-Funktionalität (vergleichbar ICA- oder RDP-Zugriff) bereitgestellt.
- Var3: Client-seitig wird ein VPN-Client installiert, der nicht über IPsec, sondern eben über SSL funktioniert.



Var1: VPN-Gateway als reverse proxy

User mit Browser



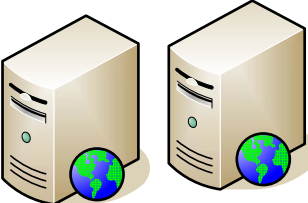
HTTP über SSL



„VPN-Gateway“



Server m. Web-Applikationen
oder Portal(en)



VPN-Gateway als reverse proxy

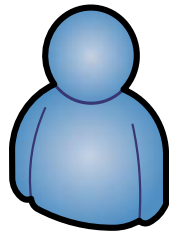


- Technologie: VPN-Gateway operiert als *reverse proxy* und SSL-Terminierer
- Client-Komponente: Browser
- Authentifizierung des Clients: beliebig, meist Passwort-basiert
- Authentifizierung des Gateways: Zertifikat (durch wen ausgestellt?)
- Applikations-Zugriff: nur Web-Applikationen
- Zielgruppe: alle Mitarbeiter oder Externen, die Zugriff auf Web-Applikationen benötigen



Var2: VPN-Gateway stellt grafisches Remote-Terminal bereit

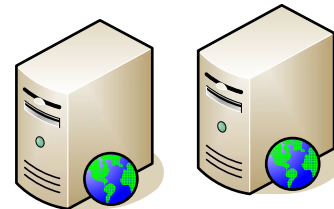
User mit Browser +
Client-seitige (z.B.
JAVA-) Applikation



HTTP + JAVA über SSL



„VPN-Gateway“, das seinerseits
typische (Client-) Applikationen [etwa
SAP-GUI oder Notes-Client] ‚publiziert‘
und mit JAVA-Applikation des Clients
kommuniziert



Systeme mit Server-Diensten (SAP,
MS Exchange, Lotus Notes)



VPN-Gateway stellt grafisches Remote-Terminal bereit

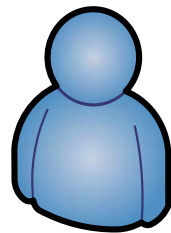


- Technologie: VPN-Gateway operiert als Applikations-Gateway, das an den Web-basierten Client eine JAVA-Applikation aushändigt, die eine Art grafisches Remote-Terminal für Applikationen bereitstellt, deren Client-Komponenten (SAP-GUI, Notes Client) wiederum vom VPN-Gateway ‚publiziert‘ werden.
- Client-Komponente: Browser + JAVA-Applikation
- Authentifizierung des Clients: beliebig, meist Passwort-basiert
- Authentifizierung des Gateways: Zertifikat (durch wen ausgestellt?)
- Applikations-Zugriff: Web-basierte Applikationen + diverse Client/Server-Applikationen
- Zielgruppe: alle Mitarbeiter oder Externen, die Zugriff auf solche Applikationen benötigen (ohne dass ein Deployment einer Client-SW möglich/notwendig wäre). D.h. ausdrücklich etwa auch User im Internet-Cafe...



Var3: Client-seitig wird SSL-basierter VPN-Client installiert

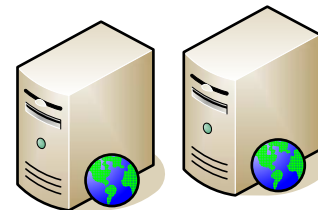
User mit beliebiger Applikation
(aber *installiertem* VPN-Client)



TCP/UDP über SSL



„VPN-Gateway“ als
(SSL-) Tunnelendpunkt



Beliebige Kommunikations-
Endpunkte



Client-seitig wird SSL-basierter VPN-Client installiert



- Technologie: vergleichbar üblichem IPsec-basierten Zugriff mittels einer dedizierten Client-Komponente, die den IP-Stack modifiziert
- Client-Komponente: installierter VPN-Client, beliebige Applikation
- Authentifizierung des Clients: beliebig, meist Passwort-basiert
- Authentifizierung des Gateways: Zertifikat (durch wen ausgestellt?)
- Applikations-Zugriff: beliebige Applikationen
- Zielgruppe: typischer ADM, der über Corporate-Laptop verfügt und vielfältigen Applikations-Zugriff benötigt.



Nochmals die o.g. Thesen zu Sicherheitsproblemen bei IPsec



- Endpunkt-Problematik
- Protokoll-Design & -Schwächen
- Mangelndes Knowhow bei Sysadmins
- Einsatz ohne ausreichende Risiko-Analyse (neue Sicherheits-Risiken durch neue Technologie?)



Endpunkt-Problematik



- Die Client-seitige Komponente in den Varianten 1 und 2 ist... der Browser...
- Hallo? Jawohl, der *Browser*...
- Provokant gefragt: *kann* der Schritt zu Browser-basierten Applikations-Zugriffen heutzutage ein Sicherheits-*Gewinn* sein?
- Will ich wirklich, dass ein User im Internet-Cafe auf die Corporate ERP-Anwendung zugreifen kann? Und sich dabei über sein übliches Windows-PW authentifiziert?
- Warum sollte angesichts der aktuellen ‚Markt-Begeisterung‘ die Client-Software in Var. 3 *keine* Kinderkrankheiten (wie ehemals die meisten IPsec-Clients) haben?



Protokoll-Design & -Schwächen

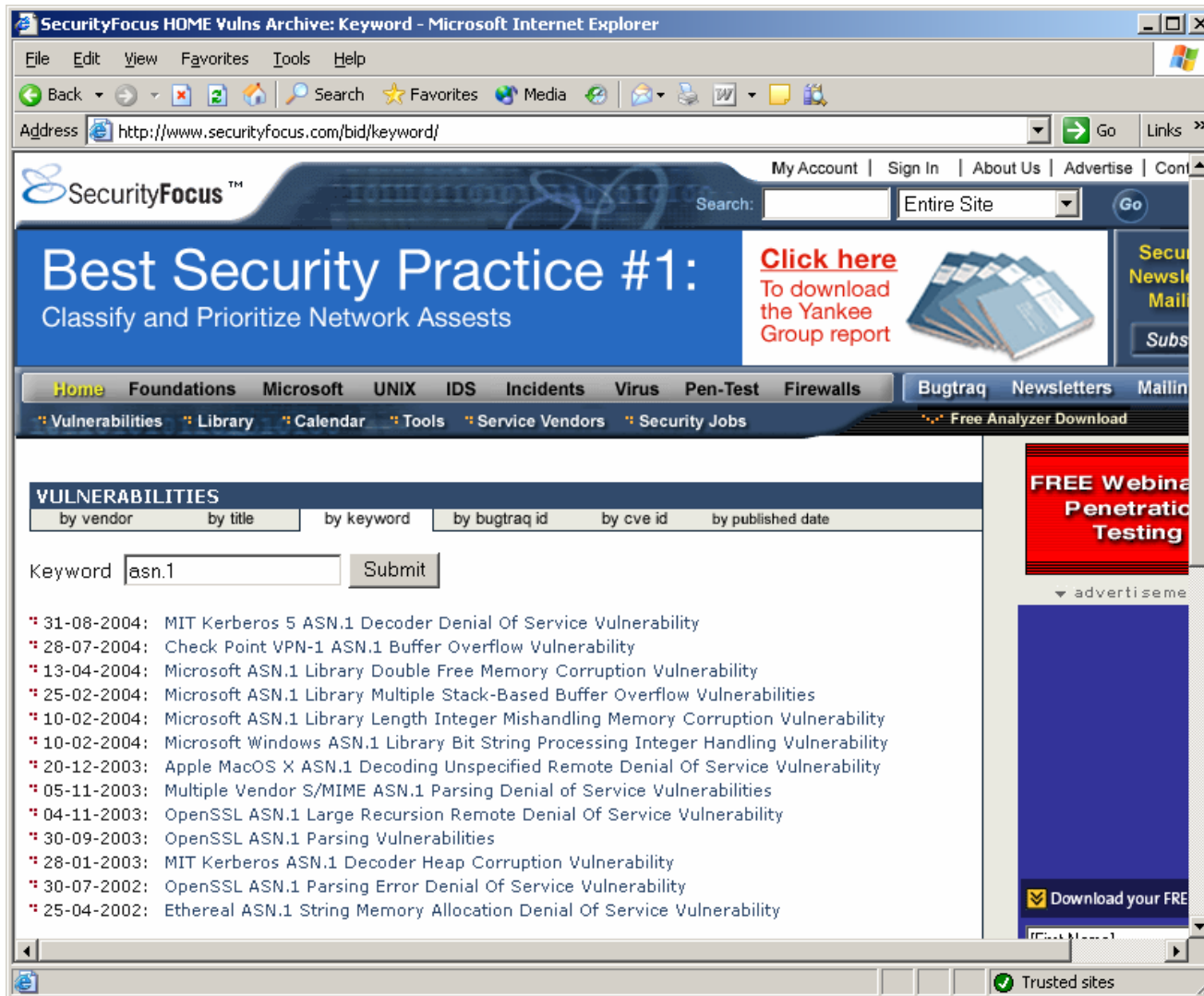


Mögliche Probleme von SSL:

- Bei vielen SSL-Implementierungen sind schwache Verfahren verhandelbar (NULL Encryption, 40Bit-Verfahren, DES).
- Diverse SSL-Implementierungen (auch in Appliances) sind *openssl*-basiert...
- SSL basiert hochgradig auf *ASN.1*. *ASN.1* gilt als die moderne ‚Büchse der Pandora‘ vieler Krypto-Mechanismen (aktuelles Beispiel: MIT Kerberos).

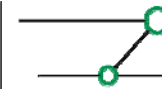


ASN.1



The screenshot shows a Microsoft Internet Explorer browser window displaying the SecurityFocus website. The address bar shows the URL <http://www.securityfocus.com/bid/keyword/>. The page features a navigation menu with categories like Home, Foundations, Microsoft, UNIX, IDS, Incidents, Virus, Pen-Test, Firewalls, Bugtraq, Newsletters, and Mailin. A search bar is visible with the text "Entire Site" and a "Go" button. Below the navigation, there is a section titled "VULNERABILITIES" with a search input field containing "asn.1" and a "Submit" button. The search results are listed as follows:

- * 31-08-2004: MIT Kerberos 5 ASN.1 Decoder Denial Of Service Vulnerability
- * 28-07-2004: Check Point VPN-1 ASN.1 Buffer Overflow Vulnerability
- * 13-04-2004: Microsoft ASN.1 Library Double Free Memory Corruption Vulnerability
- * 25-02-2004: Microsoft ASN.1 Library Multiple Stack-Based Buffer Overflow Vulnerabilities
- * 10-02-2004: Microsoft ASN.1 Library Length Integer Mishandling Memory Corruption Vulnerability
- * 10-02-2004: Microsoft Windows ASN.1 Library Bit String Processing Integer Handling Vulnerability
- * 20-12-2003: Apple MacOS X ASN.1 Decoding Unspecified Remote Denial Of Service Vulnerability
- * 05-11-2003: Multiple Vendor S/MIME ASN.1 Parsing Denial of Service Vulnerabilities
- * 04-11-2003: OpenSSL ASN.1 Large Recursion Remote Denial Of Service Vulnerability
- * 30-09-2003: OpenSSL ASN.1 Parsing Vulnerabilities
- * 28-01-2003: MIT Kerberos ASN.1 Decoder Heap Corruption Vulnerability
- * 30-07-2002: OpenSSL ASN.1 Parsing Error Denial Of Service Vulnerability
- * 25-04-2002: Ethereal ASN.1 String Memory Allocation Denial Of Service Vulnerability



Allgemeine Aspekte



- SSL ist weniger komplex als IPsec, gravierende Konfigurations-Fehler sind deshalb seltener zu erwarten.
- Fehlerhafte (SW-) Implementierungen können aber nicht ausgeschlossen werden, weder auf Client-Seite noch auf Gateway-Seite.
- *Segregation of Duties* ist daher sicher hilfreich...
- Der Client-seitige Endpunkt ist wohl noch anfälliger als bei typischen IPsec-Clients.
- => dedizierte Risiko-Analysen Endpunkt-basierter Risiken sind notwendig.

Fazit: der *Security Impact* SSL-basierter VPN-Technologien kann noch nicht abschliessend beurteilt werden. Eine **genaue Evaluierung** d. eingesetzten Techniken und zugehörige **Risiko-Analysen** sind erforderlich.



Offene Fragen & Diskussion



Vielen Dank für Ihre Aufmerksamkeit!



Quellen



- [1] Vortrag *Mobile Security*:
<http://www.ernw.de/publikationen/mobilesecurity.pdf>
- [2] Rey/Thumann – PSK Cracking using IKE Aggressive Mode:
<http://www.ernw.de/publikationen/pskattack.pdf>
- [3] John Pliam – Authentication Vulnerabilities in IKE and Xauth with Weak Pre-Shared Secrets: <http://www.ima.umn.edu/~pliam/xauth/>
- [4] William Allen Simpson – IKE/ISAKMP considered harmful:
<http://www.usenix.org/publications/login/1999-12/features/harmful.html>

