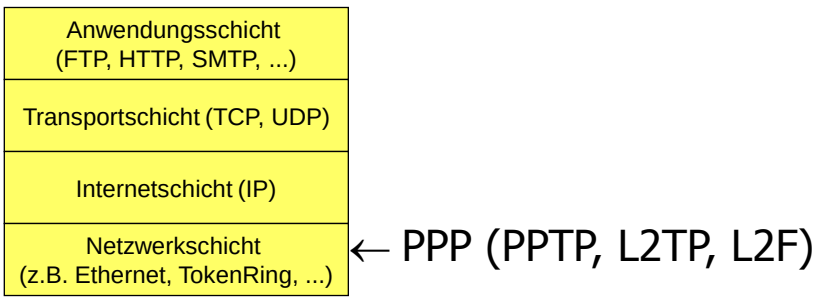
Netzsicherheit 4:
Layer 2-Sicherheit – Das Point-to-Point-Protokoll und seine Erweiterungen

Jörg Schwenk
Lehrstuhl für Netz- und Datensicherheit

Das TCP/IP-Schichtenmodell



Jörg Schwenk
Lehrstuhl für Netz- und Datensicherheit

Gliederung

- Layer 2: Ethernet, ...
- PPP: Point-to-Point protocol
- PAP und CHAP
- AAA: Authentication, Autorisation and Accounting (RADIUS, SecureID)
- PPP-Extensions: L2F, PPTP, L2TP
- Der PPTP-Angriff von Schneier und Mudge

Layer 2: Ethernet & Co

- Übertragungsprotokolle für Teilnetze mit gleicher Technologie
- Ethernet: ursprünglich Broadcast-Netz
- PPP: Punkt-zu-Punkt-Verbindung
- WLAN: Broadcast-Netz
- DVB: Broadcast-Netz mit Fehlerkorrektur

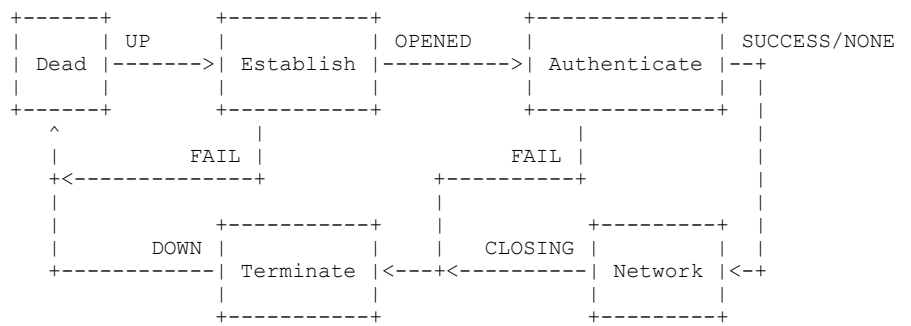
Point-to-Point Protocol (PPP)

RFC 1661: The Point to Point Protocol (PPP). W. Simpson, Juy 1994

- Benötigt: Voll-Duplex, simultane, bidirektionale Verbindung zwischen zwei Hosts (z.B. ISDN)
- Encapsulation: Verpackt beliebige Protokolle
- Link Control Protocol: Aushandlung von PPP-Optionen, auch Authentisierung
- Network Control Protocol: Parameter für höhere Protokolle, z.B. für die Zuweisung von IP-Adressen

Point-to-Point Protocol (2)

Ablauf eines PPP-Verbindungsaufbaus



Point-to-Point Protocol (4)

Ablauf eines PPP-Verbindungsaufbaus

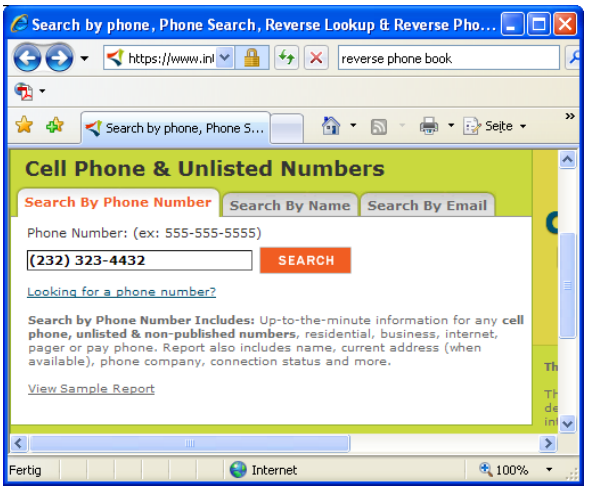
1. PPP-Pakete mit protocol=c021 LCP
2. PPP-Pakete mit protocol=c023 PAP/c223 CHAP
3. PPP-Pakete mit protocol=8*** NCP
4. PPP-Pakete mit protocol=???? IP

RFC 1334: PPP Authentication Protocols

Password Authentication Protocol (PAP)

- Voraussetzung: PPP-Verbindung steht
- Client sendet wiederholt (im Klartext) das Paar (ID, Passwort)
- Network Access Server (NAS) überprüft das Passwort gegen den zur ID gespeicherten Wert (besser: den Hashwert des Passworts)
  - Überprüfung erfolgreich: ACK
  - Überprüfung nicht erfolgreich: NACK

Wörterbuch-Attacken



common-passwords.txt

http://www.openwall.com/wordlists/
- ca. 40 Millionen Passwörter
- entspricht einer Komplexität von 2^{25} - 2^{26}

Wörterbuch-Attacken

- Annahme: Passwörter werden gehasht, oder immer mit dem gleichen Schlüssel verschlüsselt.
- Angreifer bildet den Hashwert aller Worte in einem Wörterbuch.
- Die Paare (Wort, Hashwert) werden nach Hashwert sortiert.
- Ein gehashtes Passwort kann in dieser Liste leicht gefunden werden.
- Funktioniert, weil nur wenige Zeichenkombinationen als Passwörter verwendet werden (kleines Wörterbuch)
- Gegenmaßnahme: Für jeden Benutzer ein öffentlich bekanntes „Salt“ einführen. Das hat zur Konsequenz, dass für jeden Benutzer ein eigenes Wörterbuch angelegt werden muss.

RFC 1994: PPP Authentication Protocols (2)

Challenge Handshake Authentication Protocol (CHAP)

- Voraussetzung: PPP-Verbindung steht
- Network Access Server (NAS) sendet „challenge“-Nachricht
- Client antwortet mit res = hash(secret, challenge)
- NAS überprüft, ob res = hash(secret, challenge) ist
  - Überprüfung erfolgreich: ACK
  - Überprüfung nicht erfolgreich: NACK

PPP-Erweiterungen

- Viele neue Vorschläge zu PPP findet man unter http://ietf.org/html.charters/pppext-charter.html
  - The PPP Encryption Control Protocol (ECP) (RFC 1968)
  - PPP Extensible Authentication Protocol (EAP) (RFC 2284)
  - The PPP DES Encryption Protocol, Version 2 (DESE-bis) (RFC 2419)
  - The PPP Triple-DES Encryption Protocol (3DESE) (RFC 2420)
  - Microsoft PPP CHAP Extensions (RFC 2433)
  - PPP EAP TLS Authentication Protocol (RFC 2716)
  - Microsoft PPP CHAP Extensions, Version 2 (RFC 2759)
  - Microsoft Point-To-Point Encryption (MPPE) Protocol (RFC 3078)
- EAP-Protokolle werden auch im Bereich WLAN intensiv untersucht

AAA: Authentication, Authorization and Accounting

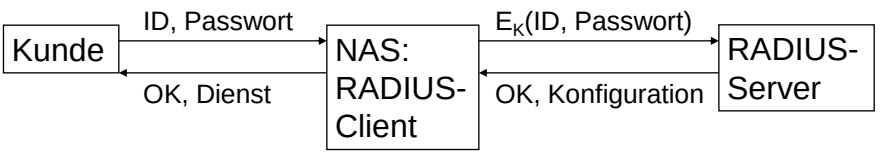
AAA wird vor allem von Internet Service Providern (ISP, z.B. T-Online) benötigt, um gegenüber Kunden abrechnen zu können.

- Architektur: RADIUS (RFC 2058)
- AAA-Protokolle:
  - PAP (meistens)
  - CHAP
  - SecureID
  - Kerberos

Remote Authentication Dial-In User Service (RADIUS)

RFC 2058: RADIUS (Lucent Technologies)

- Client-Server-Lösung zur Authentisierung von Kunden



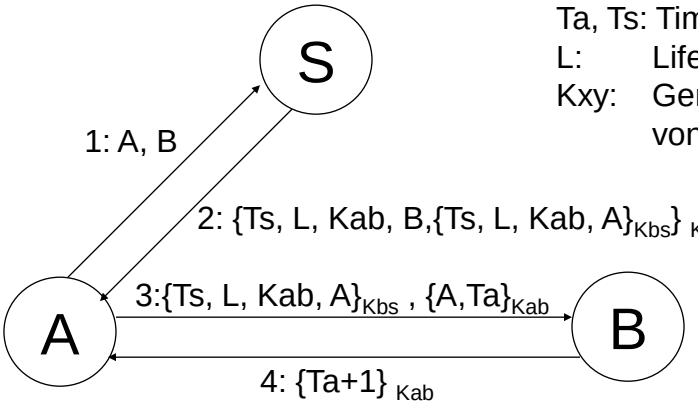
SecureID

Produktlinie von RSA Inc.

- Alle 10 Sekunden wird im Client-Token und im Server eine neue Zufallszahl generiert
- Server überprüft, ob eine gesendete Zufallszahl im zulässigen Zeitfenster liegt.

Kerberos (MIT)

Kerberos wurde 1987 am MIT entwickelt



Ta, Ts: Timestamps
L: Lifetime
Kxy: Gemeinsamer Schlüssel von X und Y

PPP-Verlängerung

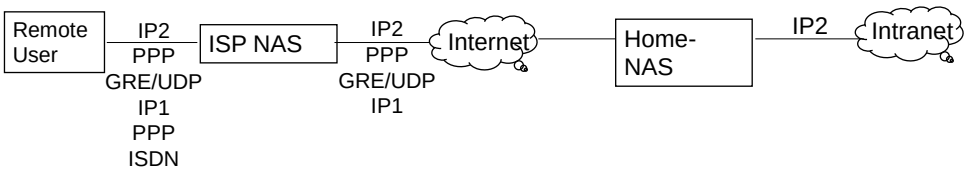
PPP-Verlängerung

- PPP bietet heute die besten AAA-Features
- Viele Außendienst-Mitarbeiter wählen sich über eine direkte Modem-Verbindung und PPP ins Firmennetz ein
- Idee zur Kostensenkung: Einwahl der Mitarbeiter lokal bei einem ISP
  - Verlängere PPP über ein IP Backbone-Netz
  - Authentifizierung am NAS der Firma
- Problem: Verschlüsselung!
  - PAP über PPP übers Internet ist nicht sicher.

PPP-Verlängerung (2)

Client-initiierter Tunnel

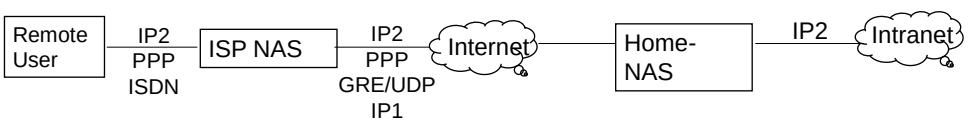
1. Client stellt IP-Verbindung zum NAS der Firma her
2. Client sendet PPP-Pakete über diese Verbindung



PPP-Verlängerung (3)

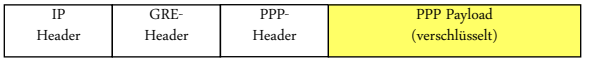
NAS-initiierter Tunnel

1. Client stellt PPP-Verbindung zum NAS des ISP her
2. NAS sendet PPP-Pakete über IP-Verbindung an den NAS der Firma



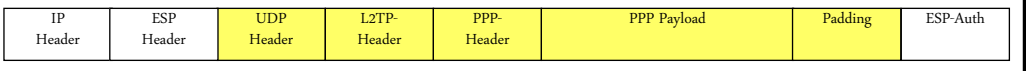
Layer 2: PPTP, NCP

- Einbettung in das TCP/IP-Schichtenmodell:
  - PPTP verlängert PPP mit Hilfe von GRE (Generic Routing Encapsulation)
  - PPTP-Kontrollnachrichten mit TCP
  - Transportnetzwerk: IP
- Verschlüsselung und Authentikation auf PPP-Ebene („link encryption“):
  - Optionales Schlüsselmanagement: Microsoft EAP-TLS
  - Sicherheitsprobleme bei PPTP v1 (Mudge, Schneier, 1998)



Layer 2: L2TP

- „Best of“ PPTP (Microsoft) und L2F (Cisco)
- Einbettung in das TCP/IP-Schichtenmodell:
  - Verlängert PPP-Tunnel mit UDP (auch Kontrollnachrichten)
  - Transportnetzwerk: IP (fertig), X.25, Frame Relay, ATM (geplant)
- Authentikation auf PPP-Ebene (PAP, CHAP, ...)
- Verschlüsselung mit IPSec ESP
- http://ietf.org/html.charters/l2tpext-charter.html



Kryptoanalyse von MS-PPTPv1

- B. Schneier and Mudge, "Cryptanalysis of Microsoft's Point-to-Point Tunneling Protocol (PPTP)," Proceedings of the 5th ACM Conference on Communications and Computer Security, ACM Press, pp. 132-141. http://www.counterpane.com/pptp.html.

Kryptoanalyse von MS-PPTPv1(2)

Authentisierung/Verschlüsselung bei MS-PPTPv1:

1. Passwort im Klartext senden/keine Verschlüsselung möglich
2. Hashwert des Passworts senden/ keine Verschlüsselung möglich
3. MS-CHAP: Hashwert des Passworts wird zum Verschlüsseln der Challenge benutzt/ Verschlüsselung möglich

Kryptoanalyse von MS-PPTPv1(3)

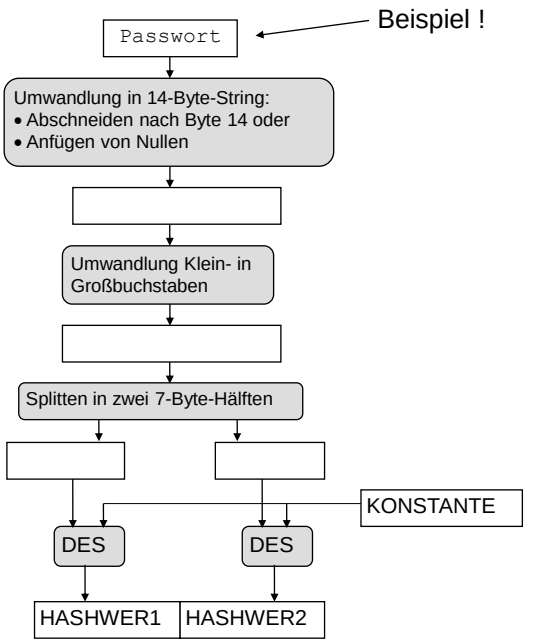
Berechnung von zwei Hashwerten aus dem Passwort:

- Windows NT Hash (sicherere Variante, wird hier nicht betrachtet).
- LAN Manager Hash:
  1. Wandle das Passwort in einen 14-Byte-String um, entweder durch Kürzen längerer Passworte, oder durch Anfügen von Nullen an kürzere Passworte
  2. Wandle alle Klein- in Grossbuchstaben um. Zahlen und andere Zeichen werden nicht verändert.
  3. Teile den String in zwei 7-Byte-Hälften.
  4. Verwende jede der beiden Hälften als 56-Bit DES-Schlüssel und verschlüssele damit jeweils eine feste Konstante.
  5. Füge die beiden Ergebnisse zu einem 16-Byte-Wert zusammen.

Jörg Schwenk
Lehrstuhl für Netz- und Datensicherheit

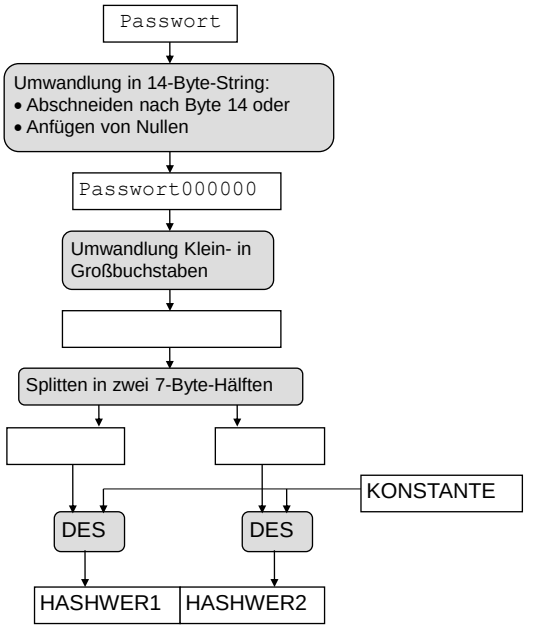
Kryptoanalyse (4)

MS-CHAP:
Berechnung des LMH



Kryptoanalyse (4)

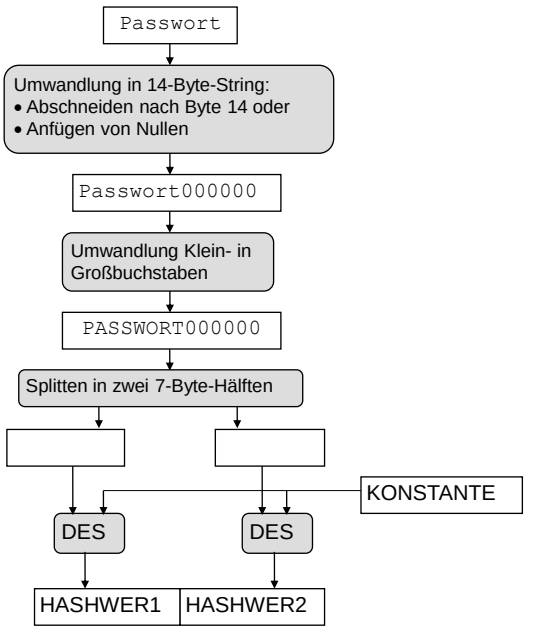
MS-CHAP:
Berechnung
des LMH



Lehrstuhl für

Kryptoanalyse (4)

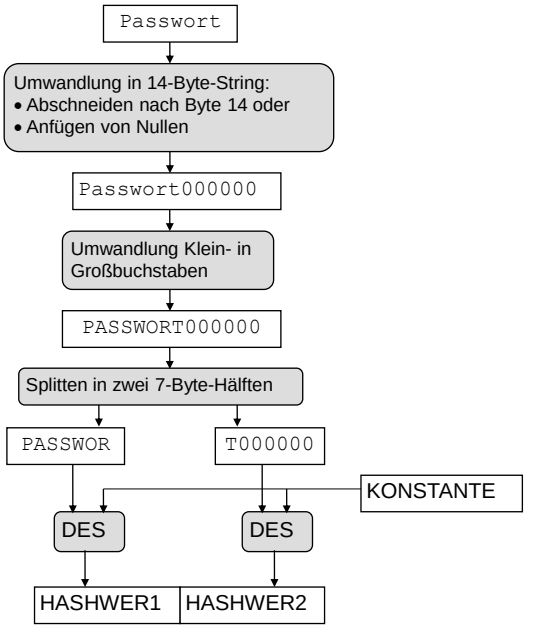
MS-CHAP:
Berechnung
des LMH



Lehrstuhl für

Kryptoanalyse (4)

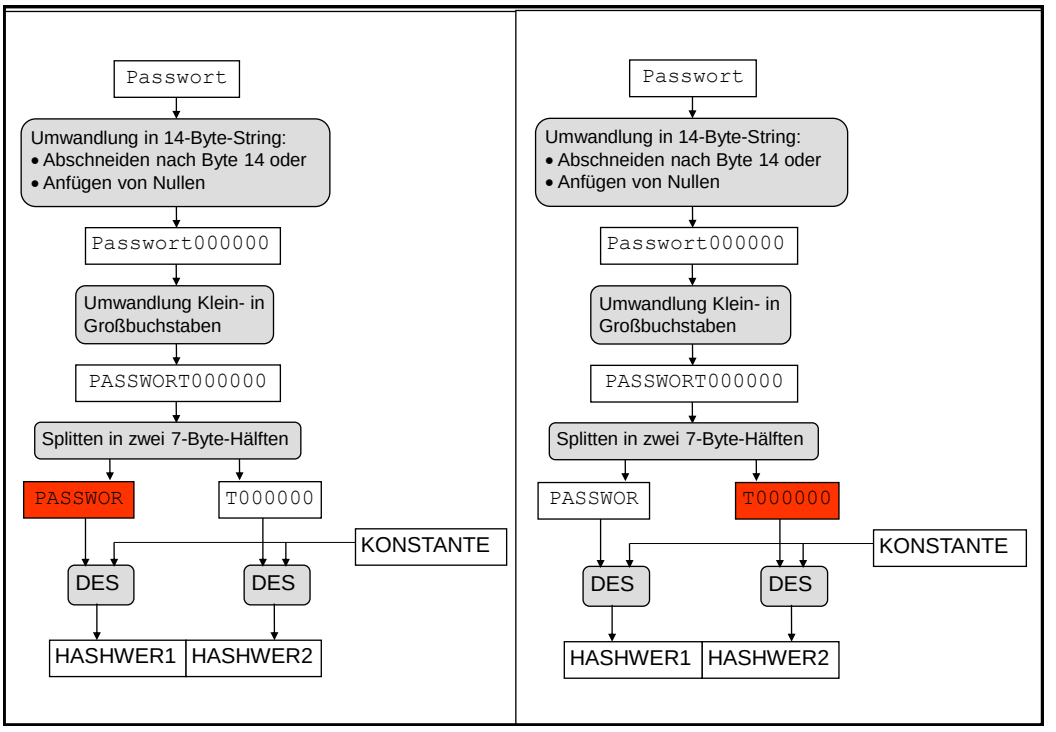
MS-CHAP:
Berechnung
des LMH



Kryptoanalyse von MS-PPTPv1(5)

Angriff auf Authentisierungs-Variante 2: Berechnung des Passworts aus den beiden Hashwerten.

- Windows NT Hash und LAN Manager Hash werden immer beide gesendet
- Greife zuerst den LAN Manager Hash an: Wörterbuch-Attacke gegen die beiden 8-Byte Hälften des Hashs.
  - Längere Passwörter sind nicht sicherer als 7-Byte Passwörter
  - Größe des benötigten Wörterbuchs wird durch die Umwandlung von Klein- in Grossbuchstaben weiter reduziert
  - Es gibt kein Salt, also kann das gleiche Wörterbuch für alle Benutzer verwendet werden
- Aus dem so gefundenen Passwort kann man das Originalpasswort durch Variation der Groß-Kleinschreibung und Anwendung des Windows NT Hash berechnen.



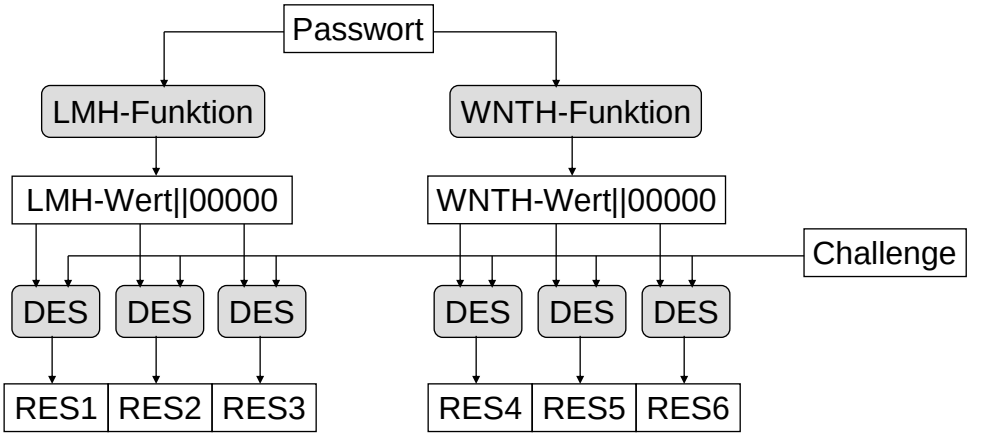
Kryptoanalyse von MS-PPTPv1(7)

Berechnung der Response in MS-CHAP:

- Server sendet 8 Byte (=64 Bit) Challenge
- Client verschlüsselt Challenge mit LAN Manager Hash:
  1. Füge 5 Null-Bytes an den LMH an, um 21 Bytes zu erhalten.
  2. Splitte die 21 Byte in drei DES-Schlüssel, und verschlüssele die Challenge mit jedem dieser Schlüssel separat unter DES.
  3. Sende die Ergebnisse als RES1, RES2, RES3 an den Server zurück.
- Client verfährt analog mit dem WNT-Hash; das Ergebnis sei RES4, RES5, RES6.

Kryptoanalyse von MS-PPTPv1(8)

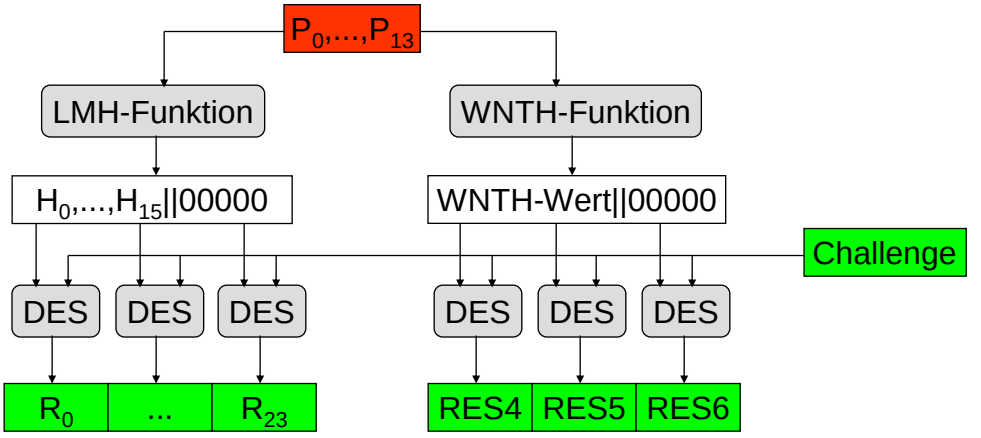
MS-CHAP: Berechnung der Response



Jörg Schwenk
Lehrstuhl für Netz- und Datensicherheit

Kryptoanalyse von MS-PPTPv1(9)

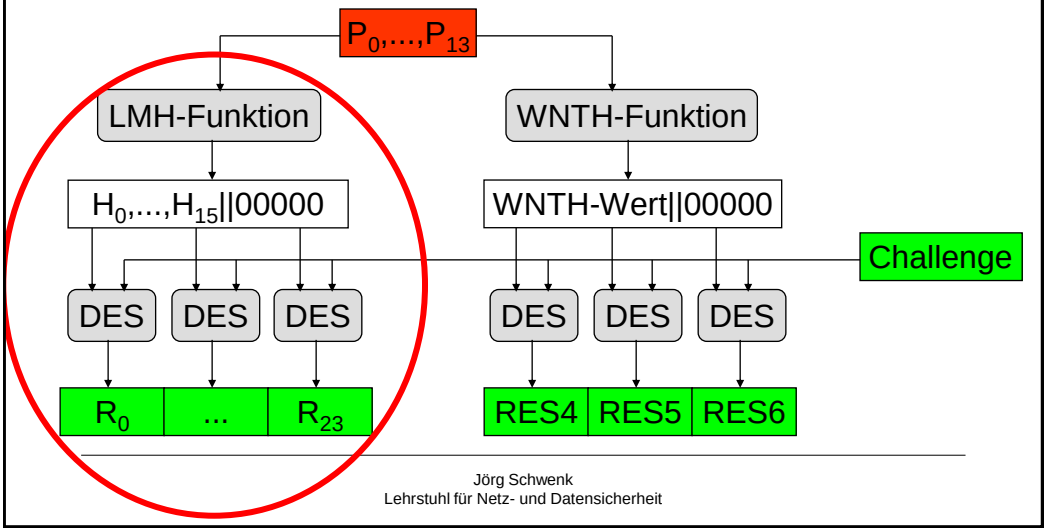
MS-CHAP: Berechnung des Passworts



Jörg Schwenk
Lehrstuhl für Netz- und Datensicherheit

Kryptoanalyse von MS-PPTPv1(9)

MS-CHAP: Berechnung des Passworts

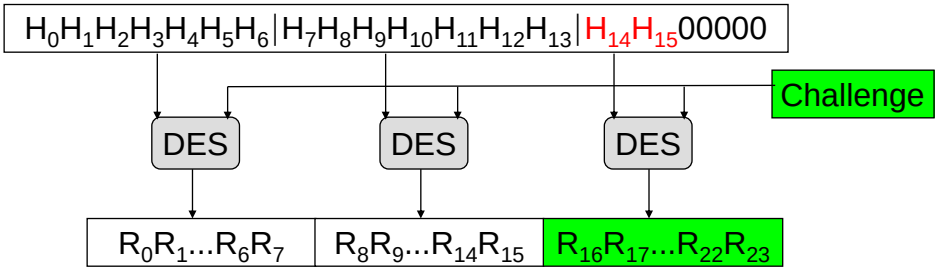


Jörg Schwenk
Lehrstuhl für Netz- und Datensicherheit

Kryptoanalyse von MS-PPTPv1(10)

MS-CHAP: Berechnung des Passworts

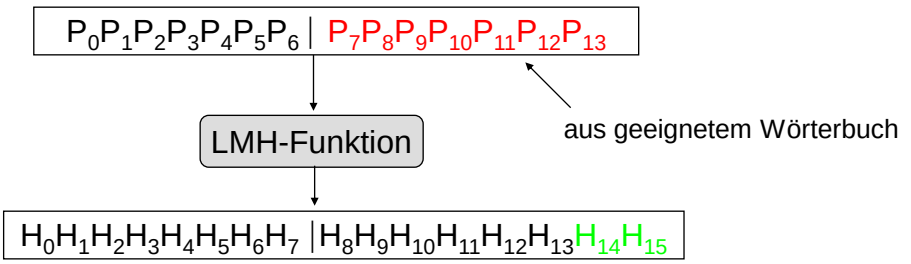
1. Teste alle möglichen Werte (2^{16}) für H_{14} und H_{15}. Die richtigen Werte sind gefunden, wenn die Verschlüsselung der Challenge mit DES und dem Schlüssel $H_{14}H_{15}00000$ den Wert $R_{16}...R_{23}$ ergibt.



Jörg Schwenk
Lehrstuhl für Netz- und Datensicherheit

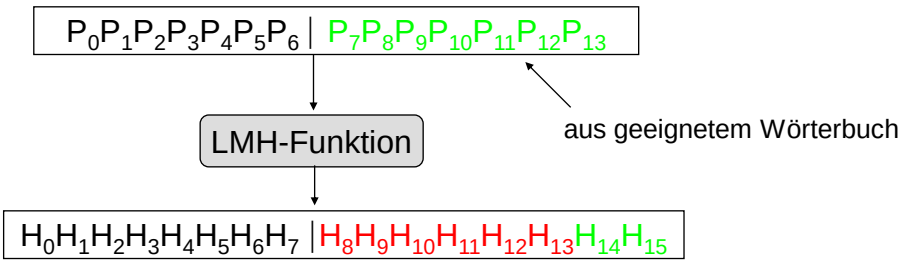
Kryptoanalyse von MS-PPTPv1(11)

2. Teste alle wahrscheinlichen Möglichkeiten (die 7 letzten Byte von möglichen Passwörtern, ggf. mit vielen Nullen) für P_7, …, P_{13}. Die meisten falschen Werte können aussortiert werden, indem man den LM-Hash von P_7, …, P_{13} bildet und überprüft, ob die letzten beiden Bytes gleich H_{14} und H_{15} sind.



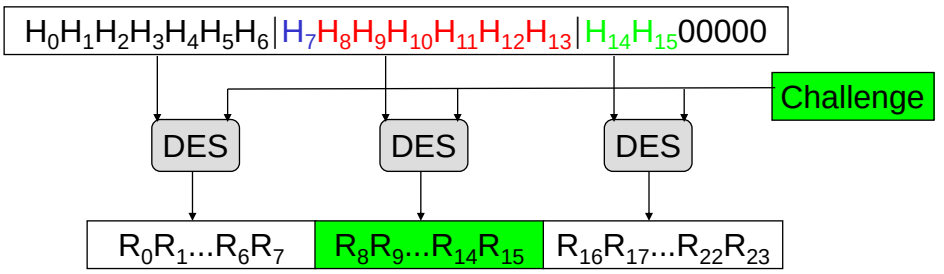
Kryptoanalyse von MS-PPTPv1(12)

3. Teste die Kandidaten P_7, …, P_{13} wie folgt
   - Berechne für die Kandidaten P_7, …, P_{13} die Werte H_8, …, H_{13}. (H_{14} und H_{15} sind bereits bekannt.)



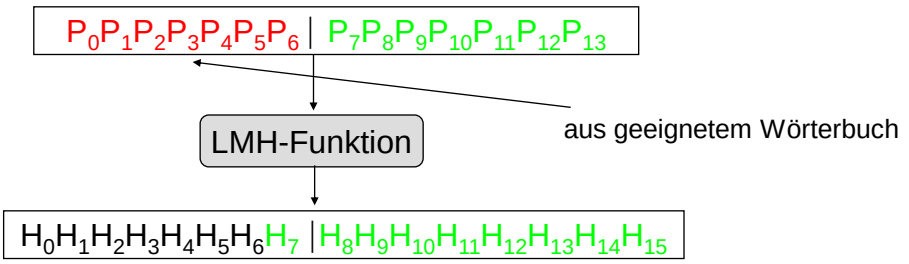
Kryptoanalyse von MS-PPTPv1(13)

- Für jeden der 28 möglichen Werte von H_7, verschlüssele die Challenge mit $H_7H_8…H_{13}$. Wenn das Ergebnis gleich $R_8…R_{15}$ ist, so sind H_7 und damit auch P_7, …, P_{13} mit an Sicherheit grenzender Wahrscheinlichkeit die korrekten Werte.
- Liefert kein möglicher Wert für H_7 das gewünschte Resultat, so war der Kandidat falsch.



Kryptoanalyse von MS-PPTPv1(14)

4. Wähle aus dem Wörterbuch für die linke Hälfte des Passworts die Kandidaten P_0 … P_6 aus, die den bekannten Wert H7 liefern.
5. Teste diese Kandidaten dahingehend, ob der Schlüssel $H_0H_1H_2H_3H_4H_5H_6$ die Challenge zu R_0 … R_7 verschlüsselt .



Kryptoanalyse von MS-PPTPv1(15)

Alternative zu 4. und 5.

- Wenn P7, …, P13 bekannt sind, so kann man P0, …, P6 durch eine Wörterbuchattacke ermitteln, indem man zu jedem möglichen Wert die LMH-Response berechnet und mit dem tatsächlichen Wert vergleicht. Da kein Salt verwendet wird, kann dieses Wörterbuch für alle PPTP-Clients verwendet werden.

Der beschriebene Angriff wurde im Tool L0phtcrack implementiert.