Downgrade Attacks

Compatibility breaks Security

Michael Rodler

2010-12-14

Vorstellung

Michael Rodler

- aka f0rk, f0rki...
- SIB09
- Security Monkey/„Researcher“

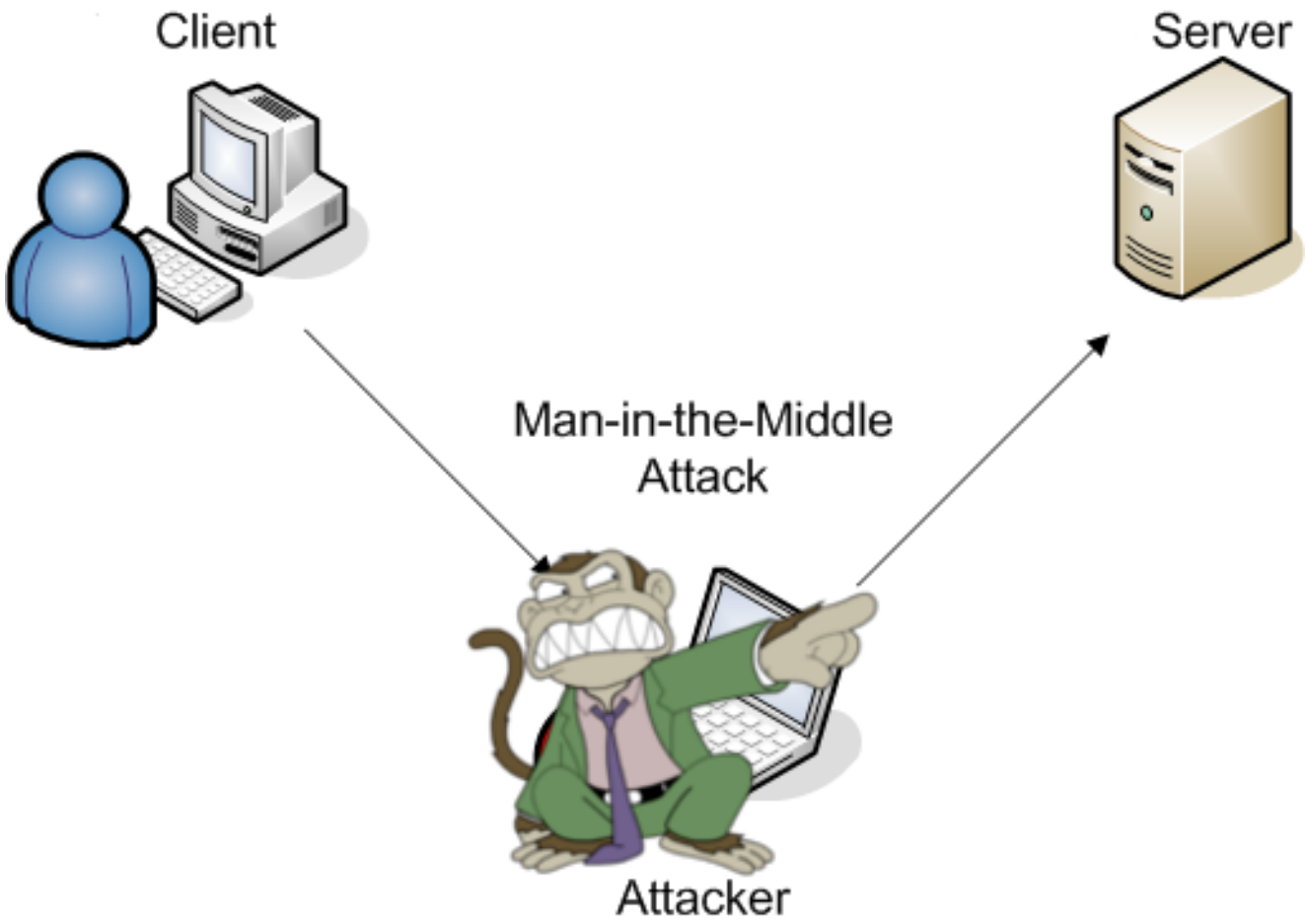
Was sind „Downgrade Attacks“?

- In (fast) jedem Netzwerkprotokoll gibt es einen Handshake
- Im Handshake wird ein *gemeinsamer Nenner* gesucht
  - Protokoll Features
  - Unterstützte Krypto-Algorithmen

Was sind „Downgrade Attacks“?

- In (fast) jedem Netzwerkprotokoll gibt es einen Handshake
- Im Handshake wird ein *gemeinsamer Nenner* gesucht
  - Protokoll Features
  - Unterstützte Krypto-Algorithmen

- *Monkey*-in-the-middle Szenario (z.B. mit arp spoofing, nd spoofing, fake ra, etc.)
- Angreifer ist in der Lage Netzwerk-Traffic zu verändern
- Downgrade Attack = Handshake abändern $\rightarrow$ Security Features deaktivieren oder abschwächen


Client
Server
Man-in-the-Middle
Attack
Attacker

Oracle

Einige Paper und Präsentationen vorhanden: László Tóth [1], Steve Ocepek und Wendel G. Henrique [2]

Oracle Protokolle

- Proprietäre Protokolle
  - Specs nur gegen $$$
  - $\rightarrow$ sehr mühsam zu analysieren
- Transparent Network Substrate (TNS)
  - primitiv und simpel
  - Wireshark decoder existiert
- Net8 bzw. SQL*Net
  - komplex und undurchsichtig
  - kein Wireshark decoder (bzw. nur kleine Teile implementiert)
- TNS transportiert Net8

Oracle Authentifizierung I

- Challenge-Response Verfahren
- Verwendete Algorithmen hängen von Version ab

Oracle 8i

- Server schickt Session Key
  Verschlüsselt mit DES, Schlüssel ist Oracle Hash des User Passwortes
- Client schickt Passwort
  Verschlüsselt mit DES, Schlüssel ist entschlüsselter Session Key

Oracle 9i

- Ähnlich zu 8i, aber 3DES wird verwendet

Oracle Authentifizierung II

Oracle 10g/11g

- Client/Server schicken beide Session Key
  $\rightarrow$ MD5(XOR(KeyServer, KeyClient))
- AES-128/192 kommen zum Einsatz

- Bruteforce Angriff ist bei 8i möglich
- Java Thin Client bis Version 10 kennt nur 8i Protokoll!

Downgrade Attacks

Einige Downgrade Angriffe in Publikationen beschrieben

- Gegen alte Versionen von Oracle 11 JDBC Treiber
- „Downgrade through Replay“
  - Login Pakete werden durch alte Versionen dieser ersetzt
  - Kombinationen verschiedener Versionen und Plattformen verhalten sich anders
    - Viele *WTF?!?* Momente...
- Angriff gegen Oracle 10g Windows Client und Server
  - Downgrade auf Oracle 8 level
  - von mir als Metasploit Modul implementiert
  - keine Demo heute :(

Attack!

No.	Source	Destination	Info
1	192.168.209.1	192.168.209.41	Request, Connect (1), Connect
2	192.168.209.41	192.168.209.1	Response, Resend (11)
3	192.168.209.1	192.168.209.41	Request, Connect (1), Connect
4	192.168.209.41	192.168.209.1	Response, Accept (2), Accept
5	192.168.209.1	192.168.209.41	Request, Data (6), SNS
6	192.168.209.41	192.168.209.1	Response, Data (6), SNS
7	192.168.209.1	192.168.209.41	Request, Data (6), Data
8	192.168.209.41	192.168.209.1	Response, Data (6), Data
9	192.168.209.1	192.168.209.41	Request, Data (6), Data
10	192.168.209.41	192.168.209.1	Response, Data (6), Data
11	192.168.209.1	192.168.209.41	Request, Data (6), Data
12	192.168.209.41	192.168.209.1	Response, Data (6), Data

```
0000  00 0c 29 7f 15 dc 00 0c  29 88 1b 7a 08 00 45 00   ..)..... )..z..E.
0010  00 4d b8 c6 40 00 80 06  1e 68 c0 a8 d1 01 c0 a8   .M..@... .h......
0020  d1 29 04 c3 05 f1 9d 09  c3 ce e4 ba ab 02 50 18   .)...... ......P.
0030  ff 58 2a 00 00 00 00 25  00 00 06 00 00 00 00 00   .X*....% ........
0040  01 05 05 04 03 02 01 00  49 42 4d 50 43 2f 57 49   ........ IBMPC/WI
0050  4e 5f 4e 54 2d 38 2e 31  2e 30 00                 N_NT-8.1 .0.
```

first value was changed from 0x06 to 0x05

Attack!

No.	Source	Destination	Info
3	192.168.209.1	192.168.209.41	Request, Connect (1), Connect
4	192.168.209.41	192.168.209.1	Response, Accept (2), Accept
5	192.168.209.1	192.168.209.41	Request, Data (6), SNS
6	192.168.209.41	192.168.209.1	Response, Data (6), SNS
7	192.168.209.1	192.168.209.41	Request, Data (6), Data
8	192.168.209.41	192.168.209.1	Response, Data (6), Data
9	192.168.209.1	192.168.209.41	Request, Data (6), Data
10	192.168.209.41	192.168.209.1	Response, Data (6), Data
11	192.168.209.1	192.168.209.41	Request, Data (6), Data
12	192.168.209.41	192.168.209.1	Response, Data (6), Data
13	192.168.209.1	192.168.209.41	Request, Data (6), Data

```
0000  00 50 56 c0 00 04 00 0c  29 88 1b 7a 08 00 45 00   .PV..... )..z..E.
0010  00 b3 1e 9e 40 00 80 06  b8 2a c0 a8 d1 29 c0 a8   ....@... .*...)..
0020  d1 01 05 f1 04 c3 e4 ba  ab 02 9d 09 c3 f3 50 18   ........ ......P.
0030  f9 48 39 50 00 00 00 8b  00 00 06 00 00 00 00 00   .H9P.... ........
0040  01 05 00 49 42 4d 50 43  2f 57 49 4e 5f 4e 54 2d   ...IBMPC /WIN_NT-
0050  38 2e 31 2e 30 00 b2 00  01 00 00 00 64 00 00 00   8.1.0... ....d...
0060  60 01 24 0f 05 0b 0c 03  0c 0c 05 04 05 0d 06 09   `.$..... ........
0070  07 08 05 05 05 05 05 0f  05 05 05 05 05 0a 05 05   ........ ........
0080  05 05 05 04 05 06 07 08  08 23 47 23 23 08 11 23   ........ .#G##..#
0090  08 11 41 b0 23 00 83 00  b2 07 d0 03 00 00 00 00   ..A.#... ........
00a0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00b0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00c0  00                                                 .
```

downgrade was accepted

Attack!

No.	Source	Destination	Info
2	192.168.209.41	192.168.209.1	Response, Resend (11)
3	192.168.209.1	192.168.209.41	Request, Connect (1), Connect
4	192.168.209.41	192.168.209.1	Response, Accept (2), Accept
5	192.168.209.1	192.168.209.41	Request, Data (6), SNS
6	192.168.209.41	192.168.209.1	Response, Data (6), SNS
7	192.168.209.1	192.168.209.41	Request, Data (6), Data
8	192.168.209.41	192.168.209.1	Response, Data (6), Data
9	192.168.209.1	192.168.209.41	Request, Data (6), Data
10	192.168.209.41	192.168.209.1	Response, Data (6), Data
11	192.168.209.1	192.168.209.41	Request, Data (6), Data
12	192.168.209.41	192.168.209.1	Response, Data (6), Data
13	192.168.209.1	192.168.209.41	Request, Data (6), Data

```
0040  03 73 03 90 80 a6 03 04  00 00 00 01 01 00 00 24   .s...... .......$
0050  ef 12 00 0c 00 00 00 cc  eb 12 00 b4 fb 12 00 04   ........ ........
0060  78 64 62 61 0d 00 00 00  0d 41 55 54 48 5f 50 41   xdba.... .AUTH_PA
0070  53 53 57 4f 52 44 11 00  00 00 11 32 37 31 37 31   SSWORD.. ...27171
0080  36 46 46 46 35 37 44 31  31 34 39 34 00 00 00 00   6FFF57D1 1494....
0090  08 00 00 00 08 41 55 54  48 5f 52 54 54 05 00 00   .....AUT H_RTT...
00a0  00 05 37 36 37 36 33 00  00 00 00 0d 00 00 00 0d   ..76763. ........
00b0  41 55 54 48 5f 43 4c 4e  54 5f 4d 45 4d 04 00 00   AUTH_CLN T_MEM...
00c0  00 04 34 30 39 36 00 00  00 00 0d 00 00 00 0d 41   ..4096.. .......A
00d0  55 54 48 5f 54 45 52 4d  49 4e 41 4c 08 00 00 00   UTH_TERM INAL....
00e0  08 4d 43 48 30 36 39 35  43 00 00 00 00 0f 00 00   .MCH0695 C.......
00f0  00 0f 41 55 54 48 5f 50  52 4f 47 52 41 4d 5f 4e   ..AUTH_P ROGRAM_N
0100  4d 0b 00 00 00 0b 73 71  6c 70 6c 75 73 2e 65 78   M.....sq lplus.ex
0110  65 00 00 00 00 0c 00 00  00 0c 41 55 54 48 5f 4d   e.......  ..AUTH_M
```

Mitigation

- Passwort Policy! (wir müssen immer noch cracken...)
- Neueste Versionen der Software benutzen
- Aktuelle JDBC Driver von Oracle 11 verwenden
- Minimal akzeptierte net8 Version am Server konfigurieren

  `SQLNET.ALLOWED_LOGON_VERSION`
- (Oracle Advanced Security kaufen)
- Über SSH oder SSL tunneln

Fragen?

Microsoft SQL Server

- Verwendet Tabular Data Stream Protokoll (TDS)
  - Offene Spezifikation
    $\rightarrow$ angenehmer als Oracle ;)
  - Wireshark Decoder existiert
- Zwei Arten der Authentifizierung
  - Native Authentication
  - Integrated/Windows Authentication

Native Authentication

- Authentifizierung mit „Login7“ Paket
- Kein kryptographisches Challenge-Response Verfahren
- Obfuscation des Passwortes
  - Methode ist bekannt und in der Spezifikation beschrieben

Native Authentication

- Authentifizierung mit „Login7“ Paket
- Kein kryptographisches Challenge-Response Verfahren
- Obfuscation des Passwortes
  - Methode ist bekannt und in der Spezifikation beschrieben

Aber...

Wireshark – Normaler Login Traffic

4	192.168.209.1	192.168.209.11	TDS7 pre-login message
5	192.168.209.11	192.168.209.1	Response
6	192.168.209.1	192.168.209.11	TDS7 pre-login message
7	192.168.209.11	192.168.209.1	TDS7 pre-login message
8	192.168.209.1	192.168.209.11	TDS7 pre-login message
9	192.168.209.11	192.168.209.1	TDS7 pre-login message
10	192.168.209.1	192.168.209.11	Unknown Packet Type: 23[Unreassembled Packet]
11	192.168.209.11	192.168.209.1	Response[Unreassembled Packet]
12	192.168.209.1	192.168.209.11	SQL batch
13	192.168.209.11	192.168.209.1	Response[Unreassembled Packet]

Wireshark – Decode as SSL

4	192.168.209.1	192.168.209.11	Ignored Unknown Record
5	192.168.209.11	192.168.209.1	Ignored Unknown Record
6	192.168.209.1	192.168.209.11	Ignored Unknown Record
7	192.168.209.11	192.168.209.1	Ignored Unknown Record
8	192.168.209.1	192.168.209.11	Ignored Unknown Record
9	192.168.209.11	192.168.209.1	Ignored Unknown Record
10	192.168.209.1	192.168.209.11	Application Data
11	192.168.209.11	192.168.209.1	Ignored Unknown Record
12	192.168.209.1	192.168.209.11	Ignored Unknown Record
13	192.168.209.11	192.168.209.1	Ignored Unknown Record

Native Authentication

- SSL Handshake innerhalb der TDS Pre-Login Pakete
  - Zertifikat wird nicht überprüft!

Native Authentication

- SSL Handshake innerhalb der TDS Pre-Login Pakete
  - Zertifikat wird nicht überprüft!
- Erstes Pre-Login Paket
  - Übermittelt Version, Protokoll Features, etc.
  - Ein Feld ist als „Encryption“ spezifiziert

Native Authentication

- SSL Handshake innerhalb der TDS Pre-Login Pakete
  - Zertifikat wird nicht überprüft!
- Erstes Pre-Login Paket
  - Übermittelt Version, Protokoll Features, etc.
  - Ein Feld ist als „Encryption“ spezifiziert

ENCRYPT_OFF	0x00	Encryption available but off.
ENCRYPT_ON	0x01	Encryption is available and on.
ENCRYPT_NOT_SUP	0x02	Encryption is not available.
ENCRYPT_REQ	0x03	Encryption is required.

Demo: Attack!!!

1. MITM Angriff
2. Transparenter „TDS-Proxy“ als Metasploit Modul
   - Setzt „Encryption“ Feld auf „ENCRYPT_NOT_SUP“
3. ???
4. PROFIT!!!

Demo!

Mitigation

- Windows Integrated Authentifizierung verwenden
  - Default beim Setup
  - „Force Encryption“ Option aktivieren

Responsible Disclosure $\rightarrow$ Antwort

> *„Please note that SQL Server does not offer an option to enforce encryption of only the login packet (a.k.a. username & password), and at this point we have no plans to introduce such option.“*
>
> *– Microsoft Incident Handler*

Fragen?

Literatur I

- Downgrading the Oracle native authentication, László Tóth, 2007-02-05, http://www.pwc.com/en_HU/hu/services/assets/oraauthdg-pub.pdf
- Oracle, Interrupted: Stealing Sessions and Credentials, Steve Ocepek and Wendel G. Henrique, 2010-04-20, https://www.trustwave.com/downloads/spiderlabs/Trustwave-SpiderLabs-Oracle-Interrupted-Henrique-and-Ocepek.pdf
- Hacktivity 2009: Oracle authentication, László Tóth, 2009, http://soonerorlater.hu/download/hacktivity_lt_2009_en.pdf
- Analysis of Oracle 9, 10 Authentication, László Tóth, http://www.soonerorlater.hu/index.khtml?article_id=511 (abgerufen am 2011-11-28)
- Analysis of Oracle 11 Authentication, László Tóth, http://www.soonerorlater.hu/index.khtml?article_id=512 (abgerufen am 2011-11-28)

Literatur II

 Microsoft TDS Spezifikation http://msdn.microsoft.com/en-us/library/dd304523%28v=PROT.13%29.aspx (V.10)