- create ceritifcates cert.sh
- install debian tools mitm-install.sh

Dell's documentation

- DellRemoteAccessController5Security.Pdf
- DellRemoteAccessController4Security.Pdf

t=0x8b7ebf8 [0,0]

Contents: [Dobrica PavlinuÅ¡iÄ 's random unstructured stuff]

I will try to collect useful protocol information about Dell's (actually ""<>) RAC protocol

My main goal is to use Dell RAC from Linux, without all troubles described in my blog post

Hardware

According to Exploring the DRAC5:

- AMD Alchemy Au1550 333 MHz processor
- Virtual media performance with up to 1.5 MB/sec transfer speeds
- Data storage through remote and local 16 MB USB keys
- Improved maximum supported screen resolution 1280*1024

Proprietary ports

t=0x8b85338

Port	Protocol	Type	Ver	Enc	Direction	Usage	Configurable
3668	Proprietary	TCP	1.0	None	In/Out	CD/diskette virtual media service	Yes

3669	Proprietary	TCP	1.0	128-bit SSL	In/Out	CD/diskette virtual media service	Yes
5900	Proprietary	TCP	1.0	128-bit SSL	In/Out	Video redirection	Yes
5901	Proprietary	TCP	1.0	128-bit SSL	In/Out	Keyboard/Mouse redirection	Yes

Supported SSL Cipher Suites

DRAC 5 supports SSL version 3 and TLS version 1.0. The following are ciphers supported on DRAC 5:

- SSL_RSA_WITH_RC4_128_MD5
- SSL_RSA_WITH_RC4_128_SHA
- SSL_RSA_WITH_3DES_EDE_CBC_SHA
- SSL_RSA_WITH_3DES_EDE_CBC_MD5
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA

IPMI RMCP+ Encryption

DRAC 5 IPMI over LAN and SOL use RMCP+ for Authentication and Key exchange. For details on the RMCP+ protocol, see the IPMI 2.0 specification.

DRAC 5 IPMI supports the following encryption algorithms:

- AES-CBC-128 (128-bit AES with CBC)
- RC4-128 (128-bit RC4)

Console Redirection Security

Authentication and Encryption

DRAC 5 can continuously redirect the managed system's video, keyboard and mouse (KVM) to the management station. It is a very powerful feature, is very easy to use, and does not require any software installation on the managed system. A user can access this feature to remotely manage the system as if they were sitting in front of the system. A security authentication and encryption protocol has been implemented in console redirection to prevent a hostile, rogue client from breaking into the console redirect path without authenticating though the web server. 128-bit SSL encryption secures the keyboard keystrokes during the remote console redirection and therefore does not allow unauthorized "snooping" of the network traffic. The following sequence of security protocol operations is performed during the establishment of a console redirection session:

1. A user logs into the main web GUI then clicks the "Open Consoles" tab.

1. The Web GUI sends a pre-authentication request to the DRAC 5 web server via the HTTPS channel (SSL encrypted).

1. The DRAC 5 web server returns a set of secret data (including an encryption key) via the SSL channel. The console redirection authentication key (32 bytes long) is dynamically generated to prevent replay attack.

1. The Console redirection client sends a login command with an authentication key to a console redirection server keyboard/mouse port for authentication via SSL channel.

1. If authentication is successful, a console redirection session and two console redirection pipes (one for keyboard/mouse and one for video) are established. The keyboard/mouse pipe is always SSL encrypted. The video pipe encryption is optional. (Users can choose to encrypt or not to encrypt the video pipe before they start their console redirection session).

Video redirection

```
root@klin:~# ssldump -r /tmp/rac_t1.pcap
New TCP connection #1: klin.local(52028) <-> 10.60.0.102(5900)
1 1  0.0148 (0.0148)  C>S  Handshake
      ClientHello
        Version 3.0
        cipher suites
        SSL_RSA_WITH_RC4_128_MD5
        SSL_RSA_WITH_3DES_EDE_CBC_SHA
        SSL_RSA_WITH_DES_CBC_SHA
        compression methods
                  NULL
1 2  0.0165 (0.0016)  S>C  Handshake
      ServerHello
        Version 3.0
        session_id[0]=

        cipherSuite         SSL_RSA_WITH_RC4_128_MD5
        compressionMethod                   NULL
```

SSL man in the middle

First, we need a really old distribution to support cipher suites. http://www.debian.org/distrib/archive

openssl versions:

- potato - 0.9.4-5 - includes just sslv2, so it's too old
- woody - 0.9.6c-2.woody.7

```
sudo debootstrap --arch i386 woody woody http://archive.debian.org/debian-archive/debian
sudo chroot woody
```

```
# /etc/apt/sources.list
deb http://archive.debian.org/debian-archive/debian potato main non-free contrib
deb http://archive.debian.org/debian-non-US/ potato/non-US main contrib non-free
```

```
apt-get install stunnel

openssl req -new -x509 -days 365 -nodes -out cert.pem -keyout cert.pem
```

```
# https mitm
stunnel -p cert.pem -d 443 -r 5443
stunnel -c -d 5443 -r 10.60.0.100:443

# 5900 mitm
stunnel -p cert.pem -d 5900 -r 5999
stunnel -c -d 5999 -r 10.60.0.100:5900
```

Check ssl connection

```
ssldump -i eth0 'port 5900' -A -N
```

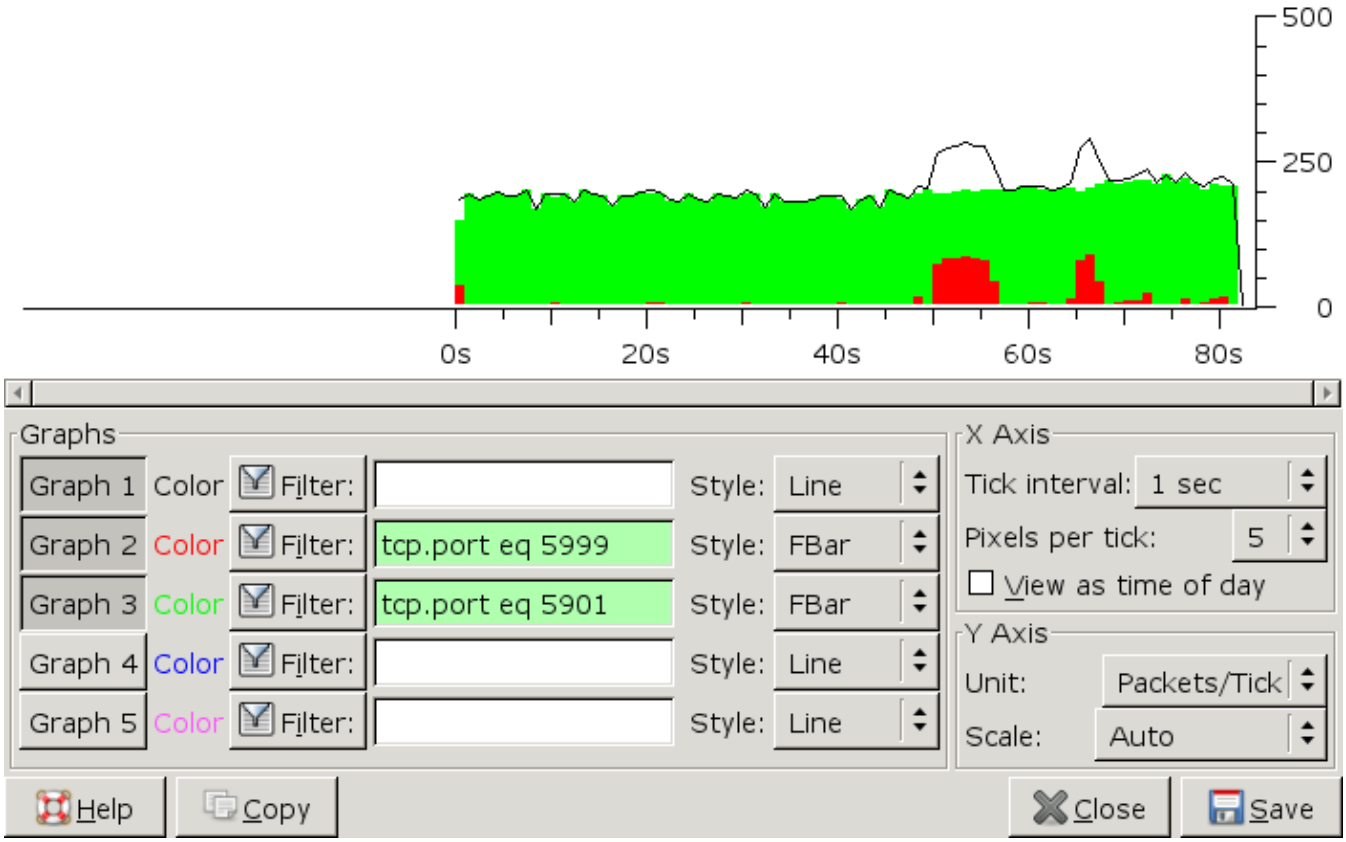
Following is **bad**

```
2 2  0.0489 (0.0000)  S>CV3.0(2)  Alert
    level           fatal
    value           handshake_failure
```

Dump unencrypted communication

```
sudo tshark -w /tmp/5900-plain.pcap 'port 5999'
```

5900 and 5901 traffic with two keystrokes:



- http://svn.rot13.org/index.cgi/scripts/view/trunk/mitm-ssl.pl

Dump all traffic:

- 5999 - unencrypted 5900
- 5443 - unencrypted 443 (https)
- 5901 - just port redir

```
sudo tshark -w /tmp/590x-3.pcap -i any 'port 5999 or port 5901 or port 5443'
```

```
# create client certificate
openssl req -new -x509 -days 365 -nodes -out ssl.cert -keyout ssl.key

root@opr:~/rac-ssl# ./mitm-ssl.pl --lport 5900 --laddr 10.60.0.91 --rport 5900 --raddr 10.60.0.10

root@opr:~/rac-ssl# ./mitm-ssl.pl --lport 443 --laddr 10.60.0.91 --rport 443 --raddr 10.60.0.100
```

Video adjust

- PS - Pixel sampling 00 - f0

```
# 0                                                PS
S>C 42454546 82020020 0080005a 0f42001b 04200000 03200258 00000002 00000000
C>S 42454546 03090010 00080000 00000000
```

```
C>S 42454546 03000010 00000000 00000000
# 10
S>C 42454546 82020020 0080005a 0f42001b 04200050 03200258 00000002 00000000
C>S 42454546 03090010 00500000 00000000
C>S 42454546 03000010 00000000 00000000
# 30
S>C 42454546 82020020 0080005a 0f42001b 042000f0 03200258 00000002 00000000
C>S 42454546 03090010 00f00000 00000000
```

- HORI - Horizontal position

```
# 0                             HORI
S>C 42454546 82020020 0080005a 0e74001b 042000f0 03200258 00000002 00000000
C>S 42454546 04000010 00000000 00000000
# ~100
S>C 42454546 82020020 0080005a 0eda001b 042000f0 03200258 00000002 00000000
C>S 42454546 04000010 00000000 00000000
# 100
S>C 42454546 82020020 0080005a 0ed8001b 042000f0 03200258 00000002 00000000
C>S 42454546 04000010 00000000 00000000
# 200
S>C 42454546 82020020 0080005a 0f3c001b 042000f0 03200258 00000002 00000000
# 400
S>C 42454546 82020020 0080005a 1004001b 042000f0 03200258 00000002 00000000
```

- VERT - Vertical position

```
# 0                             VERT
42454546 82020020 0080005a 1004000a 042000f0 03200258 00000002 00000000
# 10
42454546 82020020 0080005a 1004001e 042000f0 03200258 00000002 00000000
# 40
42454546 82020020 0080005a 10040032 042000f0 03200258 00000002 00000000
```

- CO - Contrast

```
# 0                     CO
42454546 82020020 00800000 10040032 042000f0 03200258 00000002 00000000
# 255
42454546 82020020 008000ff 10040032 042000f0 03200258 00000002 00000000
```

Keyboard redirection protocol 5900

mouse

```
# top-left               x    y
42454546 02010010 0000 000c 0008 0000
# bottom-right
42454546 02010010 0000 0282 0383 0000
# mouse click in the middle of screen
42454546 02010010 0001 018a 0147 0000
```

keyboard

```
# a b c d ...          down
C>S 42454546 02000010 00010004 00000000
C>S 42454546 02000010 00000005 00000000
C>S 42454546 02000010 00010005 00000000
C>S 42454546 02000010 00000006 00000000
C>S 42454546 02000010 00010006 00000000
C>S 42454546 02000010 00000007 00000000
C>S 42454546 02000010 00010007 00000000
```

Virtual media 3668

```
sudo tshark -w /tmp/drac-vmedia.pcap -i any 'port 5443 or port 3668'
```