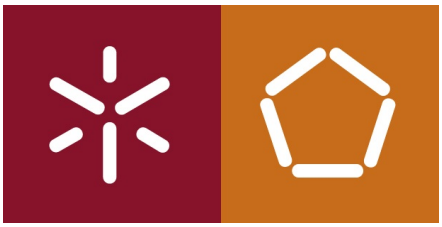

Engenharia de Segurança
Grupo 7
Aula 3

Bruno Machado - A74941
Diogo Gomes - A73825
Francisco Mendes - A75097

Fevereiro 2018

1 Assinaturas cegas (Blind signatures) baseadas no Elliptic Curve Discrete Logarithm Problem (ECDLP)

Os ficheiros encontram-se no repositório `git` do grupo numa diretoria cujo nome corresponde a esta alínea em questão.

2 Protocolo SSL/TLS

2.1

As Câmaras Municipais Portuguesas escolhidas foram: a câmara municipal de Águeda, de Albufeira, de Baião e de Braga, e os respetivos `SSL Server Test` encontram-se no repositório git do grupo numa diretoria cujo nome corresponde a esta alínea em questão.

2.2

Como é possível verificar, através de `SSL Server Test`, a maioria dos sites correspondentes às câmaras municipais selecionadas, encontram-se na zona de classificação **A**, contudo o site referente à câmara municipal de Braga apresenta a classificação **C** devido ao `POODLE attack`, sendo esta classificação a pior.

Esta classificação deve-se ao facto de o site ainda usar para as assinaturas o `SHA1`, que já foi quebrado. Também é usado o `RC4 no TLS`, que já é considerado inseguro e ainda não está implementado o `Forward secrecy`, que não permite, no caso de se descobrir a chave privada do servidor, decifrar as conversas que já aconteceram.

2.3

Como é possível observar no teste referente à câmara municipal de Braga, esta é vulnerável a `POODLE attack`.

O `POODLE attack` explora uma vulnerabilidade do `SSL 3.0`, que permite a um atacante da rede calcular o `plaintext` em conexões seguras. Esta vulnerabilidade pode ser mitigada como o uso de `TLS FALLBACK SCSV`, que impede o atacante de forçar um `downgrade` até o `SSL 3.0`, contudo o ataque ainda é possível caso o servidor e o cliente usem o `SSL 3.0`.

3 Protocolo SSH

3.1

As entidades comerciais em Madrid escolhidas foram a Telefonica de Espana e a Vodafone Spain. O resultado do `ssh-audit` de ambas são respetivamente as figuras 2 e 3 que se encontram nos apêndices, na secção Apêndices A no final do documento.

3.2

- **Telefonica de Espana:** `Dropbear SSH 0.46`
- **Vodafone Spain:** `OpenSSH 6.0p1`

3.3

Ambas as versões de *software* têm o mesmo número de vulnerabilidades. (Apêndices secção B)

3.4

É o `OpenSSH 6.0p1` que apresenta a vulnerabilidade mais grave, tendo um *score* de 7.8 contra os 7.5 da vulnerabilidade mais grave do `DropbearSSH 0.46` (Apêndices B - figura 5 e 4 respetivamente).

3.5

Esta vulnerabilidade permite que atacantes remotos executem ataques de negação de serviço (DoS) ao executar repetições de pedidos afim de saturar o sistema, impossibilitando o servidor de dar resposta a tantos pedidos. Segundo a nota no final da descrição, este tipo de ataques não compromete a segurança de um sistema, pois nenhum tipo de dados confidenciais são comprometidos.

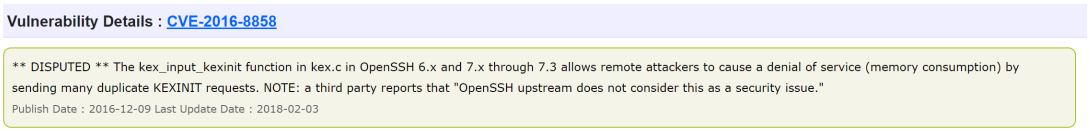

Figura 1: `CVE-2016-8858` - `OpenSSH 6.0p1` - Vodafone Spain

Apêndices

A Resultado do ssh-audit

```
user@CSI:~/Tools/ssh-audit$ python ssh-audit.py 83.52.62.219
# general
(gen) banner: SSH-2.0-dropbear_0.46
(gen) software: Dropbear SSH 0.46
(gen) compatibility: OpenSSH 2.5.0-6.6, Dropbear SSH 0.28+
(gen) compression: disabled

# security
(cve) CVE-2016-3116              -- (5.5) bypass command restrictions via xauth command injection
(cve) CVE-2013-4434              -- (5.0) discover valid usernames through different time delays
(cve) CVE-2013-4421              -- (5.0) cause DoS (memory consumption) via a compressed packet
(cve) CVE-2007-1099              -- (7.5) conduct a MitM attack (no warning for hostkey mismatch)
(cve) CVE-2006-1206              -- (7.5) cause DoS (slot exhaustion) via large number of connections
(cve) CVE-2006-0225              -- (4.6) execute arbitrary commands via scp with crafted filenames
(cve) CVE-2005-4178              -- (6.5) execute arbitrary code via buffer overflow vulnerability

# key exchange algorithms
(kex) diffie-hellman-group1-sha1 -- [fail] removed (in server) since OpenSSH 6.7, unsafe algorithm
                                 `- [fail] disabled (in client) since OpenSSH 7.0, logjam attack
                                 `- [warn] using small 1024-bit modulus
                                 `- [warn] using weak hashing algorithm
                                 `- [info] available since OpenSSH 2.3.0, Dropbear SSH 0.28

# host-key algorithms
(key) ssh-rsa                    -- [info] available since OpenSSH 2.5.0, Dropbear SSH 0.28

# encryption algorithms (ciphers)
(enc) 3des-cbc                   -- [fail] removed (in server) since OpenSSH 6.7, unsafe algorithm
                                 `- [warn] using weak cipher
                                 `- [warn] using weak cipher mode
                                 `- [warn] using small 64-bit block size
                                 `- [info] available since OpenSSH 1.2.2, Dropbear SSH 0.28

# message authentication code algorithms
(mac) hmac-sha1                  -- [warn] using encrypt-and-MAC mode
                                 `- [warn] using weak hashing algorithm
                                 `- [info] available since OpenSSH 2.1.0, Dropbear SSH 0.28
(mac) hmac-md5                   -- [fail] removed (in server) since OpenSSH 6.7, unsafe algorithm
                                 `- [warn] disabled (in client) since OpenSSH 7.2, legacy algorithm
                                 `- [warn] using encrypt-and-MAC mode
                                 `- [warn] using weak hashing algorithm
                                 `- [info] available since OpenSSH 2.1.0, Dropbear SSH 0.28

# algorithm recommendations (for Dropbear SSH 0.46)
(rec) -hmac-md5                  -- mac algorithm to remove
```

Figura 2: Telefonica de Espana

```
user@CSI:~/Tools/ssh-audit$ python ssh-audit.py 47.60.175.185
# general
(gen) banner: SSH-2.0-OpenSSH_6.0p1 Debian-4+deb7u4
(gen) software: OpenSSH 6.0p1
(gen) compatibility: OpenSSH 5.9-6.0, Dropbear SSH 2013.62+ (some functionality from 0.52)
(gen) compression: enabled (zlib@openssh.com)

# key exchange algorithms
(kex) ecdh-sha2-nistp256                    -- [fail] using weak elliptic curves
                                            `- [info] available since OpenSSH 5.7, Dropbear SSH 2013.62
(kex) ecdh-sha2-nistp384                    -- [fail] using weak elliptic curves
                                            `- [info] available since OpenSSH 5.7, Dropbear SSH 2013.62
(kex) ecdh-sha2-nistp521                    -- [fail] using weak elliptic curves
                                            `- [info] available since OpenSSH 5.7, Dropbear SSH 2013.62
(kex) diffie-hellman-group-exchange-sha256  -- [warn] using custom size modulus (possibly weak)
                                            `- [info] available since OpenSSH 4.4
(kex) diffie-hellman-group-exchange-sha1    -- [fail] removed (in server) since OpenSSH 6.7, unsafe algorithm
                                            |- [warn] using weak hashing algorithm
                                            `- [info] available since OpenSSH 2.3.0
(kex) diffie-hellman-group14-sha1           -- [warn] using weak hashing algorithm
                                            `- [info] available since OpenSSH 3.9, Dropbear SSH 0.53
(kex) diffie-hellman-group1-sha1            -- [fail] removed (in server) since OpenSSH 6.7, unsafe algorithm
                                            |- [fail] disabled (in client) since OpenSSH 7.0, logjam attack
                                            |- [warn] using small 1024-bit modulus
                                            |- [warn] using weak hashing algorithm
                                            `- [info] available since OpenSSH 2.3.0, Dropbear SSH 0.28

# host-key algorithms
(key) ssh-rsa                               -- [info] available since OpenSSH 2.5.0, Dropbear SSH 0.28
(key) ssh-dss                               -- [fail] removed (in server) and disabled (in client) since OpenSSH 7.0, weak algorithm
                                            |- [warn] using small 1024-bit modulus
                                            |- [warn] using weak random number generator could reveal the key
                                            `- [info] available since OpenSSH 2.1.0, Dropbear SSH 0.28
(key) ecdsa-sha2-nistp256                   -- [fail] using weak elliptic curves
                                            |- [warn] using weak random number generator could reveal the key
                                            `- [info] available since OpenSSH 5.7, Dropbear SSH 2013.62

# encryption algorithms (ciphers)
(enc) aes128-ctr                            -- [info] available since OpenSSH 3.7, Dropbear SSH 0.52
(enc) aes192-ctr                            -- [info] available since OpenSSH 3.7
(enc) aes256-ctr                            -- [info] available since OpenSSH 3.7, Dropbear SSH 0.52
(enc) arcfour256                            -- [fail] removed (in server) since OpenSSH 6.7, unsafe algorithm
                                            |- [warn] disabled (in client) since OpenSSH 7.2, legacy algorithm
                                            |- [warn] using weak cipher
                                            `- [info] available since OpenSSH 4.2
(enc) arcfour128                            -- [fail] removed (in server) since OpenSSH 6.7, unsafe algorithm
                                            |- [warn] disabled (in client) since OpenSSH 7.2, legacy algorithm
                                            |- [warn] using weak cipher
                                            `- [info] available since OpenSSH 4.2
(enc) aes128-cbc                            -- [fail] removed (in server) since OpenSSH 6.7, unsafe algorithm
                                            |- [warn] using weak cipher mode
                                            `- [info] available since OpenSSH 2.3.0, Dropbear SSH 0.28
(enc) 3des-cbc                              -- [fail] removed (in server) since OpenSSH 6.7, unsafe algorithm
                                            |- [warn] using weak cipher
                                            |- [warn] using weak cipher mode
                                            |- [warn] using small 64-bit block size
                                            `- [info] available since OpenSSH 1.2.2, Dropbear SSH 0.28
(enc) blowfish-cbc                          -- [fail] removed (in server) since OpenSSH 6.7, unsafe algorithm
                                            |- [fail] disabled since Dropbear SSH 0.53
                                            |- [warn] disabled (in client) since OpenSSH 7.2, legacy algorithm
                                            |- [warn] using weak cipher mode
                                            |- [warn] using small 64-bit block size
                                            `- [info] available since OpenSSH 1.2.2, Dropbear SSH 0.28
(enc) cast128-cbc                           -- [fail] removed (in server) since OpenSSH 6.7, unsafe algorithm
                                            |- [warn] disabled (in client) since OpenSSH 7.2, legacy algorithm
                                            |- [warn] using weak cipher mode
                                            |- [warn] using small 64-bit block size
                                            `- [info] available since OpenSSH 2.1.0
(enc) aes192-cbc                            -- [fail] removed (in server) since OpenSSH 6.7, unsafe algorithm
                                            |- [warn] using weak cipher mode
                                            `- [info] available since OpenSSH 2.3.0
(enc) aes256-cbc                            -- [fail] removed (in server) since OpenSSH 6.7, unsafe algorithm
                                            |- [warn] using weak cipher mode
                                            `- [info] available since OpenSSH 2.3.0, Dropbear SSH 0.47
(enc) arcfour                               -- [fail] removed (in server) since OpenSSH 6.7, unsafe algorithm
                                            |- [warn] disabled (in client) since OpenSSH 7.2, legacy algorithm
                                            |- [warn] using weak cipher
                                            `- [info] available since OpenSSH 2.1.0
(enc) rijndael-cbc@lysator.liu.se           -- [fail] removed (in server) since OpenSSH 6.7, unsafe algorithm
                                            |- [warn] disabled (in client) since OpenSSH 7.2, legacy algorithm
                                            |- [warn] using weak cipher mode
                                            `- [info] available since OpenSSH 2.3.0

# message authentication code algorithms
(mac) hmac-md5                              -- [fail] removed (in server) since OpenSSH 6.7, unsafe algorithm
                                            |- [warn] disabled (in client) since OpenSSH 7.2, legacy algorithm
                                            |- [warn] using encrypt-and-MAC mode
                                            |- [warn] using weak hashing algorithm
                                            `- [info] available since OpenSSH 2.1.0, Dropbear SSH 0.28
(mac) hmac-sha1                             -- [warn] using encrypt-and-MAC mode
                                            |- [warn] using weak hashing algorithm
                                            `- [info] available since OpenSSH 2.1.0, Dropbear SSH 0.28
(mac) umac-64@openssh.com                   -- [warn] using encrypt-and-MAC mode
                                            |- [warn] using small 64-bit tag size
                                            `- [info] available since OpenSSH 4.7
(mac) hmac-sha2-256                         -- [warn] using encrypt-and-MAC mode
                                            `- [info] available since OpenSSH 5.9, Dropbear SSH 2013.56
(mac) hmac-sha2-256-96                      -- [fail] removed since OpenSSH 6.1, removed from specification
                                            |- [warn] using encrypt-and-MAC mode
                                            `- [info] available since OpenSSH 5.9
(mac) hmac-sha2-512                         -- [warn] using encrypt-and-MAC mode
                                            `- [info] available since OpenSSH 5.9, Dropbear SSH 2013.56
(mac) hmac-sha2-512-96                      -- [fail] removed since OpenSSH 6.1, removed from specification
                                            |- [warn] using encrypt-and-MAC mode
                                            `- [info] available since OpenSSH 5.9
(mac) hmac-ripemd160                        -- [fail] removed (in server) since OpenSSH 6.7, unsafe algorithm
                                            |- [warn] disabled (in client) since OpenSSH 7.2, legacy algorithm
                                            |- [warn] using encrypt-and-MAC mode
                                            `- [info] available since OpenSSH 2.5.0
(mac) hmac-ripemd160@openssh.com            -- [fail] removed (in server) since OpenSSH 6.7, unsafe algorithm
                                            |- [warn] disabled (in client) since OpenSSH 7.2, legacy algorithm
                                            |- [warn] using encrypt-and-MAC mode
                                            `- [info] available since OpenSSH 2.1.0
(mac) hmac-sha1-96                          -- [fail] removed (in server) since OpenSSH 6.7, unsafe algorithm
                                            |- [warn] disabled (in client) since OpenSSH 7.2, legacy algorithm
                                            |- [warn] using encrypt-and-MAC mode
                                            |- [warn] using weak hashing algorithm
                                            `- [info] available since OpenSSH 2.5.0, Dropbear SSH 0.47
(mac) hmac-md5-96                           -- [fail] removed (in server) since OpenSSH 6.7, unsafe algorithm
                                            |- [warn] disabled (in client) since OpenSSH 7.2, legacy algorithm
                                            |- [warn] using encrypt-and-MAC mode
                                            |- [warn] using weak hashing algorithm
                                            `- [info] available since OpenSSH 2.5.0

# algorithm recommendations (for OpenSSH 6.0)
(rec) -diffie-hellman-group14-sha1          -- kex algorithm to remove
(rec) -diffie-hellman-group-exchange-sha1   -- kex algorithm to remove
(rec) -diffie-hellman-group1-sha1           -- kex algorithm to remove
(rec) -ecdh-sha2-nistp256                   -- kex algorithm to remove
(rec) -ecdh-sha2-nistp521                   -- kex algorithm to remove
(rec) -ecdh-sha2-nistp384                   -- kex algorithm to remove
(rec) -ecdsa-sha2-nistp256                  -- key algorithm to remove
(rec) -ssh-dss                              -- key algorithm to remove
(rec) -arcfour                              -- enc algorithm to remove
(rec) -rijndael-cbc@lysator.liu.se          -- enc algorithm to remove
(rec) -blowfish-cbc                         -- enc algorithm to remove
(rec) -3des-cbc                             -- enc algorithm to remove
(rec) -aes256-cbc                           -- enc algorithm to remove
(rec) -arcfour256                           -- enc algorithm to remove
(rec) -cast128-cbc                          -- enc algorithm to remove
(rec) -aes192-cbc                           -- enc algorithm to remove
(rec) -arcfour128                           -- enc algorithm to remove
(rec) -aes128-cbc                           -- enc algorithm to remove
(rec) -hmac-md5-96                          -- mac algorithm to remove
(rec) -hmac-sha2-256-96                     -- mac algorithm to remove
(rec) -hmac-ripemd160                       -- mac algorithm to remove
(rec) -hmac-sha1-96                         -- mac algorithm to remove
(rec) -umac-64@openssh.com                  -- mac algorithm to remove
(rec) -hmac-md5                             -- mac algorithm to remove
(rec) -hmac-ripemd160@openssh.com           -- mac algorithm to remove
(rec) -hmac-sha1                            -- mac algorithm to remove
(rec) -hmac-sha2-512-96                     -- mac algorithm to remove
```

Figura 3: Vodafone Spain

B Vulnerabilidades dos softwares SSH

Cpe Name:*cpe:/a:matt_johnston:dropbear_ssh_server:0.46*
CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9
Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending
Copy Results Download Results

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2013-4434	189			2013-10-25	2017-11-14	5.0	None	Remote	Low	Not required	Partial	None	None
Dropbear SSH Server before 2013.59 generates error messages for a failed logon attempt with different time delays depending on whether the user account exists, which allows remote attackers to discover valid usernames.														
2	CVE-2013-4421	189		DoS	2013-10-25	2017-11-14	5.0	None	Remote	Low	Not required	None	None	Partial
The buf_decompress function in packet.c in Dropbear SSH Server before 2013.59 allows remote attackers to cause a denial of service (memory consumption) via a compressed packet that has a large size when it is decompressed.														
3	CVE-2007-1099				2007-02-26	2017-07-28	7.5	None	Remote	Low	Not required	Partial	Partial	Partial
dbclient in Dropbear SSH client before 0.49 does not sufficiently warn the user when it detects a hostkey mismatch, which might allow remote attackers to conduct man-in-the-middle attacks.														
4	CVE-2006-1206			DoS	2006-03-13	2017-07-19	5.0	None	Remote	Low	Not required	None	None	Partial
Matt Johnston Dropbear SSH server 0.47 and earlier, as used in embedded Linux devices and on general-purpose operating systems, allows remote attackers to cause a denial of service (connection slot exhaustion) via a large number of connection attempts that exceeds the MAX_UNAUTH_CLIENTS defined value of 30.														
5	CVE-2005-4178			Exec Code Overflow	2005-12-12	2008-09-05	6.5	User	Remote	Low	Single system	Partial	Partial	Partial
Buffer overflow in Dropbear server before 0.47 allows authenticated users to execute arbitrary code via unspecified inputs that cause insufficient memory to be allocated due to an incorrect expression that does not enforce the proper order of operations.														

Total number of vulnerabilities : **5** Page : 1 (This Page)

Figura 4: `DropbearSSH 0.46` - Telefonica de Espana

Cpe Name:*cpe:/a:openbsd:openssh:6.0:p1*
CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9
Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending
Copy Results Download Results

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2017-15906	275			2017-10-25	2018-01-31	5.0	None	Remote	Low	Not required	None	Partial	None
The process_open function in sftp-server.c in OpenSSH before 7.6 does not properly prevent write operations in readonly mode, which allows attackers to create zero-length files.														
2	CVE-2016-10708	476		DoS	2018-01-21	2018-02-08	5.0	None	Remote	Low	Not required	None	None	Partial
sshd in OpenSSH before 7.4 allows remote attackers to cause a denial of service (NULL pointer dereference and daemon crash) via an out-of-sequence NEWKEYS message, as demonstrated by Honggfuzz, related to kex.c and packet.c.														
3	CVE-2016-8858	399		DoS	2016-12-09	2018-02-03	7.8	None	Remote	Low	Not required	None	None	Complete
** DISPUTED ** The kex_input_kexinit function in kex.c in OpenSSH 6.x and 7.x through 7.3 allows remote attackers to cause a denial of service (memory consumption) by sending many duplicate KEXINIT requests. NOTE: a third party reports that "OpenSSH upstream does not consider this as a security issue."														
4	CVE-2016-0778	119		DoS Overflow	2016-01-14	2017-02-16	4.6	None	Remote	High	Single system	Partial	Partial	Partial
The (1) roaming_read and (2) roaming_write functions in roaming_common.c in the client in OpenSSH 5.x, 6.x, and 7.x before 7.1p2, when certain proxy and forward options are enabled, do not properly maintain connection file descriptors, which allows remote servers to cause a denial of service (heap-based buffer overflow) or possibly have unspecified other impact by requesting many forwardings.														
5	CVE-2016-0777	200		+Info	2016-01-14	2017-11-20	4.0	None	Remote	Low	Single system	Partial	None	None
The resend_bytes function in roaming_common.c in the client in OpenSSH 5.x, 6.x, and 7.x before 7.1p2 allows remote servers to obtain sensitive information from process memory by requesting transmission of an entire buffer, as demonstrated by reading a private key.														

Total number of vulnerabilities : **5** Page : 1 (This Page)

Figura 5: `OpenSSH 6.0p1` - Vodafone Spain