

Universidade do Minho

Lic. em Matemática e Ciências de Computação
Criptografia Aplicada
2007/2008

Site para uma intranet com autenticação baseada em
certificados X509

Rui Carlos A. Gonçalves (41031)

8 de Janeiro de 2008

Resumo

Neste relatório descreve-se de forma sucinta o trabalho realizado no âmbito da disciplina de Criptografia Aplicada, onde se pretendia desenvolver um *site* para uma *intranet*, com zonas de acesso público e zonas de acesso restrito, onde a autenticação seria realizada através de certificados.

Conteúdo

1	Introdução	1
2	Cenário Desenvolvido	1
3	Configuração do Servidor	1
4	Conclusão	3

1 Introdução

Nos dias de hoje, as redes informáticas fornecem um meio de comunicação muito usado. Através deste, é fácil disponibilizar aos outros informações e serviços. No entanto, frequentemente, não se pretende permitir o acesso a estas informações/serviços a qualquer pessoa. É assim necessário possuir meios que permitam definir quem o pode fazer e quem não pode.

Este trabalho aborda precisamente esta questão. Assim, pretende-se desenvolver um *site* onde, para além de zonas acessíveis a todos, existem também outras áreas às quais só podem aceder pessoas devidamente autorizadas.

Existem várias formas de implementar mecanismos de controlo de acesso. Uma delas é a utilização de certificados. Esta é particularmente adequada a *sites* onde todos os *clientes* que podem aceder aos locais de acesso restrito são conhecidos. Será este o método usado para o trabalho proposto.

Para implementar o trabalho, será usado um servidor com o sistema operativo *Mac OS X 10.4.11* e o *software Apache 1.3.33*.

2 Cenário Desenvolvido

No cenário desenvolvido, o *site* terá a seguinte estrutura de directórios:

- dep1 - zona ao departamento 1
 - priv - zona privada do departamento 1
 - * admin - zona de administração do departamento 1
 - * staff - zona do *staff* do departamento 1
- dep2 - zona do departamento 2
 - priv - zona privada do departamento 2

Os directórios *dep1* e *dep2* estão acessíveis a qualquer pessoa. Já os directórios *priv* só estão acessíveis a quem possuir certificados emitidos pela autoridade de certificação do respectivo departamento¹. Não existe, no entanto, mais nenhuma restrição nos certificados para aceder a estes directórios. No caso dos directórios *admin* e *staff*, para além de terem que possuir certificados emitidos pelo departamento 1, estes terão mais algumas restrições. No caso do directório *staff*, a *Organization Unit* terá que ser igual a “staff” ou “admin”, e para aceder ao directório *admin*, o seu valor só poderá ser “admin”.

3 Configuração do Servidor

O primeiro passo foi criar a estrutura de directório descrita na secção anterior.

Agora é necessário configurar o *Apache*. Tal será feita adicionando algumas instruções no seu ficheiro de configuração (no caso */etc/httpd/httpd.conf*). Activou-se então o *SSL*. Para tal foi usado o seguinte código:

```
1 Listen 443
2
3 NameVirtualHost *:443
```

¹Serão criadas duas autoridades de certificação, *ca01* para o departamento 1, e *ca02* para o departamento 2

```

4
5 <VirtualHost *:443>
6     SSLEngine on
7     SSLCertificateFile /etc/httpd/ssl/server.crt
8     SSLCertificateKeyFile /etc/httpd/ssl/server.key
9
10     DocumentRoot /Library/WebServer/Documents
11 </VirtualHost>

```

Desta forma, o *Apache* activará o *SSL* para todas a conexões realizadas através da porta 443. É ainda indicada a localização dos ficheiros contendo a chave e respectivo certificado do servidor (linhas 7 e 8).

De seguida, são indicadas as restrições relativas aos vários directórios. O seguinte excerto de código, é responsável por essa parte:

```

1 SSLCertificateFile /etc/httpd/ssl/cacert.pem
2 SSLVerifyClient none
3 SSLVerifyDepth 1
4
5 <Location /cripto/dep1/priv>
6     SSLVerifyClient require
7     SSLRequireSSL
8     SSLRequire %{SSL_CLIENT_I_DN_CN} eq "ca01"
9 </Location>
10
11 <Location /cripto/dep2/priv>
12     SSLVerifyClient require
13     SSLRequireSSL
14     SSLRequire %{SSL_CLIENT_I_DN_CN} eq "ca02"
15 </Location>
16
17 <Location /cripto/dep1/priv/staff>
18     SSLVerifyClient require
19     SSLRequireSSL
20     SSLRequire %{SSL_CLIENT_I_DN_CN} eq "ca01"\
21         and %{SSL_CLIENT_S_DN_OU} in {"admin","staff"}
22 </Location>
23
24 <Location /cripto/dep1/priv/admin>
25     SSLVerifyClient require
26     SSLRequireSSL
27     SSLRequire %{SSL_CLIENT_I_DN_CN} eq "ca01"\
28         and %{SSL_CLIENT_S_DN_OU} eq "admin"
29 </Location>

```

Nesta fase, é indicada a localização de um ficheiro contendo os certificados das várias autoridades de certificação (linha 1), é indicado que por omissão não é necessário certificados (linha 2), é indicado que o tamanho máximo da cadeia de certificação, que neste caso será 1 (linha 3), e as restrições de acesso para cada uma da localizações não públicas. Para estas, será exigido certificado (linhas 6, 12, 18 e 25), só poderão ser feitas conexões a esses directórios se o *SSL* estiver activo (linhas 7, 13, 19 e 26), e, no caso dos directórios *dep1/priv* e *dep2/priv*, os certificados

terão que ser emitidos pela autoridade de certificação cujo *Common Name* é “ca01” e “ca02”, respectivamente (linhas 8 e 14). Adicionalmente, para directório `dep1/priv/staff`, a *Organization Unit* terá ainda de ter o valor “admin” ou “staff” (linha 21), e no caso de `dep1/priv/admin` este campo do certificado deverá ter o valor “admin” (linha 28).

Por fim, apenas falta criar as autoridades de certificação e colocar os seus certificados no ficheiro já referido (e, obviamente, gerar os certificados para os clientes). Tal foi feito recorrendo ao *OpenSSL*.

4 Conclusão

No final deste trabalho, sublinha-se que os objectivos propostos foram alcançados, tendo-se obtido um *site* onde o acesso a determinadas zonas é controlado através de certificados.

Este trabalho permitiu também ganhar uma maior familiaridade com a *software OpenSSL* para criação de autoridades de certificação, geração de chaves e emissão de certificados, assim como conhecer as funcionalidades ao nível do protocolo *SSL* do *Apache*.

Referências

- [1] <http://httpd.apache.org>
- [2] <http://www.debian-administration.org/>
- [3] <http://linuxfreechoice.blogspot.com/>
- [4] <http://www.openssl.org>