UNIVERSIDADE LUSÓFONA
de Humanidades e Tecnologias
Humani nihil alienum

Engenharia Informática

Infra-estrutura VoIP com Segurança

RELATÓRIO

Trabalho Final de Curso:	**Infra-estrutura VoIP com Segurança**
Aluno:	**Paulo Alexandre Fialho Jerónimo**
Número:	**A20062937**
Turma:	**3N1**
Curso:	**Engenharia Informática**

Paulo Jeronimo

ÍNDICE

Abstracto

O VoIP está actualmente no topo da lista de investimentos em tecnologia e constitui para muitos gestores empresariais uma fonte inequívoca de vantagens. Para muitas organizações, a sua principal vantagem consiste na utilização a custo reduzido de tecnologias apenas disponíveis em centrais e Call Centers dispendiosos. Outros reconhecerão a plenitude das vantagens da tecnologia, o que faz com que a transição para o VoIP esteja a ocorrer rapidamente à escala global.

As vantagens da convergência da voz para a mesma infra-estrutura física de dados, ou por outras palavras, as vantagens da transmissão da voz em tempo real num ambiente de comutação de pacotes, diferente, e estruturalmente adverso ao ambiente tradicional da voz, baseado em redes de comutação de circuitos, são no entanto acompanhadas de riscos e novos desafios no domínio da engenharia de redes. O equilíbrio entre a segurança nos diferentes níveis do processo de transmissão da voz sobre IP, e o nível da experiência de utilização e da qualidade fundamental do serviço, constitui o mais importante dos desafios. Este documento descreve passo-a-passo a constituição de uma infra-estrutura VoIP que implementa fortes mecanismos de segurança e fornece uma qualidade de experiência superior para o utilizador.

O confronto com a existência de um leque grande de oferta de soluções VoIP é normalmente o primeiro desafio para o projecto. Existem muitas soluções de fabricantes com grande implantação no mercado tecnológico. Soluções em appliances de hardware como a Unified Communications da CISCO, o Business Communications Manager da NORTEL, ou o Unified Access da AVAYA competem directamente com soluções de software como a Unified Communications da Microsoft ou o Asterisk (General Public Licence). Independentemente do tipo de solução, todas partilham uma infra-estrutura comum de protocolos e a todas se colocam os mesmos desafios.

Este documento baseia-se na configuração da segurança da infra-estrutura em torno do Unified Communications OCS2007 da Microsoft. Para a escolha desta infra-estrutura contribuiu o facto do sistema operativo Windows ser actualmente um standard nas redes empresariais. Por outro lado, talvez motivado pelo facto do VoIP ser uma oferta recente para este fabricante, com o IP-PBX baseado em OCS2007, a Microsoft revela ter usado o tempo com inteligência, e apresenta uma solução VoIP baseada nos mesmos standards, mas diferenciada no que respeita a características inovadoras, sendo já referida como a que melhor equilibra a segurança, a performance, e a qualidade da experiência para o utilizador. Deste estudo e do trabalho de investigação nele contido, deverá assim resultar uma infra-estrutura VoIP segura, possível de replicar e implementar num contexto empresarial.

Abstract

VoIP is actually on the top of the technology investments board for many business managers and for many of them it's a strong source of advantages. For many of those organizations its main advantage is the use of technologies only available in expansive Call Centers at reduced costs. Many others are aware of the complete advantages of the technology, and this is causing a worldwide fast transition to VoIP.

The advantages of converging voice and data on the same physical infrastructure, or, using other words, the advantages of real time voice transmission in a packet-switched environment, different and adverse regarding the traditional circuit-switched voice environment, is accomplished with risks and new challenges to the network engineers. The balance between security at different levels in the process of voice transmission over the IP protocol, and the level of the experience of use and the basic quality of service, appoints the most important of the challenges. This document describes step by step the constitution of a VoIP infrastructure that implements strong security mechanisms and supplies a superior quality of experience for the user.

The confrontation with the existence of a big panel of offers regarding VoIP solutions is normally the first challenge of the project. There are many VoIP solutions available from recognized manufacturers with great introduction in the technological market. Hardware appliance solutions such as the CISCO Unified Communications, the NORTEL Business Communications Manager, or the AVAYA Unified Access compete directly with software solutions like Microsoft's Unified Communications or the Asterisk (General Public Licence). Despite the VoIP solution, they all share a common protocol infrastructure and share the same challenges.

This document focuses on the configuration of the security of the infrastructure around the Microsoft Unified Communications OCS2007. This infrastructure was chosen because of the fact that the underlying Windows operating system is actually the standard in the enterprise corporate networks. On the other end, and probably caused by the fact that VoIP is a recent offer from this manufacturer, with the IP-PBX based on OCS2007, Microsoft showed to have used the time with intelligence, presenting a VoIP solution based on the same standards, truly differentiated in what it respects to innovatory characteristics, being already mentioned as the solution that bests balances security, performance, and the quality of the experience to the user. This achievement will result in a secure VoIP infrastructure, capable of replying and implementing in a business context.

Objectivo

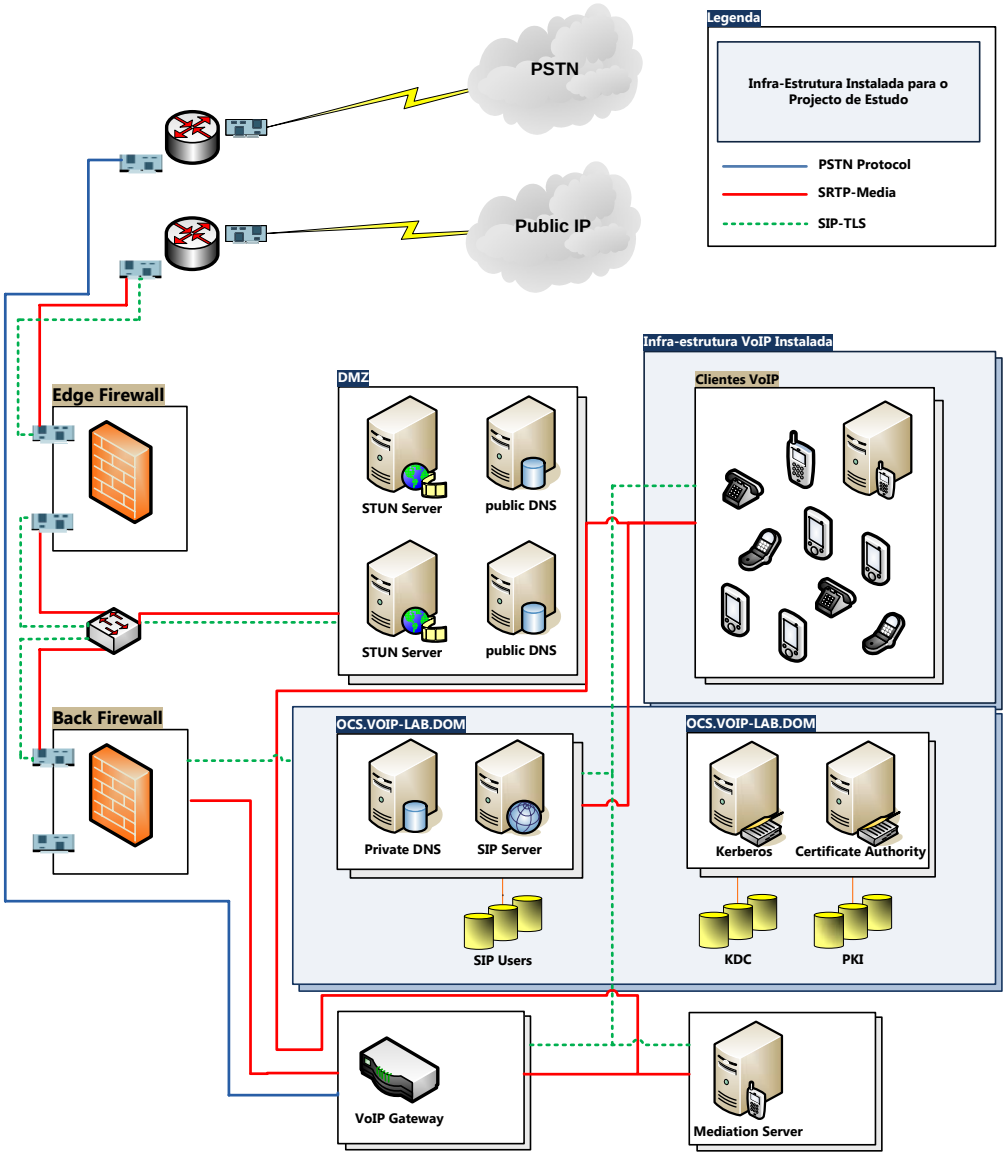
O objectivo deste trabalho de estudo é a constituição de uma infra-estrutura VoIP com segurança. Dada a extrema amplitude de contextos em que o termo segurança pode ser usado na definição dos riscos associados às redes VoIP, isto se considerarmos uma potencial violação de segurança, qualquer ameaça, ataque, ou vulnerabilidade capaz de afectar adversamente o sistema, no contexto deste projecto o termo segurança na infra-estrutura VoIP é alinhado com o objectivo de constituir e implementar as condições que devem fornecer à solução final autorização e autenticação forte, integridade, e confidencialidade durante a transmissão da voz sobre IP.

Neste sentido, o objectivo deste trabalho é constituir uma infra-estrutura VoIP que implemente as seguintes características de segurança:

- Utilização de criptografia simétrica através do protocolo Kerberos e do seu componente Key Distribution Center para autenticação e autorização dos utilizadores.
- Utilização de criptografia de chave pública/privada, através da constituição de infra-estrutura PKI, para criação das condições de segurança SIP-TLS com o objectivo de preservação da confidencialidade e integridade do canal de sinalização.
- Utilização de SRTP para transporte encriptado da voz com o objectivo de preservar a confidencialidade e a integridade da transmissão.

Arquitectura da Infra-estrutura VoIP

A arquitectura da infra-estrutura VoIP, que serve de referência ao trabalho contido neste documento, está representada no diagrama seguinte. Para a realização do trabalho recorreu-se à virtualização de um ambiente que inclui a infra-estrutura contida na área azul do diagrama. Um servidor, chamado `OCS.VOIP-LAB.DOM`, foi instalado e configurado de modo a consolidar nele próprio os serviços e os papéis de servidor SIP, Key Distribution Center, Certificate Authority, e servidor DNS.



Além do servidor `OCS.VOIP-LAB.DOM` a infra-estrutura inclui dois clientes VoIP. O `CLIENTE1.VOIP-LAB.DOM` e o `CLIENTE2.VOIP-LAB.DOM`. Estes clientes estão localizados na infra-estrutura da rede local e correm um SoftPhone que vai ser usado para realizar chamadas de VoIP com segurança.

O papel do DNS no acesso ao LDAP, Kerberos, e domínio SIP

O DNS é um sistema de nomes de domínio que ocupa um papel chave e fundamental na infra-estrutura VoIP.

Os clientes da infra-estrutura utilizam o DNS para localizar o servidor de autenticação Kerberos e para localizar o servidor SIP.

A dependência do servidor DNS é um facto incontornável na infra-estrutura. Este facto coloca o DNS na lista da equação geral da segurança do sistema. É importante recordar que o DNS foi originalmente desenhado como um protocolo aberto sendo por isso vulnerável a tentativas de ataque.

Algumas das ameaças a que o servidor DNS está sujeito incluem:

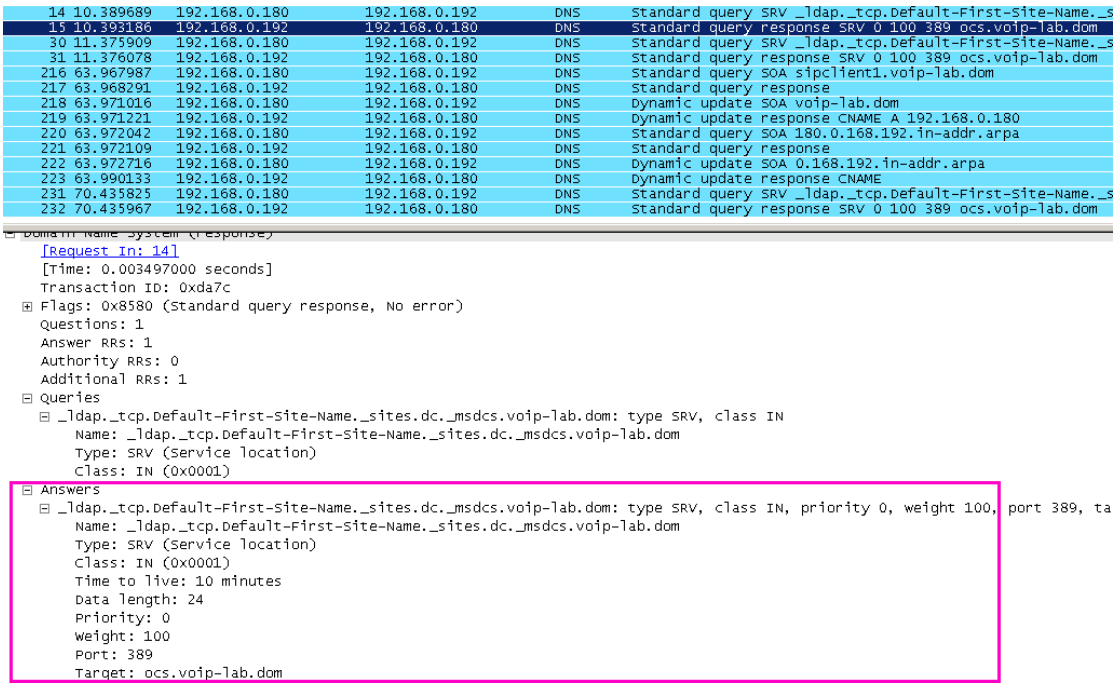
- Footprinting – O footprinting é um termo usado para descrever a capacidade de um atacante usar a informação contida nas zonas DNS para iniciar um processo de enumeração e de esquematização da infra-estrutura e da localização de serviços que este possa publicar.
- Redirecionamento – O redireccionamento é um termo que descreve a capacidade de um atacante desviar os pedidos de resolução DNS para um servidor DNS que ele controle. Uma das formas de conseguir este redireccionamento é através da poluição da cache do servidor DNS com informação preparada para direccionar futuros pedidos de resolução para servidores DNS sob o controlo do atacante.
- Denial-of-Service – Este termo refere-se à capacidade de um atacante esgotar os recursos disponíveis para executar um serviço através da inundação do serviço com inúmeros pedidos de resolução recursiva. Numa infra-estrutura como a que é demonstrada neste projecto de estudo, a indisponibilidade do único servidor DNS resultaria na incapacidade total de operação e do funcionamento do sistema.

Existem outras ameaças ao sistema de nomes de domínio, como por exemplo a capacidade de um atacante possuir a rede e os serviços enumerados (por via do processo de footprinting) e com esta informação criar pacotes IP com endereços IP válidos, dando a estes pacotes a aparência de terem origem em endereços válidos na rede. Este processo é conhecido por IP Spoofing e é um tipo de ataque à segurança extremamente preocupante, na medida em que, com um endereço IP válido numa subnet mask apropriada o atacante pode ter acesso à rede e destruir dados ou conduzir outro tipo de ataques.

No cenário deste projecto de estudo foram implementadas várias medidas fundamentais de segurança para proteger o servidor DNS. O serviço de DNS da infra-estrutura foi configurado para permitir apenas actualizações de zona seguras. Esta configuração implica que o servidor DNS autoritário para a zona referente

ao domínio VOIP-LAB.DOM aceita apenas pedidos de actualização de clientes e servidores autorizados. Outras configurações de segurança efectuadas no DNS incluem a restrição da escuta na interface de rede definida, a protecção contra poluição ou envenenamento da cache, o controlo da recursividade e o controlo da lista dos Root Servers.

Dois aspectos da importância do servidor DNS na infra-estrutura são analisados a seguir. O primeiro relaciona-se com o seu papel na autorização e na autenticação dos participantes na infra-estrutura VoIP por via do Kerberos. O segundo aspecto relaciona-se com o inicio de sessão dos clientes VoIP no domínio SIP.



Na captura do tráfego inicial gerado pelos participantes na infra-estrutura VoIP é possível observar o primeiro instante em que o cliente interroga o servidor DNS para que este lhe indique o endereço IP do sistema LDAP que possui o serviço de directórios que irá autenticar o utilizador. Por motivos relacionados com a capacidade de demonstração da infra-estrutura, o servidor SIP, identificado com o nome OCS.VOIP-LAB.DOM, desempenha todos os papéis de servidor necessários à demonstração da solução. Nestes papéis está incluído o de servidor de Active Directory. O Active Directory é o nome dado a um serviço de directórios assente no protocolo LDAP que armazena informações relativas aos objectos da rede.

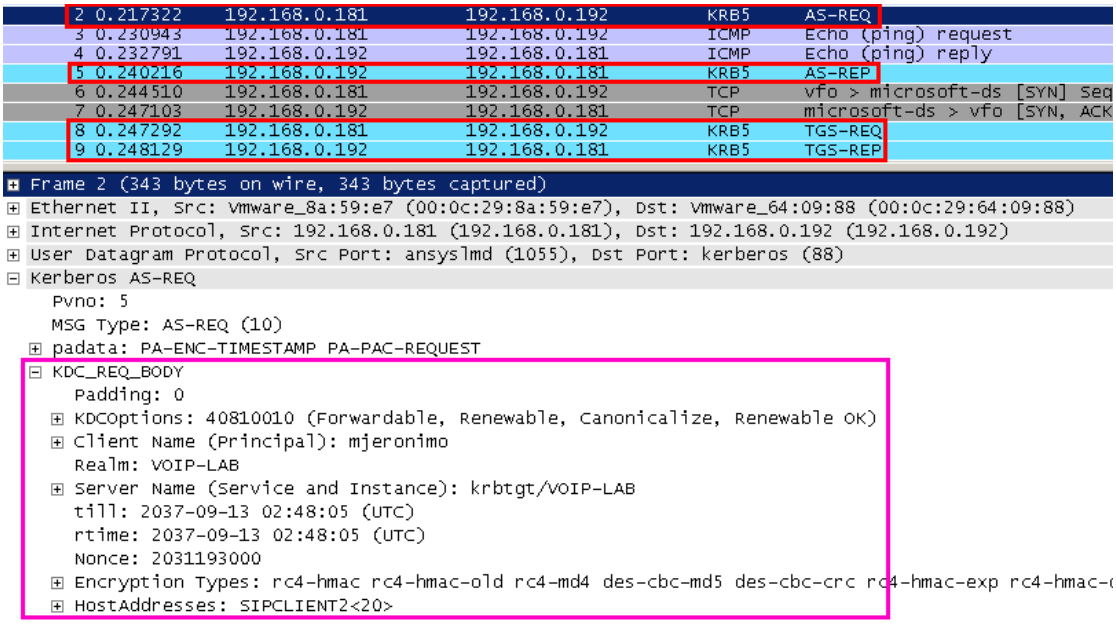
Neste cenário o DNS retorna o nome do servidor que oferece o serviço e o cliente envia um pedido LDAP através da porta UDP 389. Quando o servidor responde ao cliente, este confirma que a reposta contém a

informação correcta e inicia-se o processo de inicio de sessão na infra-estrutura VoIP. No próximo tópico será analisada utilização de Kerberos e a utilização de criptografia de chave simétrica no processo de autenticação e autorização dos utilizadores na infra-estrutura VoIP.

Autenticação e Autorização Kerberos na infra-estrutura VoIP

A segurança da infra-estrutura começa no momento em que um utilizador inicia uma sessão no domínio VOIP-LAB e é autenticado de acordo com as definições do protocolo Kerberos. A utilização de Kerberos no processo de autenticação dos utilizadores é fundamental para a segurança global da infra-estrutura VoIP. Por via da utilização de Kerberos, nenhum tráfego confidencial de autenticação é enviado através da rede em texto legível. Nem a password de autenticação do utilizador no domínio é enviada através da rede, nem mesmo de forma encriptada.

Neste ponto é importante recordar que o Kerberos opera baseado num modelo de autenticação suportado por um segredo partilhado entre o cliente e servidor de autenticação Kerberos, conhecido por criptografia de chave simétrica. Este segredo não é conhecido por nenhuma outra entidade. Quase sempre, e é este o caso nesta infra-estrutura, o segredo é a palavra passe atribuída ao utilizador. Assim, quando o cliente inicia uma sessão no domínio, a sua palavra passe em vez de ser enviada através da rede, é usada para encriptar um pacote de informação que é enviado ao servidor Kerberos. Quando o servidor recebe este pacote, desencripta-o usando uma cópia da mesma palavra passe que tem armazenado. Se a desencriptação suceder, então o servidor Kerberos entende que o cliente conhece o segredo partilhado e a autenticação termina com sucesso.



É igualmente importante mencionar que, nesta fase, o cliente está autenticado, mas isto não lhe confere qualquer acesso a recursos na infra-estrutura VoIP. O cliente terá que repetir este processo para cada recurso

que pretenda aceder. Para gerir este processo o Kerberos utiliza um Key Distribution Center (KDC). Cada KDC é constituído por dois serviços separados: o Authentication Service (AS) e o Ticket Granting Service (TGS). O Authentication Service é responsável pelo inicio de sessão do cliente na infra-estrutura VoIP enviado-lhe um Ticket Granting Ticket (TGT). Na imagem é possível observar uma captura do tráfego Kerberos estabelecido na fase do inicio de sessão de um cliente na infra-estrutura VoIP.

O destaque na imagem é o da segunda frame enviada. Nesta frame é possível observar a construção da mensagem de autenticação que será enviada ao Authentication Server que constitui o Key Distribution Center. Esta mensagem inclui o nome do utilizador, o nome do domínio (realm), o pedido de um Ticket Granting Ticket, e a informação de pré-autenticação encriptada com a chave secreta derivada da palavra passe do utilizador.

O papel do DNS no acesso ao domínio SIP

A infra-estrutura implementada permite que um utilizador depois de autenticado e autorizado possa iniciar sessão no servidor SIP de forma automática. Independentemente da localização do utilizador, dentro ou fora da rede VoIP, esta funcionalidade redirecciona o utilizador automaticamente para o seu servidor SIP. Tal como anteriormente foi observado no processo de localização do servidor de autenticação Kerberos, também na localização do servidor SIP o DNS assume um papel fundamental.

Quando o cliente VoIP é executado, o software interroga o servidor DNS para que este lhe devolva os dados necessários para estabelecer uma ligação, usando autenticação TLS, ao servidor SIP.

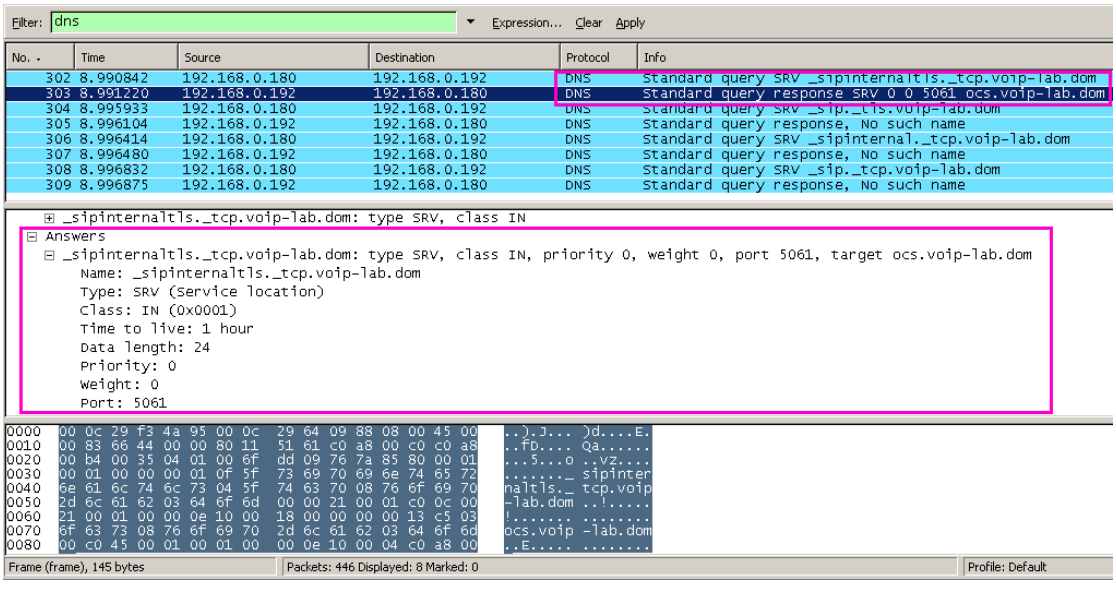
Na captura do tráfego gerado neste processo, na imagem seguinte, é possível observar que o SoftPhone interroga o servidor DNS para que este lhe devolva os nomes dos servidores que ofereçam serviços nos seguintes endereços:

_sipinternaltls._tcp.voip-lab.dom - Usado para ligações SIP com autenticação TLS na infra-estrutura local.

_sipinternal._tcp.voip-lab.dom - Usado para ligações TCP a um SIP Server interno (não autorizado)

_sip._tls.voip-lab.dom - Usado para ligações SIP com autenticação TLS a um SIP Server na Internet.

_sip._tcp.voip-lab.dom - Usado para ligações TCP a um SIP Server na Internet.



A infra-estrutura VoIP implementada está configurada para permitir apenas sessões SIP autenticadas com TLS. As restantes possibilidades não estão autorizadas no actual cenário. Na imagem acima, a resposta do servidor indica o nome do servidor SIP da infra-estrutura local que oferece o serviço SIP com autenticação TLS. Na resposta é visível, entre outros elementos, o nome do servidor SIP-TLS e a porta 5061 que o SoftPhone deve usar para iniciar a negociação de uma comunicação SIP-TLS.

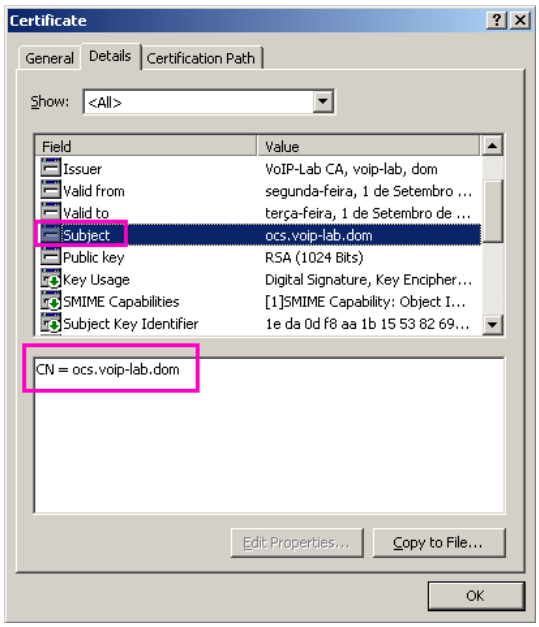
Segurança da Infra-estrutura VoIP com PKI

A infra-estrutura VoIP implementada neste projecto de estudo utiliza certificados digitais para forçar um cenário de autenticação forte no servidor SIP. Um certificado é uma estrutura de software associada a uma chave pública, em que, qualquer informação encriptada com esta chave apenas pode ser desencriptada pelo proprietário da chave privada correspondente.

A configuração desta infra-estrutura de chaves públicas (Public Key Infrastructure, ou PKI) é fundamental para o sucesso da solução. O sistema é gerido por uma entidade denominada Certificate Authority e os seguintes elementos de configuração devem ser destacados:

- **Common Name (CN) ou Subject Name (SN):**

  Identifica o Fully Qualified Domain Name (FQDN) do servidor SIP. Este campo é usado para ligar de forma autoritária o servidor SIP ao seu FQDN. Esta função previne por exemplo um cenário de envenenamento da cache de um servidor DNS que possa comprometer o FQDN do actual servidor. Num cenário de uma infra-estrutura distribuída com vários servidores SIP, o processo de localização entre estes servidores depende da resolução do seu FQDN para um endereço IP. A verificação de que o Common Name no certificado do servidor SIP exibe o FQDN correcto permite autenticar o novo servidor.

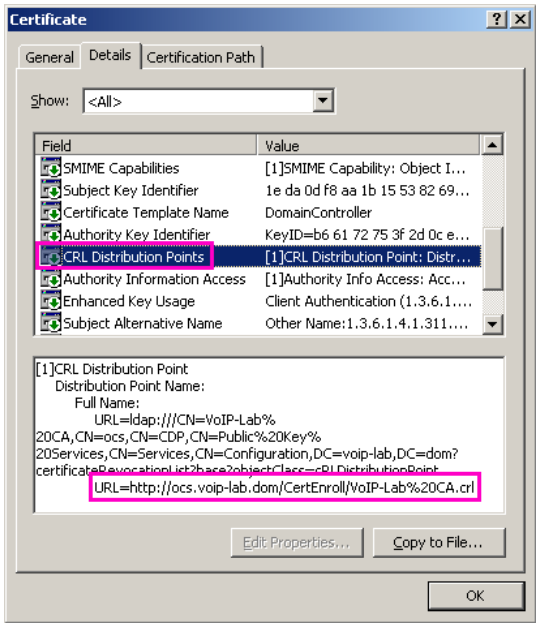


- **Subject Alternative Name (SAN):**

  Este campo pode ser usado para múltiplos domínios SIP nos cenários em que, por questões de negócio, seja conveniente expor múltiplos domínios SIP para a Internet.

- Pontos de Distribuição da **Certificate Revocation List (CRL):**

  Este campo é usado para publicar o local a partir do qual é possível efectuar o download da CRL. A Certificate Revocation List permite verificar se o certificado não foi revogado desde a altura em que foi emitido.



- **Enhanced Key Usage (EKU):**

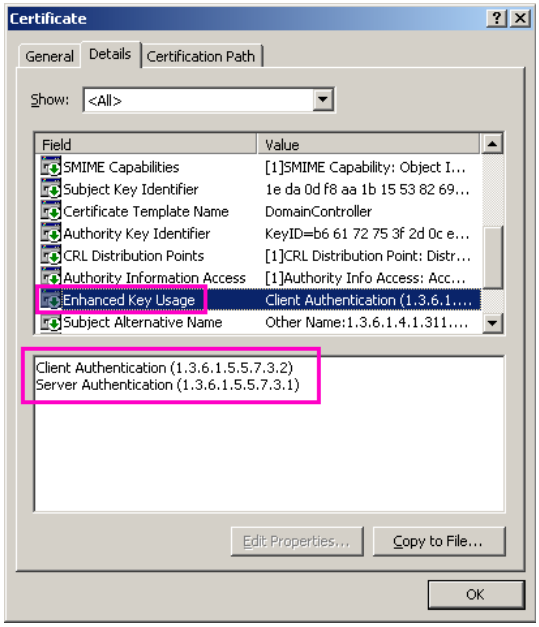
  Este campo identifica e limita o âmbito do certificado. Se o campo não tiver um valor, o certificado é válido para todos os utilizadores. A infra-estrutura VoIP instalada utiliza dois EKUs:

  - **Client Authentication**

    A presença deste EKU é necessária para que seja possível iniciar conexões Mutual-TLS com determinados tipos de servidores SIP.

  - **Server Authentication**

    A presença deste EKU é necessária para o funcionamento do servidor quando é usado Mutual-TLS.



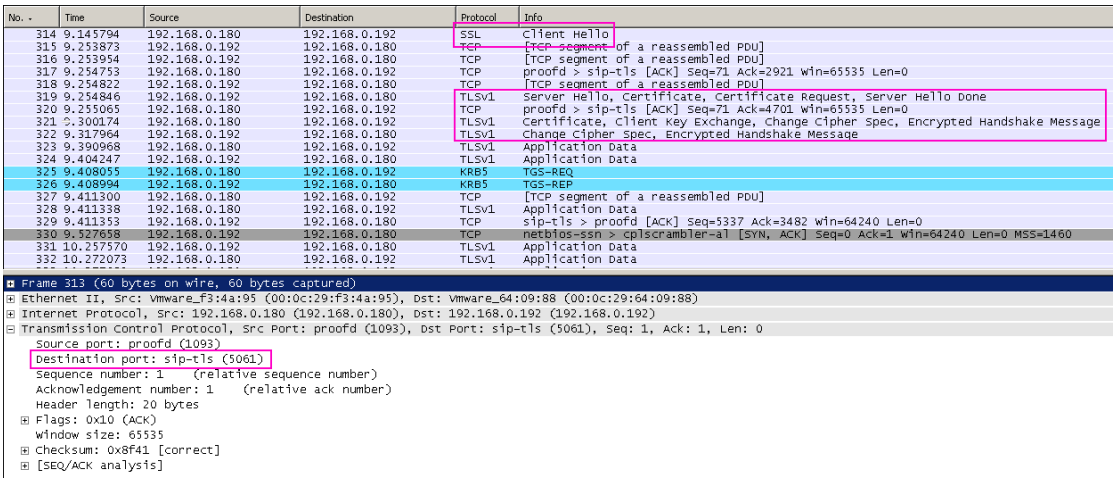
- **Certification Path**:

  O campo Certification Path representa o caminho necessário para alcançar a Certificate Authority.

Segurança da Sinalização SIP através de TLS sobre TCP

Depois do processo de localização do servidor SIP, onde foi analisado o papel determinante do servidor DNS na infra-estrutura VoIP, inicia-se processo de negociação de um canal de comunicações encriptado que vai proteger e criar condições de segurança no protocolo SIP. O SIP, ou Session Initiation Protocol é actualmente considerado um protocolo standard na sinalização multimédia. Trata-se de um protocolo baseado em texto (o H.323 é um protocolo binário) estruturalmente semelhante ao HTTP. Suporta dois tipos de transporte, TCP e UDP e consegue transferir diferentes tipos de payload com diferentes codificações. Qualquer entidade SIP pode iniciar e terminar uma sessão SIP, o que condiciona que qualquer implementação VoIP necessita implementar as funcionalidades de cliente e de servidor.

Na captura do tráfego resultante deste processo, na imagem seguinte, é possível observar o processo de negociação TLS para criar condições de segurança no protocolo SIP.



A negociação TLS envolve, por parte do servidor, uma troca de credenciais e de uma chave de encriptação simétrica que será usada para autenticar e encriptar o canal de comunicações. O processo de negociação TLS envolve os seguintes passos (http://www.ietf.org/rfc/rfc2246.txt):

1. São trocadas mensagens de `hello` e são trocados valores aleatórios com o objectivo de acordar os algoritmos.
2. São trocados parâmetros de criptografia essenciais para o cliente VoIP e o servidor acordarem um segredo inicial.
3. São trocados certificados e dados criptográficos para permitir ao cliente e ao servidor autenticarem-se a si próprios.

4. É gerado, a partir do segredo inicial, um segredo principal e são trocados valores aleatórios.
5. São fornecidos parâmetros de segurança ao TLS Record Layer.
6. Neste ponto o cliente VoIP e o servidor têm condições para verificar que um e outro calcularam os mesmos parâmetros de segurança e que o processo de handshake decorreu de forma íntegra.

Nota: No VoIP os processos de sinalização da chamada e o transporte da voz são da responsabilidade de diferentes protocolos. Esta separação é aliás uma herança de segurança da rede PSTN introduzida pelo sistema de sinalização número 7 (SS7).

Registo do cliente VoIP no Servidor SIP através de Kerberos

Depois da criação das condições de segurança no protocolo SIP através do uso de TLS, conseguida com o suporte da infra-estrutura PKI instalada, da qual a Certificate Authority é parte integrante, o cliente VoIP utiliza o canal de comunicações encriptado para realizar o registo SIP inicial.

Nesta fase da análise ao funcionamento dos protocolos e da segurança da infra-estrutura, foi programada uma função de depuração do processo de registo SIP do cliente VoIP no servidor SIP. Esta configuração permite obter um ficheiro a partir do qual o processo de análise é conveniente quando comparado com software Wireshark, largamente usado para a captura de pacotes e análise de tráfego ao longo deste trabalho. Esta conveniência deve-se à encriptação da sinalização, motivada pelo facto das mensagens SIP decorrerem agora num canal TLS seguro.

O registo do cliente VoIP no servidor SIP utiliza autenticação Kerberos, sendo o processo iniciado com o envio de uma mensagem SIP REGISTER. Esta mensagem é enviada com o objectivo de certificar que o SIP é efectivamente autorizado na porta indicada inicialmente pelo registo SRV no servidor DNS (ver: O papel do DNS no acesso ao domínio SIP), e também para que o cliente descubra qual ou quais os mecanismos de autenticação usados pelo servidor.

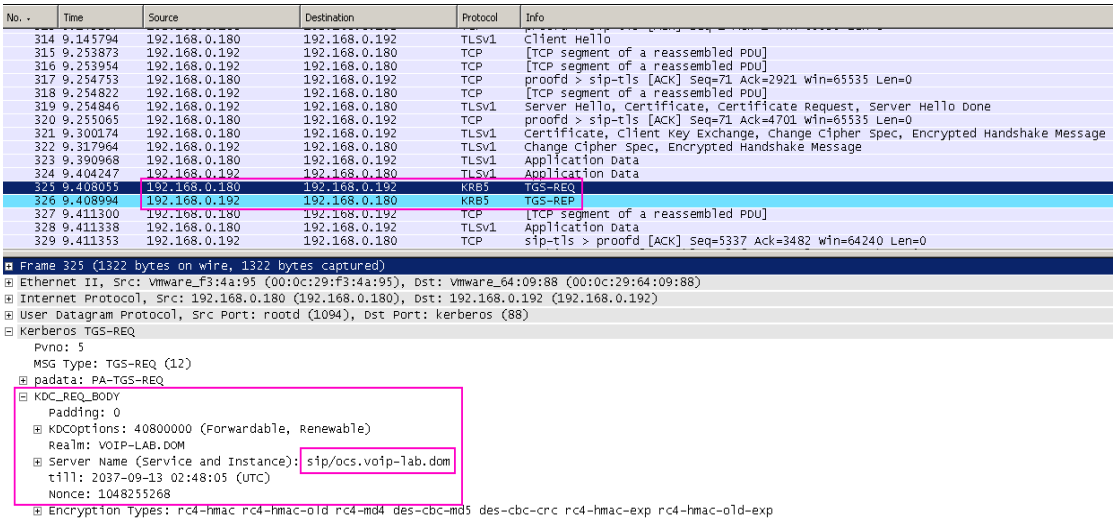
```
 97 REGISTER sip:voip-lab.dom SIP/2.0
 98 Via: SIP/2.0/TLS 192.168.0.180:1073
 99 Max-Forwards: 70
100 From: <sip:pjeronimo@voip-lab.dom>;tag=f0a39764e7;epid=500f738a14
101 To: <sip:pjeronimo@voip-lab.dom>
102 Call-ID: 243219cccd1f4fc8b612439efe92c3bb
103 CSeq: 1 REGISTER
104 Contact: <sip:192.168.0.180:1073;transport=tls;ms-opaque=b864f912af>;methods="INVITE,
105 MESSAGE, INFO, OPTIONS, BYE, CANCEL, NOTIFY, ACK, REFER,
106 BENOTIFY";proxy=replace;+sip.instance="<urn:uuid:FFBB8EA9-ECA2-5DE9-9AED-660FA3D4BBC2>"
107 User-Agent: UCCP/2.0.6362.0 OC/2.0.6362.0 (Microsoft Office Communicator)
108 Supported: gruu-10, adhoclist, msrtc-event-categories
109 Supported: ms-forking-keep-alive: UAC;hop-hop=yes:
110 Event: registrationContent-Length: 0
```

Na imagem anterior é possível observar a mensagem SIP REGISTER enviada ao servidor. Na resposta do servidor SIP é esperado que este interprete que o cliente não está autenticado e que, por este motivo, lhe lance um desafio para se autenticar. Nesta mensagem, que é possível observar na imagem seguinte, o servidor SIP reconhece a fase não autenticada do inicio do registo SIP e responde com a mensagem SIP 401 UNAUTHORIZED. Na mesma mensagem o servidor SIP informa o cliente VoIP que suporta dois mecanismos distintos de autenticação: Kerberos e NTLM. É importante observar que todo este processo decorre no contexto de um canal de comunicações seguro SIP-TLS e que esta mensagem não foi capturada com o analisador de pacotes Wireshark. Tal como foi referido anteriormente, esta mensagem

foi produzida programando uma função especial do servidor SIP que permite depurar este processo para facilidade de análise.

```
125 SIP/2.0 401 Unauthorized
126 Date: Wed, 24 Sep 2008 15:27:58 GMT
127 WWW-Authenticate: NTLM realm="SIP Communications Service",
128 targetname="ocs.voip-lab.dom", version=3
129 WWW-Authenticate: Kerberos realm="SIP Communications Service",
130 targetname="sip/ocs.voip-lab.dom", version=3
131 From: <sip:pjeronimo@voip-lab.dom>;tag=f0a39764e7;epid=500f738a14
132 To: <sip:pjeronimo@voip-lab.dom>;tag=CA2508F942F8ECA1239D52A210C46A2E
133 Call-ID: 243219cccd1f4fc8b612439efe92c3bb
134 CSeq: 1 REGISTER
135 Via: SIP/2.0/TLS 192.168.0.180:1073;ms-received-port=1073;ms-received-cid=100
136 Content-Length: 0
```

Não está em destaque na imagem acima, mas é possível também observar que a resposta do servidor SIP inclui igualmente, no campo `targetname`, o servidor `ocs.voip-lab.dom` com o qual o cliente VoIP tem que autenticar-se. A infra-estrutura VoIP configurada e descrita neste projecto de estudo implementa Kerberos para autenticação e autorização. Por este motivo o cliente VoIP vai aceitar o desafio de se autenticar no servidor SIP através de Kerberos. Para o efeito o cliente responde ao servidor enviando-lhe uma nova mensagem REGISTER de resposta onde aceita o desafio de se autenticar através de Kerberos. O facto do cliente VoIP ter tomado conhecimento, na resposta anterior do servidor SIP, que o servidor com o qual tem que autenticar-se chama-se `ocs.voip-lab.dom` faz com que o cliente solicite ao servidor de autenticação Kerberos um Ticket Granting Ticket que lhe permita validar-se perante o desafio de autenticação Kerberos que lhe foi lançado pelo servidor SIP, e que ele aceitou.



Na imagem anterior regressou-se temporariamente ao analisador de pacotes WireShark para observar o momento em que o cliente VoIP solicita ao servidor de autenticação Kerberos o TGT atrás referido.

A imagem seguinte já é a do depurador do registo no servidor SIP, sendo possível observar o envio das credenciais Kerberos.

```
157 REGISTER sip:voip-lab.dom SIP/2.0
158 Via: SIP/2.0/TLS 192.168.0.180:1073
159 Max-Forwards: 70
160 From: <sip:pjeronimo@voip-lab.dom>;tag=f0a39764e7;epid=500f738a14
161 To: <sip:pjeronimo@voip-lab.dom>
162 Call-ID: 243219cccd1f4fc8b612439efe92c3bb
163 CSeq: 2 REGISTER
164 Contact: <sip:192.168.0.180:1073;transport=tls;ms-opaque=b864f912af>;methods="INVITE,
165 MESSAGE, INFO, OPTIONS, BYE, CANCEL, NOTIFY, ACK, REFER,
166 BENOTIFY";proxy=replace;+sip.instance=
167 "<urn:uuid:FFBB8EA9-ECA2-5DE9-9AED-660FA3D4BBC2>"
168 User-Agent: UCCP/2.0.6362.0 OC/2.0.6362.0 (Microsoft Office Communicator)
169 Authorization: Kerberos qop="auth", realm="SIP Communications Service",
170 targetname="sip/ocs.voip-lab.dom", gssapi-data=
171 "YIIEvQYJKoZIhvcSAQICAQBuggSsMIIEqKADAgEFoQMCAQ6iBwMFAAAAAACjggPRYYIDzT
172 CCA8mgAwIBBaEOGwxWT01QLUxBQi5ET02iIjAgoAMCAQKhGTAXGwNzaXAbEG9jcy52b2lwLWxhY
173 i5kb22jggOMMIIDiKADAgEXoQMCAQKiggN6BIIDdrDzK11lhwW2ZQbee3LiofoTlWrZ3rC0iawx
174 m8oYm/L84JfouBp5DSkMlUAiROSF0woCThOUkkQ6OjcRVoRA1adX9hv/EjTyaLWb47Csn2Ryj4I
175 dHPkjDWTnSFpR0PgxtgQYn6wtgAFYYsAxtYuNXM74YVz4rjJG0habkpVKyHhnyFAkEMfjWYN+Nh
176 TbajduTIm3i3reqyybAVEYGK++M6SihKZEeVfDIIeRayR/6SPOHRhZ5pxkz/20MiIAEPzafzbs1
177 50+C5fNt+/4xGbyhAYfSYX5x0r+eQS9MdOyBBUoQrB39ZRTFean5aqUvLeNAp1niCsOmAyIpQ1s
178 I0GQ19B9g1nATcWYHVV/8vNw1Fwb++iqMPm9H3WuPhh1eOWoJWxE8KIAZMwChpeITZmebPEZKcd
179 klpAuX9nuCbUU6E86D7SWsCPZT41+gw9kpwPkkAGL0GOUk+JcCT5Yxw33tQMAfHudzZKjedd3jy
180 wue5nTRIgIs1lrFYjzS8hKxQag+PqoDh5Zp5GfB9i2adZhqb5E6xVxI7h+Dy5EOit9ih3w98d4j
181 0QQXAZZsVzBxmuSlyzsj1UN+szp1ozqokF6/w4U8oGJ0VNnbqPZbL4GYTuc4zpnOd2VuomirmMd
182 H6ywVb3BiwSCTBhxz1iPObGpPDGI8EcnRGasaq4HQvewS7y2/xS1p1rmIZvf4L/0J134V06KEgP
183 fo/zZHCq35dZn2P1wwX4bs50662yeYmg6heN1IAS7d5eLAIZhl2t4zEHopHC+jFfpGe5E48L0CY
184 ElGA1SVJr/zHapTo/k0d+9BOZEsorb79WR+tmbemoIW+XxSBjQT/1PbW1Ylm5KkvxvUV26BuEZk
185 rTFo3k5UVptAW3XixZbOr3dQrwKCZZvl6hnAZCb4keSblt7AHYzDZHExr3whlCX+w6MmDgjhe24
186 mwBcsbtdQOLKHR8bHOtx7mwHr5pFFogK87mpLT9xNX8veDDWNWbPWqoxdbKX3+B1Iy7ekSKxXEq
187 oE4ae3rFYKL/SjQYW0HuweuNmGWMBsYK2GPCf0ypH6YoB+e/FkzH2nIn6GZpQyzlzKZRXuMFzEU
188 tuOrkakZUhS3vsHETmZdOLa48Apr4GZ801hHVM1MCECCAgXKlUidWRiAGbPFv500kUOPdMj875f
189 Nu/cCPm0FfJpkweO0zqamKkgb0wgbqgAwIBF6KBsgSBr2YAo+sQKCx3tXOSBcrRSe7FLdT6yZZ2
190 CNv13fb6hoTbhao5C2HjxI78BkWeSVJ6n/GY0zWetdIvoEC5k4ES1mwE8GvcZCLSxoW1IjvlLjV
191 Eiqf7IN5xGwR6Wn8EFxuEafirVMqixI+PQowU3mjG85RuLqIr/CMSUDEAePyBPvQktCro8x/ZV4
192 OmOdLBdw95nRMICc8wEhQV6Y1+CrAoOLqHFfbn68/7zUVx8ZiAB80=", version=3
193 Supported: gruu-10, adhoclist, msrtc-event-categories
194 Supported: ms-forking
195 ms-keep-alive: UAC;hop-hop=yes
196 Event: registration
197 Content-Length: 0
```

As credenciais Kerberos podem constituir e ocupar uma parte significativa da mensagem para o handshake inicial, mas na realidade este custo acaba por revelar-se mínimo tendo em conta a segurança que fornece ao protocolo de sinalização. É importante referir que as futuras mensagens trocadas vão referenciar unicamente as credenciais e enviar um conjunto de dados mínimo para validar as chaves embebidas neste processo.

O processo de registo de forma segura do cliente VoIP no servidor SIP termina com o servidor a responder à mensagem de autenticação Kerberos com a mensagem 200 OK. Nesta mensagem o servidor SIP inclui credenciais para sua própria autenticação que permitem ao cliente VoIP provar que o servidor é de confiança.

```
212 SIP/2.0 200 OK
213 ms-keep-alive: UAS; tcp=no; hop-hop=yes; end-end=no; timeout=300
214 Authentication-Info: Kerberos rspauth="602306092A864886F71201020201011100FFFFFFFF
215 EBEBDE869CC13E05AE64932E13738FBA", srand="9CEAA17E", snum="1", opaque="CC4DCD15",
216 qop="auth", targetname="sip/ocs.voip-lab.dom", realm="SIP Communications Service"
217 From: "Paulo Jeronimo"<sip:pjeronimo@voip-lab.dom>;tag=f0a39764e7;epid=500f738a14
218 To: <sip:pjeronimo@voip-lab.dom>;tag=CA2508F942F8ECA1239D52A210C46A2E
219 Call-ID: 243219cccd1f4fc8b612439efe92c3bb
220 CSeq: 2 REGISTER
221 Via: SIP/2.0/TLS 192.168.0.180:1073;ms-received-port=1073;ms-received-cid=100
222 Contact: <sip:192.168.0.180:1073;transport=tls;ms-opaque=b864f912af;ms-received-cid=100>;
223 expires=7200;+sip.instance="<urn:uuid:ffbb8ea9-eca2-5de9-9aed-660fa3d4bbc2>";gruu=
224 "sip:pjeronimo@voip-lab.dom;opaque=user:epid:qY67_6Ls6V2a7WYPo9S7wgAA;gruu"
225 Expires: 7200
226 presence-state: register-action="added"
227 Allow-Events: vnd-microsoft-provisioning,vnd-microsoft-roaming-contacts,
228 vnd-microsoft-roaming-ACL,presence,presence.wpending,vnd-microsoft-roaming-self,
229 vnd-microsoft-provisioning-v2
230 Supported: adhoclist
231 Server: RTC/3.0
232 Supported: msrtc-event-categories
233 Content-Length: 0
```

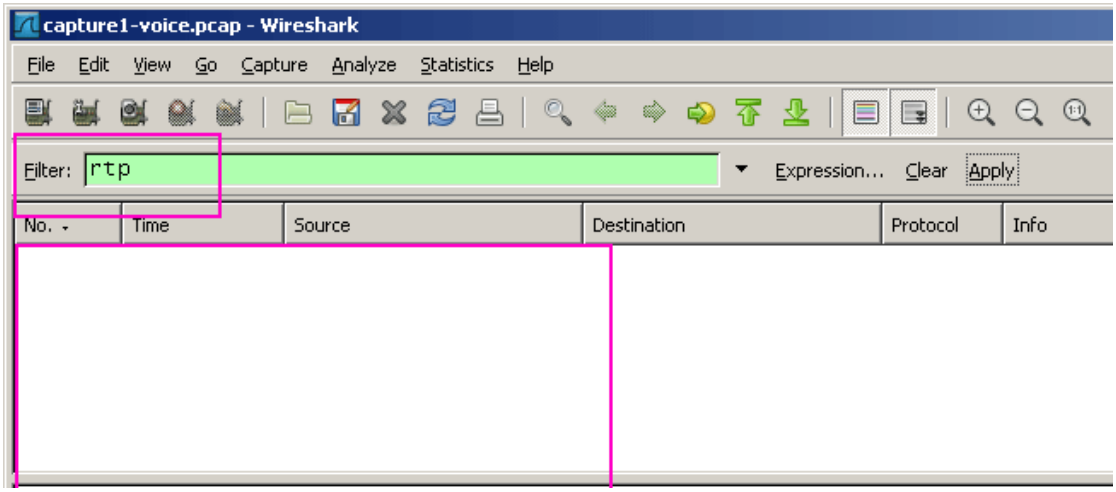
É possível também identificar no header `Authentication-Info` os campos `rspauth` e `targetname`. Estes campos incluem os dados criptográficos que fazem prova de que o servidor de autenticação identifica-se a ele próprio com o nome `ocs.voip-lab.dom`. No final da mensagem, o header `Expires` informa o cliente VoIP durante quanto tempo este registo é válido no servidor SIP. O processo de registo tem que ser refrescado depois de decorridas 2 horas (7200 segundos).

Segurança do transporte da voz através de SRTP e ICE

Os pacotes que transportam a voz são protegidos ponto-a-ponto através do protocolo Secure Real-Time Transport Protocol (SRTP). Esta característica de segurança fornece ao transporte da voz na infra-estrutura VoIP confidencialidade e integridade. A chave usada para encriptar e desencriptar a voz é passada sobre TLS dentro do canal seguro de sinalização.

Este mecanismo de segurança realiza a troca de chaves Advanced Encryption Standard (AES) de 128-bit sobre o canal de sinalização seguro que ambas as partes utilizam para encriptar e desencriptar a voz durante a conversação.

O SRTP encripta a stream de áudio entre duas entidades VoIP independentemente do tipo de codec usado. A combinação de SRTP com SRTCP permite encriptar a stream de áudio, mas também permite controlar a própria sessão SRTP. A análise dos pacotes SRTP que transportam a voz entre as partes não é facilmente identificada devido ao facto do analisador de pacotes Wireshark, bem como o Network Monitor, ou Sniffer Pro, não incluírem parsers SRTP.



Na imagem acima configurou-se um filtro no programa Wireshark para listar apenas frames RTP. Como é possível observar, nenhuma frame RTP aparece listada devido ao facto do WireShark não possuir um parser para SRTP. O uso de AES no SRTP possibilita o processamento ordenado de pacotes mesmo que estes tenham sido recebidos fora de ordem.

No inicio de cada sessão VoIP os clientes utilizam o protocolo Interactive Connectivity Establishment (ICE) para, de forma dinâmica, escolher o melhor percurso para a voz. O protocolo ICE prefere os caminhos directos aos caminhos que usam relays de voz, assim como caminhos UDP em relação a

caminhos TCP. O ICE assume um papel fundamental na infra-estrutura VoIP uma vez que para muitos utilizadores de redes corporativas, e apesar de o UDP ser para a voz um transporte mais eficiente, a única forma que têm de alcançar a internet é através de TCP. O ICE posiciona-se estrategicamente na decisão por um transporte da voz sobre TCP quando um caminho UDP não está disponível.

O protocolo ICE é baseado nos protocolos Simple Traversal Underneath NAT (STUN) e Traversal Using Relay NAT (TURN). O ICE é uma solução para que a voz atravesse de forma segura NATs e Firewalls. No cenário instalado e configurado para este projecto de estudo, outros servidores e equipamentos poderiam ser instalados de forma a expandir a infra-estrutura. A realização de chamadas para a rede PSTN requer a introdução de dois componentes adicionais na infra-estrutura: um Mediation Server e uma forma de alcançar a rede PSTN, tal como um SIP Gateway. A função do Mediation Server é converter o codec Real-Time Audio (RTA) para G.711 MuLaw ou ALaw para comunicar via SIP com outras gateways VoIP. A infra-estrutura suporta os codecs G.722.1, G.723, G.726, GSM, RTA Wide, e RTA Narrow. Os Mediation Servers podem ser emparelhados com os Gateways VoIP, ou podem ser instalados múltiplos Mediation Servers a apontar para um único Gateway VoIP. O Mediation Server pode também ser usado como interface com sistemas TDM Hybrid ou outros IP-PBX através de trunks SIP.

Conclusão

Este trabalho centrou-se na constituição da infra-estrutura de segurança e na análise dos diversos componentes e protocolos que podem ser usados na criação das condições necessárias à autenticação, autorização, integridade e privacidade na transmissão da voz sobre o protocolo IP. Para a realização do trabalho implementou-se um sistema de criptografia simétrica baseado no protocolo Kerberos e observou-se com detalhe o papel que o Key Distribution Center assume na autenticação e autorização dos utilizadores na infra-estrutura. Observou-se e analisou-se também o papel chave do protocolo Kerberos na autenticação dos clientes SIP. Foi analisada a importância do servidor DNS na infra-estrutura e foi por fim analisada a implementação e o funcionamento do sistema de criptografia de chave pública/privada (PKI), do qual a Certificate Authority é parte integrante, e o seu papel na criação de canais de comunicação seguros por via de TLS.

Uma infra-estrutura VoIP requer, para além da segurança, a observação de outros conceitos, riscos, e requisitos. Para complementar o actual trabalho e produzir um estudo baseado numa análise mais abrangente da infra-estrutura VoIP, teria sido necessário considerar outros aspectos igualmente críticos, como aqueles relacionados com a qualidade do serviço e dos meios envolvidos na transmissão. Noutro âmbito, e tendo em conta que a qualidade de serviço (QoS) é fundamental para a operacionalidade de uma rede VoIP, o actual estudo poderia ser desenvolvido, e conduzido analisando as questões de segurança em paralelo com as questões de QoS, nomeadamente a análise do impacto de problemas como a latência, os efeitos e as técnicas de controlo do Jitter, o impacto da perca de pacotes e as estratégias de mitigação do problema, e de uma forma geral alargando o estudo e a análise às questões que influenciam a largura de banda.

Este foi no entanto um projecto de estudo conduzido com muito entusiasmo, na medida em que foram ultrapassados diversos desafios de operacionalização dos componentes necessários à infra-estrutura. Nesta perspectiva este foi também um importante processo de aquisição de competências e de consolidação de conhecimentos adquiridos no domínio da segurança em redes VoIP,

Referências

RFC 4120 - The Kerberos Network Authentication Service (V5)
http://www.ietf.org/rfc/rfc4120.txt

RFC 3261 - SIP: Session Initiation Protocol
http://www.ietf.org/rfc/rfc3261.txt

RFC 2246 - The TLS Protocol Version 1.0
http://www.ietf.org/rfc/rfc2246.txt

RFC 3550 – RTP Real-Time Transport Protocol
http://www.ietf.org/rfc/rfc3550.txt

Secure Real-time Transport Protocol
http://en.wikipedia.org/wiki/Secure_Real-time_Transport_Protocol

Security Considerations for Voice over IP Systems
http://csrc.nist.gov/publications/nistpubs/800-58/SP800-58-final.pdf

Addison-Wesley, Securing VoIP Networks – Theaths, Vulnerabilities, and Countermeasures, Peter Thermos and Ari Takaren, ISBN 0321437349

Microsoft Press - Office Communications Server Resource Kit, Jeremy Buch, Rui Maximo, Jochen Kunert, ISBN 0735624062

McGraw-Hill/Osborne - Hacking VoIP Exposed – Voice Over IP Security Secrets & Solutions, David Endler, Mark Collier, ISBN-9780072263640