Aplicações e comportamento da fragmentação EAP

Índice

Introdução

Este documento descreve como compreender e pesquisar defeitos sessões do Extensible Authentication Protocol (EAP). Estas edições são discutidas:

- Comportamento de server do Authentication, Authorization, and Accounting (AAA) quando retornarem o certificado de servidor para a sessão da Segurança da camada do Protocolo-transporte da autenticação extensível (EAP-TLS)
- Comportamento dos suplicantes quando retornarem o certificado de cliente para a sessão do EAP-TLS
- Interoperabilidade quando o suplicante nativo de Microsoft Windows e o gerente do acesso de rede de Cisco AnyConnect (NAM) forem usados
- Fragmentação no processo IP, de RAIO, e de EAP-TLS e de remontagem executado por

dispositivos do acesso de rede
- O atributo da unidade de transmissão do Framed-máximo do RAIO (MTU)
- O comportamento dos servidores AAA quando executarem a fragmentação de pacotes do EAP-TLS

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Protocolos EAP e de EAP-TLS
- Configuração do Cisco Identity Services Engine (ISE)
- Configuração de CLI do Switches do Cisco catalyst

Énecessário ter uma boa compreensão do EAP e do EAP-TLS a fim compreender este artigo.

Certificate chain retornado pelo server

O servidor AAA (Access Control Server (ACS) e ISE) retorna sempre a corrente completa para o pacote do EAP-TLS com os servidores hello e o certificado de servidor:

O certificado de identidade ISE (Common Name (CN) =lise.example.com) é retornado junto com o Certificate Authority (CA) que assinou o CN=win2012,dc=example,dc=com. O comportamento é o mesmo para o ACS e o ISE.

Certificate chain retornado pelo suplicante

Suplicante do nativo de Microsoft Windows

O suplicante nativo de Microsoft Windows 7 configurado a fim usar o EAP-TLS, com ou sem a “seleção de certificado simples”, não envia a corrente completa do certificado de cliente. Este comportamento ocorre mesmo quando o certificado de cliente está assinado por CA diferente (corrente diferente) do que o certificado de servidor.

Este exemplo é relacionado aos servidores hello e ao certificado apresentados no tiro de tela precedente. Para essa encenação, o certificado ISE é assinado por CA com o uso de um nome do sujeito, CN=win2012,dc=example,dc=com. Mas o certificado de usuário instalado na loja de Microsoft é assinado por CA diferente, CN=CA, C=PL, S=Cisco CA, L=Cisco CA, O=Cisco CA.

Em consequência, o suplicante de Microsoft Windows responde com o certificado de cliente somente. CA que o assina (CN=CA, S=PL, S=Cisco CA, L=Cisco CA, O=Cisco CA) não é anexado.

Devido a este comportamento, os servidores AAA puderam encontrar problemas quando validam certificados de cliente. O exemplo relaciona-se ao profissional de Microsoft Windows 7 SP1.

Solução

Um certificate chain completo deve ser instalado na loja do certificado de ACS e de ISE (todo o CA e CA secundário que assinam certificados de cliente).

Os problemas com validação certificada podem facilmente ser detectados no ACS ou no ISE. A informação sobre o certificado não confiável é apresentada e relatório ISE:

```
12514 EAP-TLS failed SSL/TLS handshake because of an unknown CA in the client
certificates chain
```

Os problemas com validação certificada no suplicante não são facilmente detectáveis. Geralmente o servidor AAA responde que o “valor-limite abandonou a sessão EAP”:

AnyConnect NAM

O AnyConnect NAM não tem esta limitação. Na mesma encenação, anexa a corrente completa do certificado de cliente (CA correto é anexado):

Suplicante nativo de Microsoft Windows junto com AnyConnect NAM

Quando ambos os serviços estão acima, AnyConnect NAM toma a precedência. Mesmo quando o serviço NAM não é executado, ainda engancha em Microsoft Windows o API e para a frente os pacotes EAP, que podem causar problemas para o suplicante do nativo de Microsoft Windows. Está aqui um exemplo de tal falha.

Você permite o seguimento em Microsoft Windows com este comando:

```
C:\netsh ras set tracing * enable
```

A mostra dos traços (**c:\windows\trace\svchost _RASTLS.LOG**):

```
[2916] 09-14 21:29:11:254: >> Received Request (Code: 1) packet: Id: 55, Length:
6, Type: 13, TLS blob length: 0. Flags: S
[2916] 09-14 21:29:11:254: << Sending Response (Code: 2) packet: Id: 55, Length:
105, Type: 13, TLS blob length: 95. Flags: L
[1804] 09-14 21:29:11:301: >> Received Request (Code: 1) packet: Id: 56, Length:
1012, Type: 13, TLS blob length: 2342. Flags: LM
[1804] 09-14 21:29:11:301: << Sending Response (Code: 2) packet: Id: 56, Length:
6, Type: 13, TLS blob length: 0. Flags:
[1804] 09-14 21:29:11:348: >> Received Request (Code: 1) packet: Id: 57, Length:
1008, Type: 13, TLS blob length: 0. Flags: M
[1804] 09-14 21:29:11:348: << Sending Response (Code: 2) packet: Id: 57, Length:
6, Type: 13, TLS blob length: 0. Flags:
[1804] 09-14 21:29:11:363: >> Received Request (Code: 1) packet: Id: 58, Length:
344, Type: 13, TLS blob length: 0. Flags:
[1804] 09-14 21:29:11:363: << Sending Response (Code: 2) packet: Id: 58, Length:
1492, Type: 13, TLS blob length: 1819. Flags: LM
[3084] 09-14 21:31:11:203: >> Received Request (Code: 1) packet: Id: 122, Length:
```

```
6, Type: 13, TLS blob length: 0. Flags: S
[3084] 09-14 21:31:11:218: << Sending Response (Code: 2) packet: Id: 122, Length:
105, Type: 13, TLS blob length: 95. Flags: L
[3420] 09-14 21:31:11:249: >> Received Request (Code: 1) packet: Id: 123, Length:
1012, Type: 13, TLS blob length: 2342. Flags: LM
[3420] 09-14 21:31:11:249: << Sending Response (Code: 2) packet: Id: 123, Length:
6, Type: 13, TLS blob length: 0. Flags:
[3420] 09-14 21:31:11:281: >> Received Request (Code: 1) packet: Id: 124, Length:
1008, Type: 13, TLS blob length: 0. Flags: M
[3420] 09-14 21:31:11:281: << Sending Response (Code: 2) packet: Id: 124, Length:
6, Type: 13, TLS blob length: 0. Flags:
[3420] 09-14 21:31:11:281: >> Received Request (Code: 1) packet: Id: 125, Length:
344, Type: 13, TLS blob length: 0. Flags:
[3420] 09-14 21:31:11:296: << Sending Response (Code: 2) packet: Id: 125, Length:
1492, Type: 13, TLS blob length: 1819. Flags: LM
```

O último pacote é um certificado de cliente (fragmento 1 do EAP-TLS com tamanho 1492 EAP) enviado pelo suplicante do nativo de Microsoft Windows. Infelizmente, Wireshark não mostra esse pacote:

E esse pacote não é enviado realmente (último era o terceiro fragmento do certificado de servidor levando do EAP-TLS). Foi consumido pelo módulo de NAM de AnyConnect esse os ganchos em Microsoft Windows API.

Épor isso não se recomenda para usar AnyConnect junto com o suplicante do nativo de Microsoft Windows. Quando você usa todos os serviços de AnyConnect, recomenda-se para usar igualmente o NAM (quando os serviços do 802.1x são precisados), não o suplicante do nativo de Microsoft Windows.

Fragmentação

A fragmentação pôde ocorrer em camadas múltiplas:

- IP
- Pares do valor de atributo RADIUS (AVP)
- EAP-TLS

O Switches do ® do Cisco IOS é muito inteligente. Podem compreender formatos EAP e de EAP-TLS. Embora o interruptor não possa decifrar o túnel TLS, é responsável para a fragmentação, e o conjunto e a remontagem dos pacotes EAP quando encapsulamento no protocolo extensible authentication sobre LAN (EAPoL) ou RAIO.

O protocolo EAP não apoia a fragmentação. Está aqui um trecho do RFC 3748 (EAP):

A “fragmentação não é apoiada dentro de EAP próprio; contudo, os métodos de EAP individuais podem apoiar este.”

O EAP-TLS é tal exemplo. Está aqui um trecho do RFC 5216 (EAP-TLS), a seção 2.1.5 (fragmentação):

“Quando um par do EAP-TLS recebe um pacote do EAP-pedido com o jogo do bit M, DEVE responder com uma EAP-resposta com EAP-Type=EAP-TLS e nenhuns dados. Isto serve como um fragmento ACK. **O server EAP DEVE esperar até que receba a EAP-resposta antes de enviar um outro fragmento**.”

A última frase descreve uma característica muito importante dos servidores AAA. Devem esperar o ACK antes que possam enviar um outro fragmento EAP. Uma regra similar é usada para o suplicante:

“O par EAP DEVE esperar até que receba o EAP-pedido antes de enviar um outro fragmento.”

Fragmentação na camada IP

A fragmentação pode ocorrer somente entre o dispositivo do acesso de rede (NAD) e o servidor AAA (IP/UDP/RADIUS usado como um transporte). Esta situação ocorre quando o NAD (interruptor do Cisco IOS) tenta enviar a requisição RADIUS que contém o payload EAP, que é então um MTU mais grande da relação:

A maioria de versões do Cisco IOS não são inteligentes bastante e não tentam montar os pacotes EAP recebidos através de EAPoL e combiná-los em um pacote de informação de RADIUS que possa caber no MTU da interface física para o servidor AAA.

Os servidores AAA são mais inteligentes (como apresentado nas próximas seções).

Fragmentação no RAIO

Este não é realmente nenhum tipo da fragmentação. Conforme o RFC 2865, um único atributo RADIUS pode ter até 253 bytes de dados. Devido ao esse, o payload EAP é transmitido sempre em atributos RADIUS múltiplos do mensagem EAP:

Aqueles atributos do mensagem EAP são remontados e interpretados por Wireshark (do “o atributo último segmento” revela o payload do pacote EAP inteiro). O encabeçamento do comprimento no pacote EAP é to1,012 igual, e quatro RAIOS AVP são exigidos para transportá-lo.

Fragmentação no EAP-TLS

Do mesmo tiro de tela, você pode ver aquele:

- O comprimento do pacote EAP é 1,012
- O comprimento do EAP-TLS é 2,342

Isto sugere que seja o primeiro fragmento do EAP-TLS e o suplicante deva esperar mais, que podem ser confirmadas se você examina as bandeiras do EAP-TLS:

Este tipo da fragmentação ocorre mais frequentemente em:

- Acesso-desafio do RAIO enviado pelo servidor AAA, que leva o EAP-pedido com o certificado de servidor do secure sockets layer (SSL) com a corrente inteira.
- A solicitação de acesso do RAIO envia pelo NAD, que leva a EAP-resposta com o certificado de cliente SSL com a corrente inteira.

Confirmação do fragmento do EAP-TLS

Como explicado mais cedo, cada fragmento do EAP-TLS deve ser reconhecido antes que os fragmentos subsequentes estejam enviados.

Está aqui um exemplo (capturas de pacote de informação para EAPoL entre o suplicante e o NAD):

Os quadros de EAPoL e o servidor AAA retornam o certificado de servidor:

- Esse certificado é enviado em um fragmento do EAP-TLS (pacote 8).
- O suplicante reconhece esse fragmento (pacote 9).
- O segundo fragmento do EAP-TLS é enviado por NAD (pacote 10).
- O suplicante reconhece esse fragmento (pacote 11).
- O terceiro fragmento do EAP-TLS é enviado por NAD (pacote 12).
- O suplicante não precisa de reconhecer este; um pouco, continua com o certificado de cliente que começa no pacote 13.

Estão aqui os detalhes do pacote 12:

Você pode ver que Wireshark remontou os pacotes 8, 10, e 12. O tamanho do EAP fragmenta is1,002, 1,002, e 338, que traz o tamanho total da mensagem do EAP-TLS a 2342 (o tamanho da mensagem total do EAP-TLS é anunciado em cada fragmento). Isto pode ser confirmado se você examina pacotes de informação de RADIUS (entre o NAD e o servidor AAA):

Os pacotes de informação de RADIUS 4, 6, e 8 levam aqueles três fragmentos do EAP-TLS. Os primeiros dois fragmentos são reconhecidos. Wireshark pode apresentar a informação sobre os fragmentos do EAP-TLS (tamanho: 1,002 + 1,002 + 338 = 2,342).

Estes encenação e exemplo eram fáceis. O interruptor do Cisco IOS não precisou de mudar o tamanho do fragmento do EAP-TLS.

Fragmentos do EAP-TLS remontados com tamanho diferente

Considere o que acontece quando o NAD MTU para o servidor AAA é 9,000 bytes (Jumbo Frame) e o servidor AAA é conectado igualmente com o uso da relação que apoia o Jumbo Frames. A maioria dos suplicantes típicos são conectados com o uso de um link 1Gbit com um MTU de 1,500.

Em tal encenação, o interruptor do Cisco IOS executa o conjunto e a remontagem “assimétricos” do EAP-TLS e muda tamanhos dos fragmentos do EAP-TLS. Está aqui um exemplo para um grande mensagem EAP enviado pelo servidor AAA (certificado de servidor SSL):

1. O servidor AAA deve enviar uma mensagem do EAP-TLS com um certificado de servidor SSL. O tamanho total desse pacote EAP é 3,000. Depois que é encapsulado no RAIO Access-Challenge/UDP/IP, é ainda menos do que a interface MTU do servidor AAA. Um único pacote IP é enviado com atributos do mensagem EAP de 12 RAIOS. Não há nenhuma fragmentação IP nem de EAP-TLS.

2. O interruptor do Cisco IOS recebe tal pacote, decapsulates ele, e decide que o EAP precisa de ser enviado através de EAPoL ao suplicante. Desde que EAPoL não apoia a fragmentação, o interruptor deve executar a fragmentação do EAP-TLS.

3. O interruptor do Cisco IOS prepara o primeiro fragmento do EAP-TLS que pode caber no MTU da relação para o suplicante (1,500).

4. Este fragmento é confirmado pelo suplicante.

5. Um outro fragmento do EAP-TLS é enviado depois que o reconhecimento é recebido.

6. Este fragmento é confirmado pelo suplicante.

7. O último fragmento do EAP-TLS é enviado pelo interruptor.

Esta encenação revela aquela:

- Sob algumas circunstâncias, o NAD deve criar fragmentos do EAP-TLS.
- O NAD é responsável para enviar/que reconhece aqueles fragmentos.

A mesma situação pode ocorrer para um suplicante conectado através de um link que apoie o Jumbo Frames quando o servidor AAA tiver um MTU menor (então o interruptor do Cisco IOS cria fragmentos do EAP-TLS quando envia o pacote EAP para o servidor AAA).

Atributo RADIUS Framed-MTU

Para o RAIO, há um atributo Framed-MTU definido no RFC 2865:

“Este atributo indica a unidade de transmissão máxima a ser configurada para o usuário, quando não é negociado por alguns outros meios (tais como o PPP). PODE ser usado em uns pacotes de aceitação acesso. **PODE ser usado em um pacote de solicitação de acesso como uma sugestão pelo NAS ao server que preferiria esse valor, mas o server não é exigido para honrar a sugestão.**”

O ISE não honra a sugestão. O valor do Framed-MTU enviado pelo NAD na solicitação de acesso não tem nenhum impacto na fragmentação executada pelo ISE.

O Switches moderno múltiplo do Cisco IOS não permite mudanças ao MTU da interface Ethernet à exceção dos ajustes do Jumbo Frames permitidos globalmente no interruptor. A configuração do Jumbo Frames impacta o valor do atributo Framed-MTU enviado na solicitação de acesso do RAIO. Por exemplo, você ajustou-se:

```
Switch(config)#system mtu jumbo 9000
```

Isto força o interruptor para enviar Framed-MTU = 9000 em todas as solicitações de acesso do RAIO. O mesmos para o MTU de sistema sem Jumbo Frames:

```
Switch(config)#system mtu 1600
```

Isto força o interruptor para enviar Framed-MTU = 1600 em todas as solicitações de acesso do RAIO.

Observe que o Switches moderno do Cisco IOS não permite que você diminua o valor do MTU de sistema abaixo de 1,500.

Servidores AAA e comportamento do suplicante quando você enviar fragmentos

EAP

ISE

O ISE tenta sempre enviar os fragmentos do EAP-TLS (geralmente servidores hello com certificado) que são 1,002 bytes por muito tempo (embora o último fragmento é geralmente menor). Não honra o RAIO FRAMED-MTU. Não é possível reconfigurá-lo para enviar uns fragmentos mais grandes do EAP-TLS.

Servidor da política da rede Microsoft (NP)

Épossível configurar o tamanho dos fragmentos do EAP-TLS se você configura o atributo Framed-MTU localmente em NP.

O evento embora configurar o tamanho de virulência EAP no artigo de Microsoft NP menciona que o valor padrão de um MTU moldado para o servidor Radius NP é 1,500, o laboratório do centro de assistência técnica da Cisco (TAC) mostrou que envia 2,000 com as configurações padrão (confirmadas em Microsoft Windows 2012 Datacenter).

Testa-se que ajustando o Framed-**MTU localmente** conforme o guia previamente mencionado está respeitado por NP, e fragmenta os mensagens EAP em fragmentos de um tamanho ajustado no Framed-MTU. Mas o atributo Framed-MTU recebido na solicitação de acesso não é usado (o mesmos que em ISE/ACS).

Ajustar este valor é uma ação alternativa válida a fim fixar edições na topologia como esta:

Suplicante [MTU 1500] ---- ---- [MTU 9000]Switch [MTU 9000] ----- ----- [MTU 9000]NPS

Atualmente o Switches não permite que você ajuste o MTU pela porta; para 6880 Switch, esta característica é adicionada com identificação de bug Cisco CSCuo26327 - EAP-TLS do 802.1x que não trabalha em portas de host FEX.

AnyConnect

AnyConnect envia os fragmentos do EAP-TLS (geralmente certificado de cliente) que são 1,486 bytes por muito tempo. Para este tamanho do valor, o frame da Ethernet é 1,500 bytes. O último fragmento é geralmente menor.

Suplicante do nativo de Microsoft Windows

Microsoft Windows envia os fragmentos do EAP-TLS (geralmente certificado de cliente) que são 1,486 ou 1,482 bytes por muito tempo. Para este tamanho do valor, o frame da Ethernet é 1,500 bytes. O último fragmento é geralmente menor.

Informações Relacionadas

- Configurando a autenticação com base na porta do IEEE 802.1X
- Suporte Técnico e Documentação - Cisco Systems