



Segurança no DataSnap com Delphi XE3

Leandro Matos

A PALAVRA CHAVE É "SEGURANÇA"



Preocupações



- Sempre nos preocupamos com a regra de negócio, e a segurança de tudo que foi feito. Pense:
 - "Como vou garantir para meu cliente que as informações dele estão seguras?"
 - "Como irei garantir que outra aplicação não use meu servidor de aplicação?"
 - "Se um funcionário mal intencionado sair da empresa, como faço para que o mesmo não tenha acesso ao servidor de aplicação?"

Soluções



Enfim, temos soluções para nossas preocupações, tanto para validações de utilizações do nosso Servidor de Aplicação, quando para a troca de informações entre as Aplicações

"Client" e os "Servers".

Mudanças no Delphi



 Uma das grandes mudanças do Delphi a partir da versão Delphi 2009 até hoje com o Delphi XE3 é o Framework do "DataSnap";

 Com isso conseguimos ter controle total sobre a segurança de nossas "AppServers"

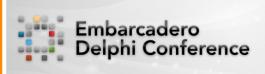






- É importante sabemos o papel de cada um na área de segurança do DataSnap:
- Acesso a Rede:
 - Porta, Servidor, Perfil de Usuário interno na Rede;

"Administradores de Rede"



Qual o nosso papel como Desenvolvedores;

Acesso a Aplicação;

Troca de informação entre as nossas APPs;



 Mesmo com os papéis definidos, não podemos esquecer uma camada muito importante, no qual ainda não falamos:

Qual é esta camada?





"O Banco de Dados" é uma outra peça fundamental a ser protegida; mas não iremos abordar aqui; falaremos apenas a parte das APPs "Delphi"

BLOQUEAR O ACESSO DIRETO



Bloqueando o Acesso Direto



- Da versão do Delphi 4 até a versão do Delphi 2007 tínhamos muitos problemas com segurança, e varias limitações.
 - Isso hoje não ocorre, pois temos domínio completo sobre nossas APPs;
 - Sobre conexão direta, temos um "Firewall" ótimo, chamado de TDSServer;
 - Qualquer aplicação que tentar acessar pára nele;

Bloqueando o Acesso Direto "TDSServer"



 O TDSSever torna minha APP uma Aplicação servidora e nele tem o Evento "OnConnect" e o "OnDisconnect";

 Iremos bloquear o Acesso direto no Evento "OnConnet", deixando assim o "Bloqueio Genérico" pois o mesmo vai travar qualquer tentativa de acesso ao nosso servidor;

Bloqueando o Acesso Direto



Então vamos bloquear este acesso direto;

"Mãos a Obra"

TRANSPORT FILTERS



Troca de Informações



 Novidade que temos com o Framework do DataSnap são os "Transport Filters" em nossa palestra iremos falar somente dos relacionados a segurança;

PC1;

RSA;

Customizados;

Troca de Informações "PC1 E RSA"



- Os filtros de criptografia que acompanham o Delphi são os PC1 e RSA;
 - Seu papel é garantir a criptografia entre a troca de informações "APP Server" e "APP Cliente";
 - Utilizam a tecnologia de criptografia existente na OpenSSL;
 - Necessitam ter duas dlls no servidor "libeay32.dll" e a "ssleay32.dll";

Troca de Informações "PC1 E RSA" - OPENSSL



- O OpenSSL é uma implementação de código aberto dos protocolos SSL e TLS, que está escrita em linguagem C;
 - Ela é baseada no Ssleay de Eric Young e Tim Hudson;
 - Importante para sistemas operacionais em 64 bytes (baixar do caminho descrito abaixo as Dlls)

http://indy.fulgan.com/SSL/

Troca de Informações "PC1 E RSA"



 Vamos ver na prática como podemos criptografar as informações trocadas entre APPServer e APPClient, fazendo uso do filter PC1 e RSA

"Mãos a Obra"

CRIANDO UM FILTER "NOVO NO DATASNAP"



Troca de Informações



 Mesmo tendo o suporte nativo no framework do DataSnap aos Filters PC1 e RSA podem surgir dúvidas:

- Será que esta criptografia logo mais não será obsoleta, e fácil de quebrar?
- E se a minha APPClient for em outra linguagem e não entender essa criptografia?
- Será que eu não poderia criar meus próprios Filters?

Filter Customizado



 Sim - podemos criar nossos próprios Filters, tanto para compactação, quando para criptografia, que é o foco de nossa palestra.

O Processo é bem simples como tudo no Delphi, basta saber duas coisas:

Qual a criptografia que iremos trabalhar;

E saber criar uma BPL no Delphi um Pacote;

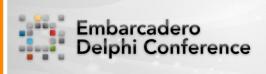
Filter Customizado



 Temos alguns pontos importantes que devemos saber:

- A Classe que implementa os Filters no Delphi é a Classe TTransportFilter;
- A Função ProcessImput é responsável pela entrada da informação;
- A Função ProcessOutput é responsável pela saída da informação;

Filter Customizado



 Vamos ver na pratica como podemos criptografar as informações trocadas entre APPServer e APPClient, fazendo o nosso próprio filter

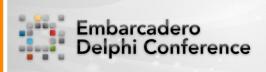
"Mãos a Obra"

Considerações Finais



- Lembre-se: temos inúmeras alternativas de segurança:
 - Validação do usuário que poderá acessar;
 - Criptografia da informação usando RCA ou PC1 direto nativas no Delphi;
 - Uso da criptografia que temos já existente no nosso ambiente de trabalho, pois essa temos domínio total;
- Outra situação que não abordamos é via HTTPs usando certificados digitais, hoje muito utilizado pelo governo brasileiro.

Links interessantes



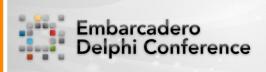
- Docwiki Filters
 http://docwiki.embarcadero.com/RADStudio/XE/en/
 Filtering_DataSnap_Byte_Stream
- OpenSSL http://openssl.org
- Transport Filters
 Pawel Glowacki
 http://edn.embarcadero.com/article/41293
- Comunidade Delphi
 Leandro Matos
 http://comunidadedelphi.blogspot.com.br

Perguntas?



- Portal de Treinamentos e Vagas http://www.edobrasil.net/treinamentos
- Embarcadero Developer Network http://edn.embarcadero.com
- Diretório de MVP's http://www.embarcadero.com.br/mvp-directory
- Documentação dos Produtos http://docs.embarcadero.com
- CodeRage 7 http://www.embarcadero.com/coderage
- YouTube http://youtube.com/user/embarcaderodobrasil
- Twitter http://twitter.com/EmbarcaderoTech
- Blogs: http://blogs.embarcadero.com
- Facebook: https://www.facebook.com/pages/Embarcadero-Delphi-Brasil/399151510134179
- atendimento@embarcadero.com.br
- (11) 5643-1333

Obrigado!



Leandro Matos



leandro@tdstecnologiasp.com.br

http://comunidadedelphi.blogspot.com

http://facebook.com/TDS-Tecnologia