Grupo de Resposta a Incidentes de Segurança – GRIS
Departamento de Ciência da Computação
Universidade Federal do Rio de Janeiro

Encriptação no meebo

Estamos seguros mesmo?

Por: Manoel Fernando de Sousa Domingues Junior

Rio de Janeiro – Brasil
2009

Universidade Federal do Rio de Janeiro
Instituto de Matemática
Departamento de Ciência da Computação
Grupo de Resposta a Incidentes de Segurança

Rio de Janeiro, RJ – Brasil

Encriptação no meebo

GRIS-2009-A-NUM

Manoel Fernando de Sousa Domingues Junior

V. 1.0.
A versão mais recente deste documento pode ser obtida na página oficial do GRIS.

Índice

1- Introdução....4
1.1 – O que é o meebo?....4
2 – Indo aos experimentos....5
2.1 – Procedimentos....5
2.2 – Ambiente dos experimentos....5
2.3 – Executando o teste....5
3 – Conclusões a cerca do teste....7
4 – Criptografia no meebo 8
4.1 - o SSL....8
4.2 – o TLS....9
5 – Referências....9

Índice de ilustrações

Página inicial do meebo em julho de 2009....4
Topologia de rede para experimento....5
Captura dos pacotes transferidos entre o cliente (10.10.10.197) e meebo (208.81.191.110) com navegador compatível com SSL e TLS....6
Pacotes com conteúdo criptografado....6
Captura dos pacotes transferidos entre o cliente (10.10.10.197) e meebo (208.81.191.110) com navegador sem suporte a SSL e TLS....7
Pacote com login em texto puro....8

1- Introdução

Com a grande massificação do uso da internet, diversas formas de comunicação foram criadas, porém a que mais se intensificou foi a feita através de mensageiros instantâneos.

Com o surgimento da web 2.0 em meados de 2004 e seu conceito de web como plataforma, começaram a ser criados webmessengers, que são na verdade, serviços que rodam na nuvem dispensando a instalação de aplicativos localmente.

1.1 – O que é o meebo?

O meebo é um serviço da web 2.0 fundado em 2005, que permite que usuários de diversas redes de mensageiros instantâneos se comuniquem sem ter que fazer a instalação e utilização de aplicativos localmente. Seu principal diferencial é sua interface de fácil utilização e o fato de poder reunir amigos em uma lista para se comunicar em tempo real utilizando diferentes protocolos de comunicação instantânea.

Hoje o meebo conta com mais de 50 milhões de pessoas partilhando mais de 5 bilhões de mensagens por mês, além de ser uma das redes socias em maior crescimento na web.[1]

Ilustração 1: Página inicial do meebo em julho de 2009

[1] Dados retirados da página do meebo na internet em 29 de julho de 2009

2 – Indo aos experimentos

2.1 – Procedimentos

Os procedimentos realizados no teste consistiram em montar um ambiente de rede controlado em que seria colocado um computador executando um sniffer na rede e outro se conectando ao serviço meebo.

2.2 – Ambiente dos experimentos

Para executar os testes de segurança foi montada uma topologia de rede em ambiente controlado seguindo o seguinte modelo.

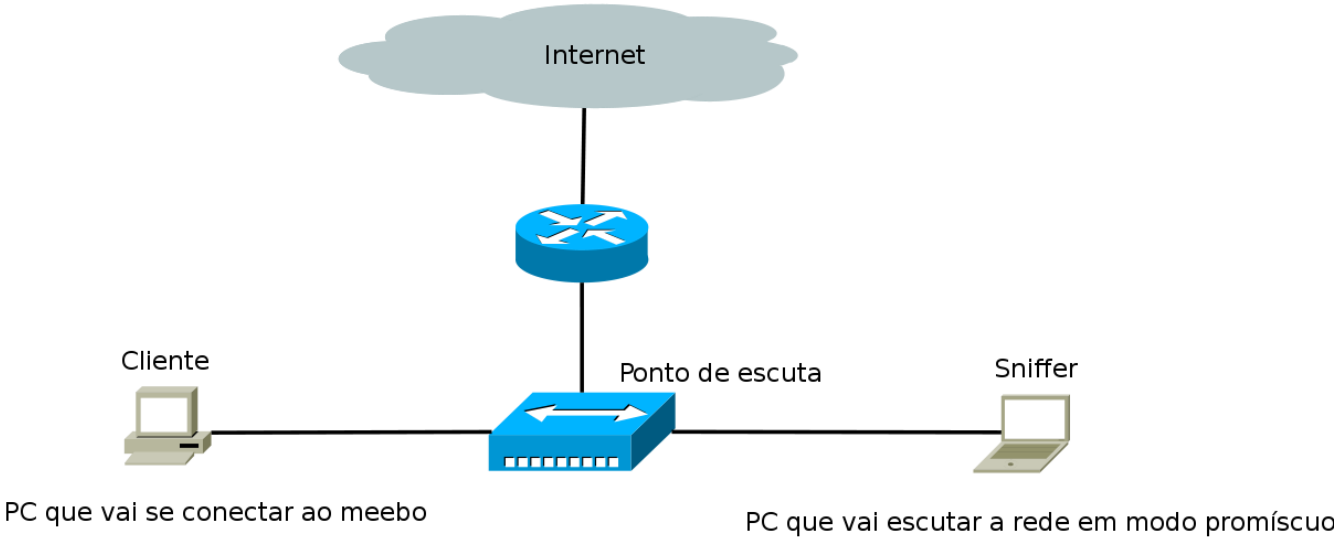

Ilustração 2: Topologia de rede para experimento

Softwares usados em cada computador:

- O computador que vai se conectar ao meebo está rodando linux e usando como navegadores o Mozilla Firefox 3.5.2 e Opera 10.00, ambos com o SSL e TLS, ora habilitados, ora desabilitados;
- O computador que vai escutar a rede em modo promiscuo está rodando linux e usando como sniffer o Wireshark 1.2.1.

2.3 – Executando o teste

Já com o software sniffer aberto e em modo de captura, nos conectamos ao meebo, e inserimos um login e senha.

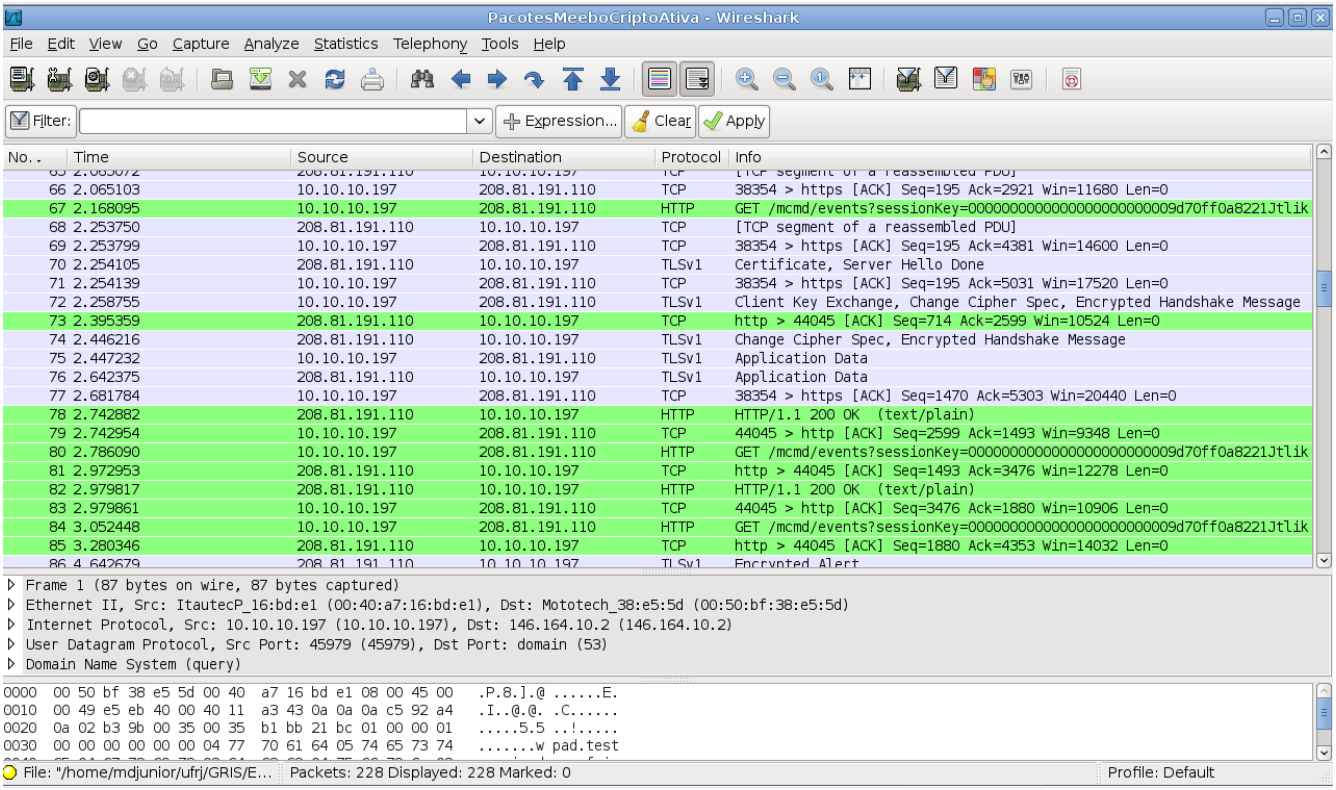

Ilustração 3: Captura dos pacotes transferidos entre o cliente (10.10.10.197) e meebo (208.81.191.110) com navegador compatível com SSL e TLS

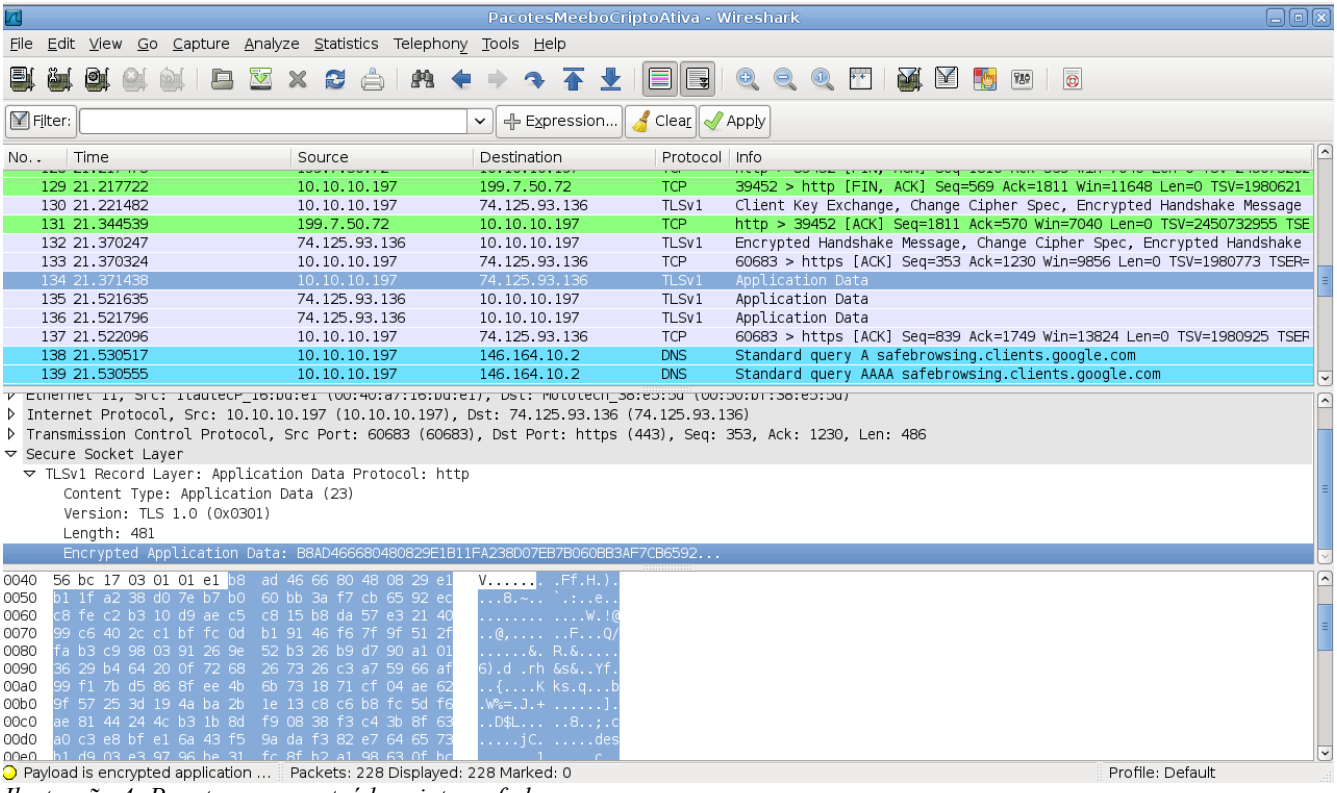

Ilustração 4: Pacotes com conteúdo criptografado

3 – Conclusões a cerca do teste

Tendo sido realizados inumeros testes para comprovar a veracidade dos resultados aqui representados, temos que o meebo utiliza criptografia (TLS 1.0, como se pode observar na ilustração 5) somente para o campo no qual diz respeito a senha de usuário, se o navegador for compatível com esse padrão. Caso o navegador não seja compatível com o TLS, o meebo utiliza um JavaScript em sua página para criptografar a senha com sua chave pública.

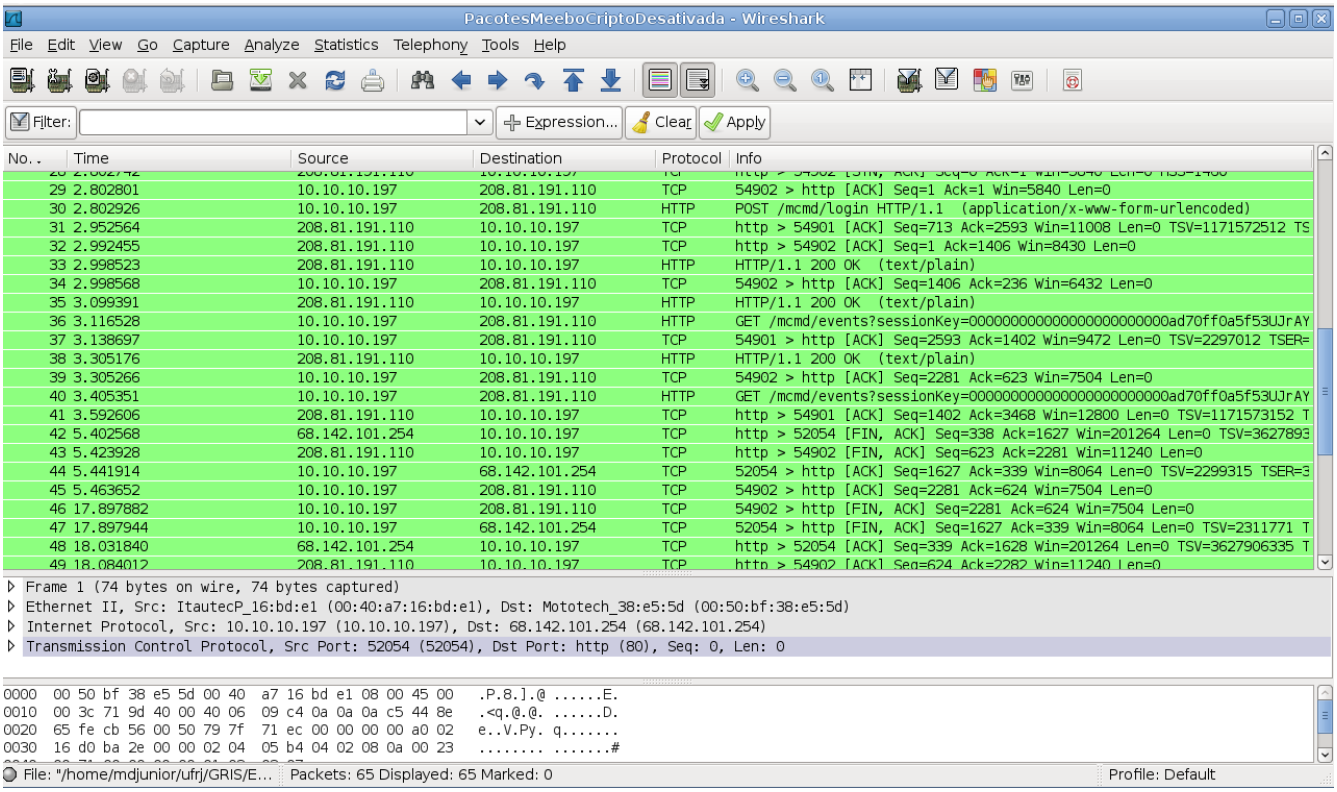

Ilustração 5: Captura dos pacotes transferidos entre o cliente (10.10.10.197) e meebo (208.81.191.110) com navegador sem suporte a SSL e TLS

Um fato importante de se observar, é que ao contrário do que diz a documentação do meebo, somente a senha é criptografada ficando o login em texto puro.

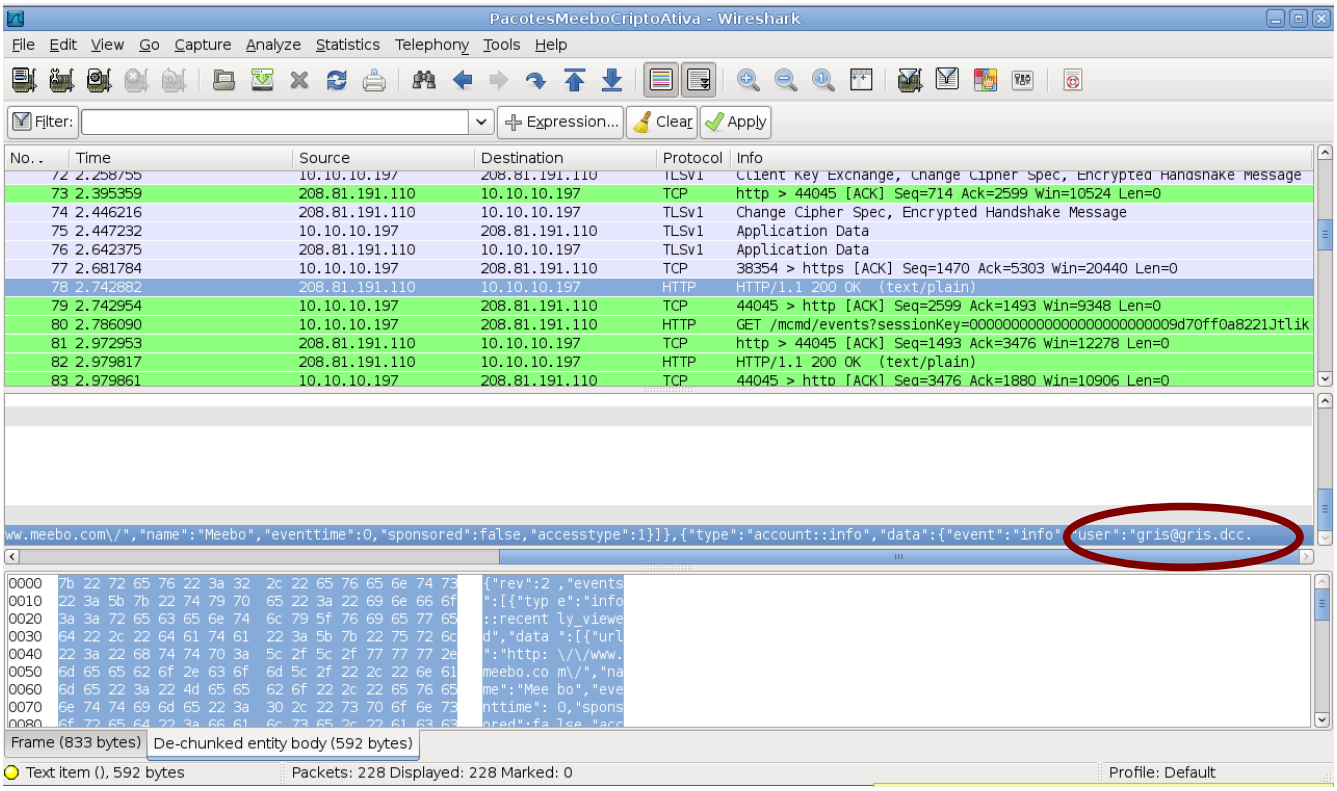

Ilustração 6: Pacote com login em texto puro

De acordo com o próprio site, ele não criptografa a página e as conversas para garantir a velocidade e uma melhor experiencia de uso. Para aqueles que preferem sacrificar a velocidade em busca de maior segurança, o serviço meebo disponibiliza o endereço: https://www.meebo.com, em que todo conteúdo é criptografado.

Outro fato interessante é que nem o descontinuado webmessenger da microsoft, o que era mais usado no Brasil, apresentava opções envolvendo criptografia de todo conteúdo.

4 – Criptografia no meebo

4.1 - o SSL

Com o uso crescente das redes de computadores nos anos 90, principalmente a internet, aumentou também a necessidade da criação de canais seguros para comunicação de dados sensíveis, dentro de redes que em sua maioria não garantem privacidade, integridade e autenticidade dos dados que nelas trafegam.

Assim foi criado o protocolo SSL, que provê privacidade, integridade e autenticidade dos dados que trafegam entre duas aplicações na rede. Isto ocorre através da autenticação das partes envolvidas e da criptografia dos dados transmitidos entre as partes. Esse protocolo ajuda a prevenir que intermediários entre as duas pontas da

comunicação tenham acesso indevido ou falsifiquem as informações que estão sendo transmitidas.

O SSL, atualmente na versão 3, funciona de forma simples: o servidor envia seu certificado digital para o cliente e este confere sua autenticidade, caso a autenticidade seja contestada a conexão é encerrada, se este for autêntico o cliente envia a requisição da chave pública do servidor, com a chave pública o cliente criptografa as informações e as envia para o servidor, somente o servidor com sua chave privada pode descriptografar as informações. Dessa forma temos a autenticidade, confidencialidade e integridade dos dados transferidos.

4.2 – o TLS

O TLS 1.0 é uma evolução do SSL 3.0. Suas principais diferenças são:

- TLS é padronizado pelas RFC 2246 (v1.0) e RFC 4346 (v1.1)
- TLS usa o algoritmo keyed-Hashing for Message Authentication Code (HMAC) enquanto o SSL apenas Message Authentication Code (MAC). O algoritmo HMAC produz hashes mais seguros que o algoritmo MAC
- No TLS nem sempre é necessário recorrer à raiz de uma AC (Autoridade de Certificação) para usar uma certificação. Pode ser usada uma autoridade intermediária
- Novas mensagens de alerta
- O algoritmo Fortezza de criptografia não é suportado, pois não é aberto ao público. (Política da IETF)
- Diferenças em alguns campos dos cabeçalhos

No mais suas características principais permanecem iguais ao SSL 3.0.

5 – Referências

- Documentação oficial do meebo - http://www.meebo.com/security/
- Grupo de Teleinformática e Automação – http://www.gta.ufrj.br
- Wikipedia: A enciclopédia livre – http://pt.wikipedia.org
- RFC 5246 - http://www.rfc-editor.org/rfc/rfc5246.txt