Grupo de Resposta a Incidentes de Segurança – Bahia/Brasil
Ponto de Presença da RNP na Bahia
Universidade Federal da Bahia

CERT.Bahia <certbahia@pop-ba.rnp.br>

Webinar sobre Heartbleed

06 de Maio de 2014

Sobre o CERT.Bahia

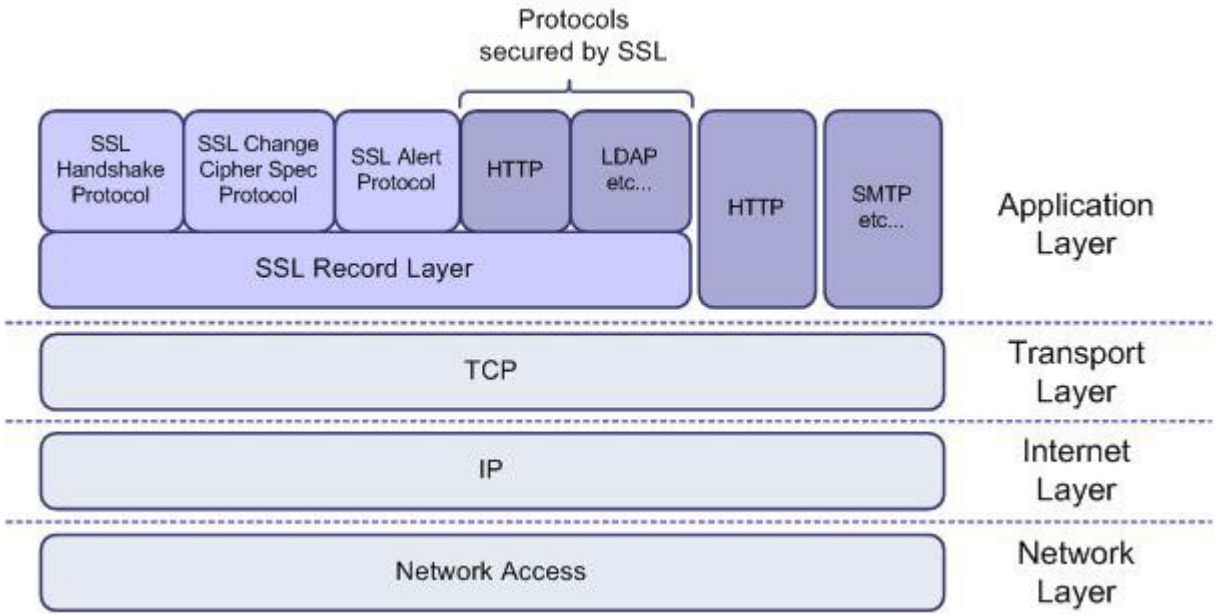
- Missão

  Auxiliar as instituições conectadas ao POP-BA/RNP e RedeCOMEP (ReMeSSA) na prevenção, detecção e tratamento dos incidentes de segurança, além de criar e disseminar boas práticas para uso e administração seguros das Tecnologias de Informação e Comunicação (TIC).

- Constituency
  - Instituições qualificadas na política de uso da RNP na Bahia
  - Instituições parceiras da ReMeSSA
- Site:
  - http://certbahia.pop-ba.rnp.br/

Definições: SSL/TLS

SSL/TLS provê comunicação segura e privada na Internet sobre as diversas aplicações, tais como: web, email, mensagens instantâneas (IM) e redes virtuais privadas (VPNs).



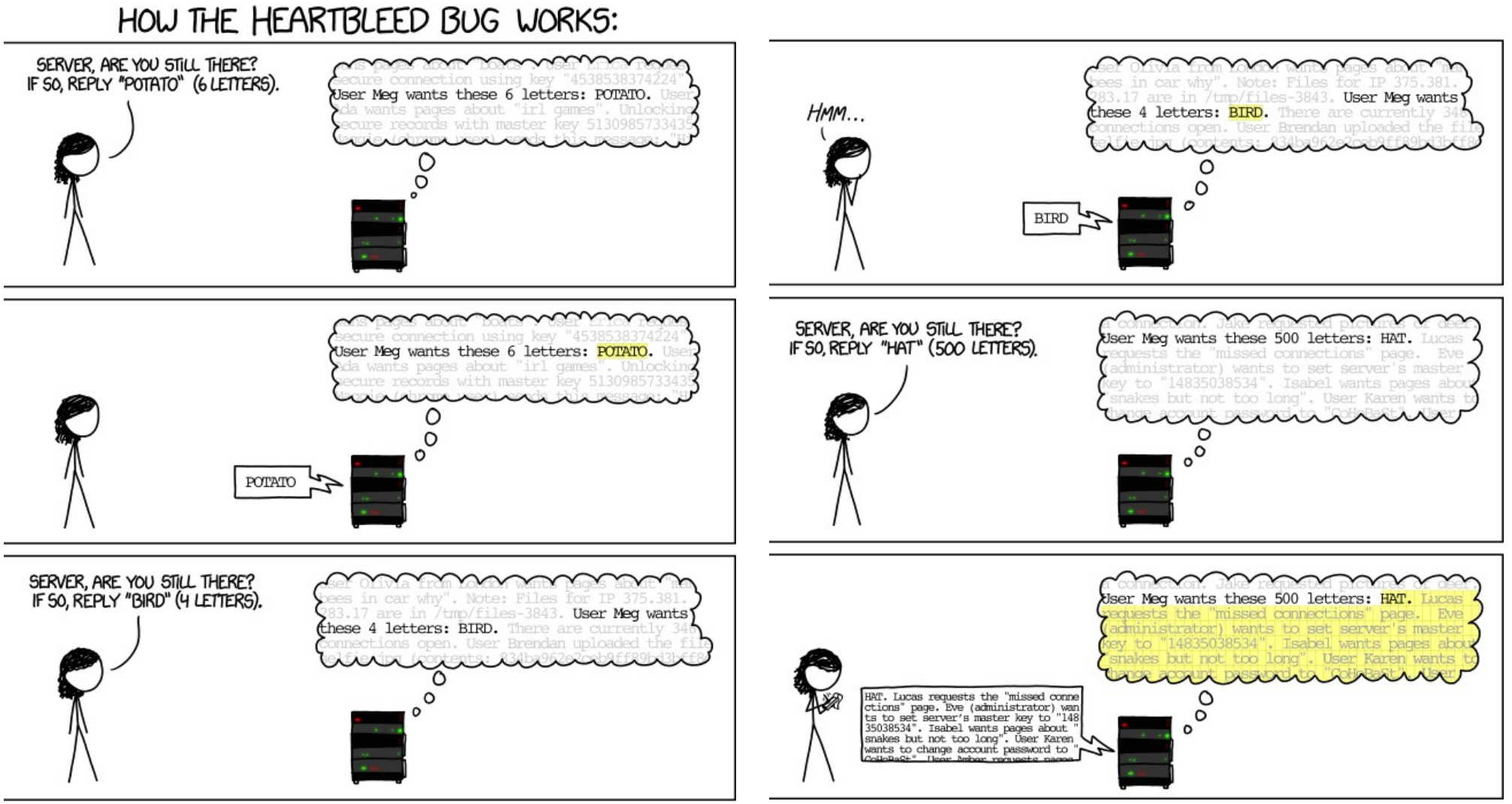
Heartbleed Bug

O bug Heartbleed

- Falha crítica do OpenSSL
  - Afeta: email, web, IM, VPNs, etc
- Divulgada no dia 07/Abr/2014
  - Presente no código do OpenSSL há +2 anos!
- Exploits amplamente disponíveis na web
- Falha de implementação na função heart beat

O problema (1/3)

- SSL/TLS Heartbeat => função de ping/pong



Fonte: http://xkcd.com/1354/

Como saber se está vulnerável?

- Verifique a versão do OpenSSL:

```
~$ openssl version -a
```

  - Versões de **1.0.1 até 1.0.1f** são afetadas

- Execute uma **varredura na sua rede**:

```
~$ nmap -p 443 --script ssl-heartbleed <target>
```

  - https://svn.nmap.org/nmap/scripts/ssl-heartbleed.nse

- Ferramentas de teste online:

  - https://www.ssllabs.com/ssltest/index.html
  - https://filippo.io/Heartbleed/

O problema (2/3)

- Serviços afetados: tudo que usa SSL/TLS via implementação do OpenSSL
  - Serviços https, smtp, imap, pop,vpn
  - Aplicações clientes, ex: wget, curl, git, Android
  - Sites*: Facebook, Yahoo!, Gmail, Instagram, Dropbox, Netflix, Youtube, etc

*Fonte: http://mashable.com/2014/04/09/heartbleed-bug-websites-affected/

O problema (3/3)

O quê é possível obter?

- 64 KB da memória do servidor (aleatoriamente)

  ou seja...

- Usuários / senhas
- Conteúdo de e-mails, documentos, etc
- Certificados digitais (chave privada!)
- Código de aplicações
- ...

Como saber se está vulnerável?

- Verifique a versão do OpenSSL:

```
~$ openssl version -a
```

  - Versões de **1.0.1 até 1.0.1f** são afetadas

- Execute uma **varredura na sua rede**:

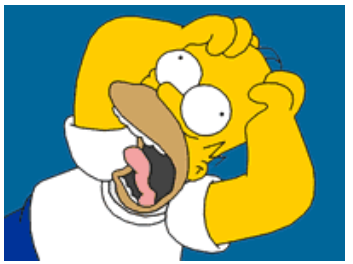
```
~$ nmap -p 443 --script ssl-heartbleed <target>
```

  - https://svn.nmap.org/nmap/scripts/ssl-heartbleed.nse

- Ferramentas de teste online:

  - https://www.ssllabs.com/ssltest/index.html
  - https://filippo.io/Heartbleed/

Estou vulnerável, o que fazer?



- **Atualizar o software** vulnerável
  - **Reiniciar** os daemons / aplicativos
- Monitorar o acesso a partir de origens suspeitas
  - Logs / correlação de eventos
  - Assinaturas IDS
- **Revogar os certificados**
- Solicitar **troca de senhas** dos usuários

Demonstração

SSL HeartBleed no PoP-BA/RNP

- O CAIS/RNP detectou diversos hosts vulneráveis no backbone acadêmico e tem **evidências de explorações**
- O CERT.Bahia identificou **14 hosts vulneráveis**, clientes da RNP / BA
  - Envio de notificações
  - Apoio na resolução do incidente
  - Testes de validação
- Produção de relatório executivo para **justificativa de troca de certificados**

Relatório executivo para troca de certificado SSL/TLS

	CERT.Bahia Modelo para Justificativa de aquisição de novo certificado SSL	
Descrição:	*Modelo para Justificativa de aquisição de novo certificado SSL*	
Autor(es):	*Equipe técnica do CERT.Bahia*	

Última atualização: terça-feira, 6 de maio de 2014

Modelo para Justificativa de aquisição de novo certificado SSL

Certificado SSL é o instrumento que possibilita oferecer um serviço através de conexão segura, assim provendo um caminho criptografado seguro entre o cliente e os serviços de internet, especialmente aqueles que realizam trânsito de informações sensíveis.

Os certificados que a **ORGANIZAÇÃO** possui são responsáveis pela segurança dos serviços que estão no seu domínio, conforme descrito abaixo:

- Certificado "coringa" ou *wildcard* (*.<DOMÍNIO-ORGANIZAÇÃO>) : Responsável pela segurança de todos os serviços que estão no nosso domínio (qualquer subdomínio direto). Por exemplo webmail.DOMINIO, smtp.DOMINIO, www.DOMINIO.

Relatório executivo para troca de certificado SSL/TLS

- Onde obter?
  - Na página do CERT.Bahia <http://certbahia.pop-ba.rnp.br/SecAlert2014001>

Como receber mais alertas?

- Alertas do CERT.Bahia:
  - <certbahia-alertas@listas.pop-ba.rnp.br>
- Alertas do CAIS/RNP:
  - http://www.rnp.br/cais/listas.php
- Encontros de Segurança Mensais do CERT.Bahia (novidade!)

Obrigado!!!
:-)

Perguntas?