

7º Fórum Brasileiro de CSIRTs

"Proposta de Implementação de Protocolo de Criptografia em Páginas Web de Órgãos do Governo "

setembro 2018

CTIR Gov

Alexandre Santos





Agenda

- AMBIENTAÇÃO
- TERMOS COMUNS
- IMPLEMENTAÇÃO
- MELHORES PRÁTICAS
- AMEAÇAS
- TESTES
- DESAFIOS

Ambientação

CTIR GOV: HISTÓRICO, SERVIÇOS E PARCERIAS



Responsabilidade Nacional

LOCATION INFORMATION
Brazil, CTIR Gov
Computer Security and Incident
Response Team - Brazilian Federal
Government

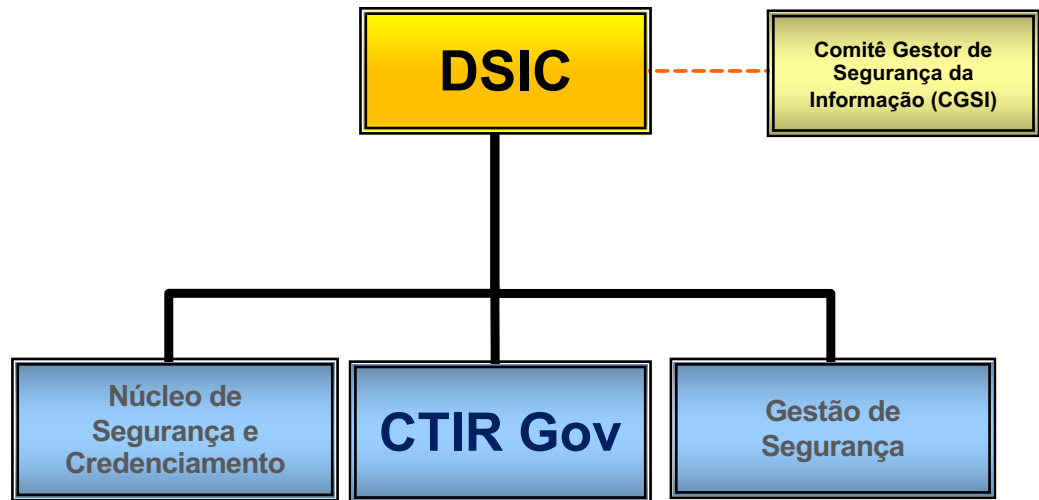
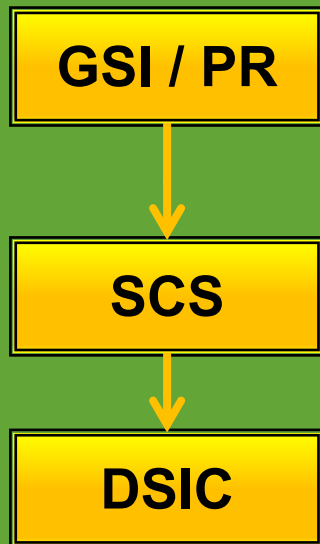
LOCATION INFORMATION
Brazil, CERT.br
Brazilian National Computer
Emergency Response Team



Coordenação Nacional

- O CTIR Gov atua como **Centro de Coordenação Nacional**, trabalhando de forma colaborativa e **não tem a intenção de concorrer com as ETIR** dos órgãos APF e dos Estados.
- Os órgãos e entidades da APF deverão **comunicar de imediato a ocorrência dos incidentes** de segurança nas redes de computadores ao CTIR Gov, com vistas a permitir que sejam dadas soluções integradas para a APF, bem como a geração de estatísticas (NC n° 05, 08 - DSIC/GSIPR).
- O CTIR Gov **não realiza** procedimentos de **investigação criminal**. Eventuais **desdobramentos** dos incidentes são **encaminhados às autoridades policiais competentes**. (NC n° 21 - DSIC/GSIPR).

Estrutura do CTIR Gov



Serviços



Tratamento de Incidentes

- Coordenação
- Notificação
- Suporte

Sensibilização

- Oficinas e Colóquios Técnicos
- Normas e Padrões
- Apresentações e Visitas

Análise de Tendências e Estatísticas

- Honeypots Distribuídos
- Sensores de Detecção
- Alertas e Estatísticas

The logo for the 2014 FIFA World Cup in Brazil. It features a stylized trophy shape composed of green and yellow segments, with a red '2014' and a green 'Brasil' integrated into the design. Below the logo, the text 'FIFA WORLD CUP' is in blue and 'Brasil' is in green. The entire logo is set against a white background with a green border.

- Rio+20 (2012)
- Copa das Confederações (2013)
- Jornada Mundial da Juventude (2013)
- Copa do Mundo FIFA (2014)
- Jogos Olímpicos RIO (2016)
- Guardião Cibernético



- OEA – Comitê Interamericano de Contraterrorismo
- FIRST – Nat CSIRTs
- FEBRABAN – GT Fraudes
- Fórum de CSIRTs do CERT.br
- Defesa – GT Inter Forças
- LACNIC – LAC CSIRT

Órgãos de Governo:

- das esferas Federal, Estadual e Municipal
- dos poderes Executivo, Judiciário e Legislativo

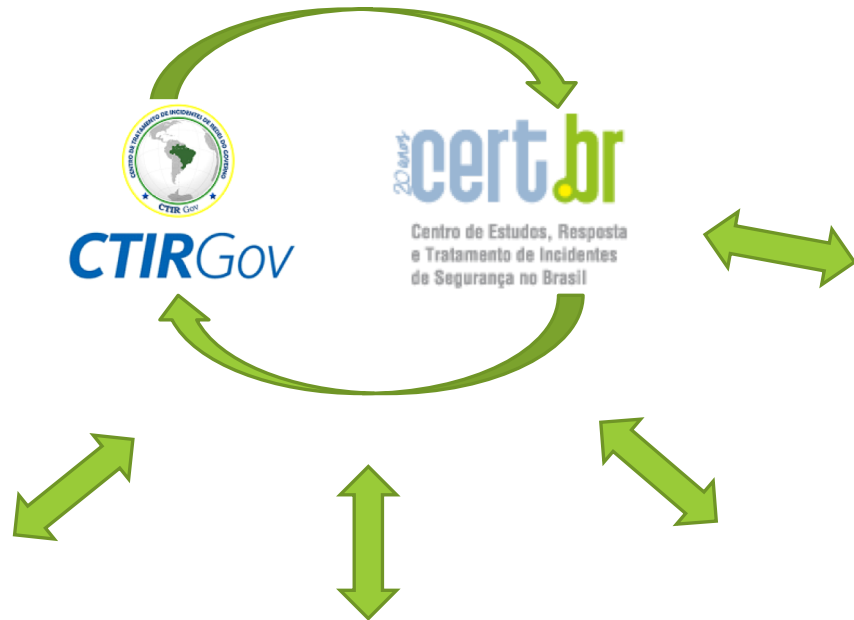
Principais Domínios

*.gov.br, *.mil.br, *.jus.br, *.leg.br, *.mp.br e *.def.br

29 pastas ministeriais,
Aproximadamente 6.000 entidades governamentais,
Aproximadamente 320 grandes redes do Governo Federal,



Parcerias





Brasil tem mais de 7,2 milhões de sites
desprotegidos



**Chrome marcará sites sem
criptografia como 'não seguros'**



**Certificados SSL dos sites de governo serão
atualizados**

Termos Comuns

DEFINIÇÕES E TERMOS COMUNS



CRIPTOGRAFIA

- A criptografia, é considerada como a ciência e a arte de escrever mensagens em forma cifrada ou em código. (Cartilha de Segurança para Internet – CERT.br).
- **CHAVE SIMÉTRICA:** Mesma chave criptográfica que cifra é utilizada para decifrar. Também chama de Criptografia de chave única (AES, Blowfish, RC4, 3DES e IDEA)
- **CHAVE ASSIMÉTRICA:** Uma chave é usada para **cifrar** (chave pública) e **outra pra decifrar** (chave privada). (RSA, DSA, ECC e Diffie-Hellman)



SSL

- O Secure Sockets Layer, ou SSL, foi desenvolvido **em meados da década de 1990 pela Netscape**, a empresa que fez o navegador mais popular na época. O SSL 1.0 nunca foi lançado ao público, pois possuía inúmeras vulnerabilidades, e o SSL 2.0 teve falhas graves. O **SSL 3.0**, lançado em 1996, foi completamente reformulado, e **preparou o cenário para o que se seguiu.**



TLS

- O Transport Layer Security - TLS tem a capacidade de trabalhar em portas diferentes e usa algoritmos de criptografia mais fortes como o keyed-Hashing for Message Authentication Code (HMAC) enquanto o SSL apenas Message Authentication Code (MAC).
- A versão do protocolo TLS foi lançada em 1999, foi padronizada pela Internet Engineering Task Force (IETF)



TLS

- Evolução do SSL e TLS
 - SSL V1 – 1994;
 - SSL V2 – 1995;
 - SSL V3 – 1996;
 - TLS 1.0 – 1999; RFC 2246 .
 - TLS 1.1 – 2006; RFC 4346 .
 - TLS 1.2 – 2008; RFC 5246 .
 - TLS 1.3 – em desenvolvimento.



HTTPS, SFTP, SSH

- Alguns protocolos foram especialmente modificados para suportar o SSL/TLS:
 - **HTTPS:** (Hyper Text Transfer Protocol Secure - protocolo de transferência de hipertexto seguro) É uma implementação do protocolo HTTP com uma camada adicional de segurança.
 - **SFTP** é uma extensão do FTP (File Transfer Protocol) usando SSL/TLS.
 - **SSH** (Secure Shell). Permite conexão a um computador remoto com segurança.



CERTIFICADO DIGITAL

- O certificado digital funciona como uma **identidade virtual que permite a identificação segura e inequívoca do autor de uma mensagem ou transação feita em meios eletrônicos.**
- Esse documento eletrônico **é gerado e assinado** por uma terceira parte confiável, ou seja, uma **Autoridade de Certificação - AC** que, **segundo regras estabelecidas pelo Comitê Gestor da ICP-Brasil**, associa uma entidade (pessoa, processo, servidor) a um par de chaves criptográficas.



AUTORIDADE DE CERTIFICAÇÃO

- Observa-se que o modelo adotado pelo Brasil foi o de certificação com raiz única, sendo que **o Instituto Nacional de Tecnologia da Informação - ITI**, além de desempenhar o papel de **Autoridade de Certificação Raiz – AC-Raiz**, também tem o papel de credenciar e descredenciar os demais participantes da cadeia, supervisionar e fazer auditoria dos processos.
- **A infra-estrutura de chaves públicas (PKI) do Brasil**, definida pela Medida Provisória Nº 2.200-2, de 24 de Agosto de 2001, **é uma cadeia hierárquica de confiança que viabiliza a emissão de certificados digitais para identificação virtual do cidadão.**



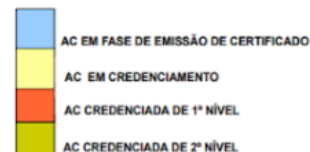
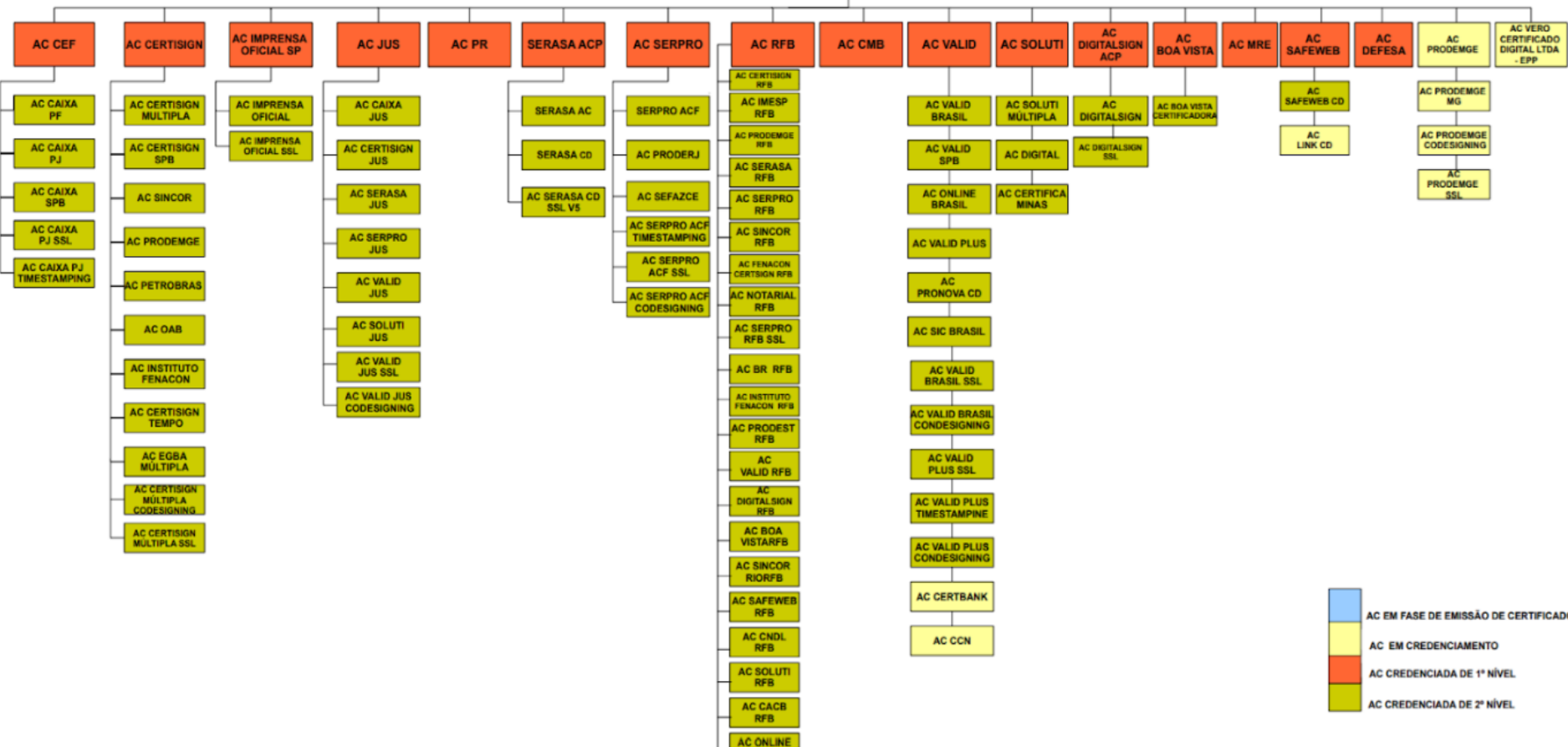
AUTORIDADE DE CERTIFICAÇÃO



Estrutura da ICP-Brasil

Atualizado: 12/07/2018

AC RAIZ



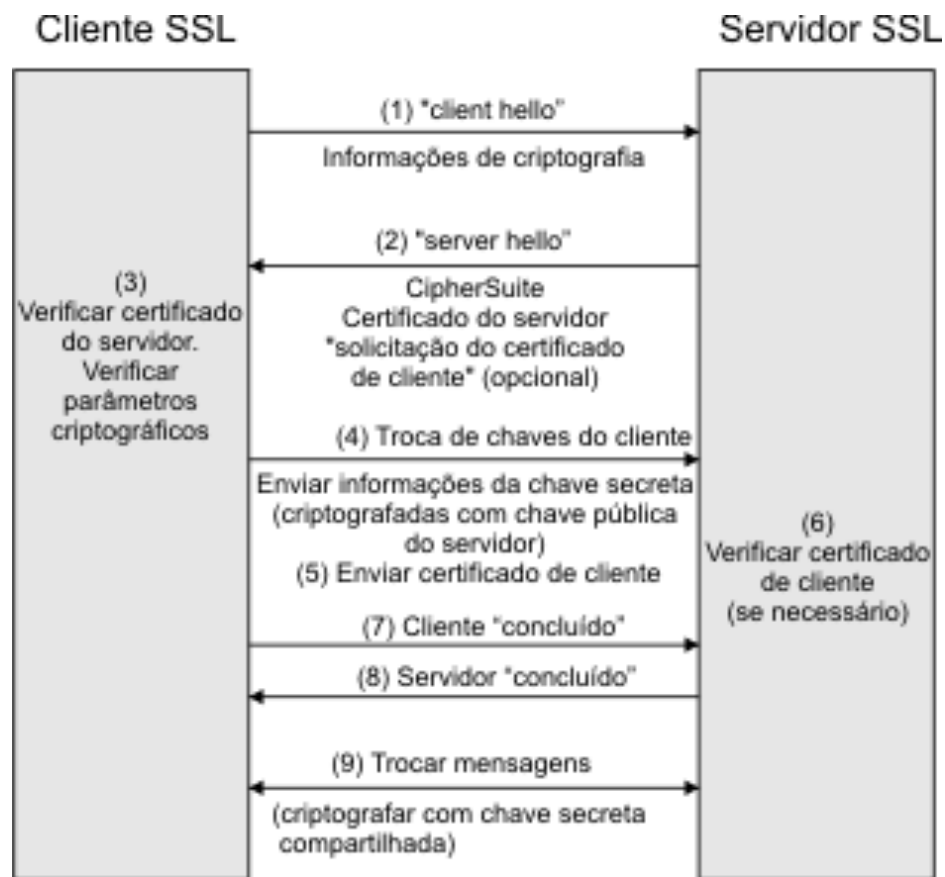


PROTOCOLO ACME

- ACME - Automatic Certificate Management Environment
- Em resumo, ele envolve vários pedidos (ou desafios) para o servidor web onde o certificado está presente. Com base nas respostas, a **Validação do Domínio** do inscrito é assegurada por uso de um par de chaves assimétricas. Existirá um cliente agente ACME configurado no servidor do domínio cadastrado que será consultado pelo servidor da autoridade certificadora (AC)
- O ACME permite que um cliente solicite ações de gerenciamento de certificado usando um conjunto de mensagens JavaScript Object Notation (JSON) transportadas por HTTPS. A emissão usando o ACME se assemelha ao processo de emissão de uma CA tradicional, em que um usuário cria uma conta, solicita um certificado e comprova o controle do (s) domínio (s) desse certificado para que a CA emita o certificado solicitado.



HTTPS handshake



Implementação

IMPLEMENTAÇÃO DE SSL/TLS EM PÁGINAS WEB –
OPENSSL - APACHE - FREEBSD





PROJETO WEB

- Reunião inicial
- Cronograma
- Análise Comparativa
- Planejamento
- Desenvolvimento
- Testes
- Publicação e Manutenção



SERVIDOR WEB

- JBOSS (Red Hat)
- IIS (Microsoft)
- Apache e Tomcat (Apache Software Foudantion)
- WebSphere (IBM)
- NGINX (Igor Sysoev)



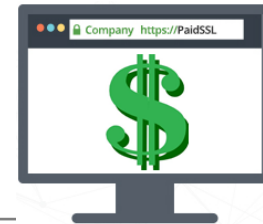
DOMÍNIOS/SUBDOMÍNIOS

- **Certificados Simples** - Protegem um subdomínio. O certificado **www.meudominio.gov.br** não serve para **mail.meudominio.gov.br**.
- **Certificados de subdomínios** - Um certificado para **www.meudominio.gov.br**, protegerá **mail.meudominio.gov.br** também.
- **Certificados de múltiplos domínios** - Para certificar duas aplicações **www.meudominio.gov.br** e **www.meudominio.com.br**, é possível utilizar um certificado para cada uma delas ou um único certificado de múltiplos domínios para todas as aplicações.



TIPOS DE CERTIFICADOS

- **Validação do Domínio** (Domain Validated - **DV**) - Utilizam a **Autoridade de Certificação apenas para verificar se o solicitante possui e administra um domínio** (ícone do cadeado será exibido na barra de endereços, mas nenhuma informação específica sobre o proprietário será exibida).
- **Validação da Organização** - (Organization Validated - **OV**) - **Exigem que a Autoridade de Certificação confirme que a atividade do solicitante esteja registrado e seja legítimo** (ícone do cadeado será exibido na barra de endereços e ao clicar neste cadeado, o nome da empresa será exibido).
- **Validação Estendida** (Extended Validation - **EV**) - **Exigem ainda mais evidências documentais sobre o solicitante**, para que a Autoridade de Certificação valide a organização (o ícone do cadeado será exibido na barra de endereços **juntamente com o nome da empresa** dentro da barra de endereços).



1º PASSO

Gerando o seu CSR (Certificate Signing Request)

Realizado pelo Administrador de Sistemas ou a equipe técnica do seu provedor.

2º PASSO

Comprando o seu Certificado

Compre seu certificado! Realizado pela área de compras da sua empresa.

3º PASSO

Validação da sua solicitação

Procedimentos obrigatórios realizados pela Autoridade de Certificação e passos que você precisará realizar para finalizar o processo de emissão do seu certificado digital com sucesso.

4º PASSO

Efetuando o pagamento

Feito pelo contato financeiro cadastrado no seu pedido. Pagamentos feito por boleto bancário enviado após a validação do seu pedido.

5º PASSO

Instalando o Certificado Digital no seu servidor

Realizado pelo Administrador de Sistemas ou a equipe técnica do seu provedor.



1º PASSO

Configurando o Servidor Web

Configure o Apache SSL no FreeBSD

2º PASSO

Instalando o Aplicativo

Instale o Lets'Encrypt no FreeBSD

(<https://www.sslforfree.com/>)

(<https://certbot.eff.org/>)

3º PASSO

Atualizando os Certificados

Atualize os Certificados Apache TLS no FreeBSD

Fonte: <https://www.tecmint.com/install-lets-encrypt-ssl-certificate-for-apache-on-freebsd/>



Let's Encrypt™



- Desenvolvido e mantido pelo Internet Security Research Group – ISRG, com sede na Califórnia. O projeto faz parte do Linux Foundation Collaborative Projects.
- Implementa o protocolo ACME com o objetivo de facilitar a configuração de um servidor HTTPS e a obtenção automática de um certificado SSL/TLS do navegador. Apesar de sua implementação ser mais simples, isto não prejudica a segurança. Os certificados emitidos baseiam-se nas melhores práticas de segurança e possuem chaves de criptografia de até 4096bits.



Fonte: <https://letsencrypt.org/how-it-works/>

Melhores Práticas

MELHORES PRÁTICAS NA IMPLEMENTAÇÃO DE
SSL/TLS



Chave Privada

- Crie chaves usando no mínimo RSA 2048 bits;
- Defina uma senha robusta;
- Quando for gerar a chave privada e a CSR (Certificate Signing Requests) utilize um computador confiável;
- Para o armazenamento das chaves privadas, utilize o HSM - Hardware Security Module. Um armazenamento das chaves em hardwares com módulos de criptografia.
- Utilize algoritmos fortes (hash SHA3)



Configure corretamente o servidor

- Utilize apenas o protocolo TLS e desabilite os protocolos SSL. A melhor opção seria apenas utilizar o TLS 1.2, porém devido a compatibilidade com navegadores antigos, você precisará deixar habilitado as versões 1.0 e 1.1.
- Apenas configure chaves que forneçam criptografia acima de 128 bits, incluindo a exclusão das chaves que utilizam Anonymous Diffie-Hellman (ADH), RC4 e 3DES.
- Desabilite a opção TLS Compression, que irá prevenir que seu servidor seja alvo de ataques.



Configure corretamente o servidor

- Habilite o HSTS (HTTP Strict Transport Security), pois irá permitir que seu site se torne acessível apenas através de HTTPS.
- Caso você não esteja utilizando o HSTS, cuidado com o conteúdo mixado entre HTTP e HTTPS, pois caso o cliente acesse uma área com HTTPS e este código chame um elemento que esteja chamando o protocolo HTTP, isso poderá gerar alertas de segurança.
- Mantenha o navegador WEB sempre atualizado e protegido contra vulnerabilidades.

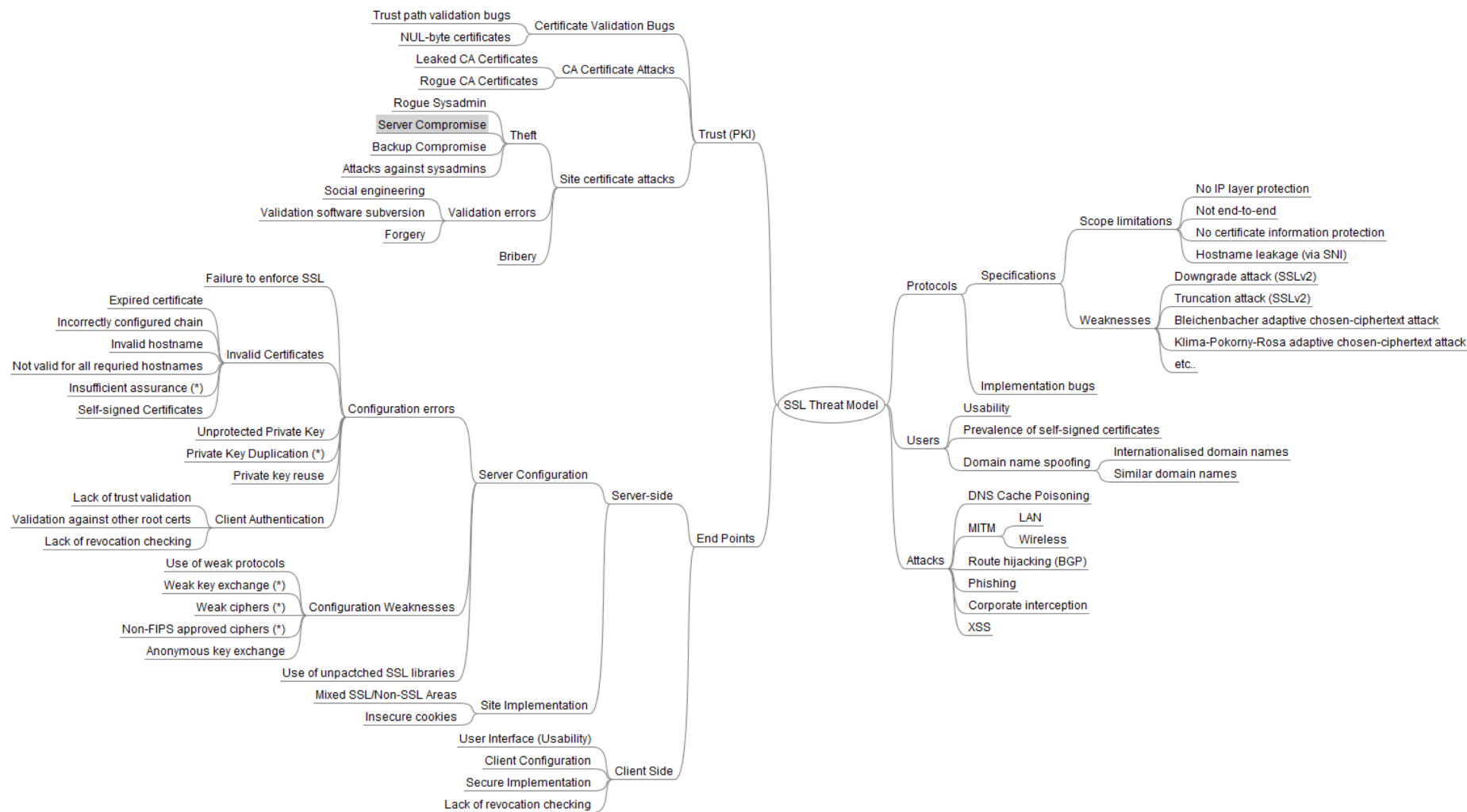
Ameaças

VULNERABILIDADES E ATAQUES A SSL/TLS/HTTPS

A solid green horizontal bar spanning the width of the slide at the bottom.



AMEAÇAS



Fonte: <https://www.ssllabs.com/projects/ssl-threat-model/index.html>



VULNERABILIDADES

- FREAK - "Factoring attack on RSA Export Keys".
- Essa falha permite que um invasor realize um ataque man-in-the-middle entre clientes e **servidores vulneráveis**, permitindo que ele espione e / ou injete códigos maliciosos em comunicações supostamente seguras.



VULNERABILIDADES

- POODLE (Padding Oracle On Downgraded Legacy Encryption).
- Tem por objetivo **forçar que a comunicação entre servidor e cliente seja criptografada através do SSLv3**, que possui brechas na sua implementação. Com isso, **o atacante consegue decifrar as mensagens** que trafegam do servidor para o cliente e vice-versa.



VULNERABILIDADES

- HEARTBLEED BUG.
- O HeartBleed é uma **falha na implementação** do OpenSSL, que permite ao atacante extrair informações trocadas entre o cliente e o servidor.
- **É importante ressaltar que essa falha não é no protocolo SSL/TLS, mas sim no OpenSSL.** As versões 1.0.0 e 0.9.8 não foram afetadas.



ATAQUES

- SSL Renegotiation Attack - Este se trata de um tipo de **vulnerabilidade** que ocorre justamente **no processo de renegociação dos protocolos SSL e TLS**, permitindo então que o invasor injete textos em todas as solicitações que o usuário realizar em uma conexão segura.



ATAQUES

DROWN (Decrypting RSA with Obsolete and Weakened eNcryption).

O ataque DROWN explora uma **falha no protocolo SSLv2**, afim de descriptar sessões no protocolo TLS. No caso em questão, nem o servidor nem o usuário precisam utilizar o SSLv2, o protocolo só precisa estar habilitado no servidor para que o atacante explore uma falha que o auxilia a descriptar o protocolo TLS.



ATAQUES

- Compression Ratio Info-Leak Mass Exploitation - conhecido como 'CRIME'. Este tipo de ataque possibilita que o invasor consiga **acesso aos conteúdos guardados em cookies** da Internet quando é utilizado TLS. Com este tipo de ataque é possível que o **invasor "sequestre" uma sessão web, conseguindo expor as informações** e comprometendo integridade do acesso do usuário.

Testes

POSSIVEIS TESTES NA IMPLEMENTAÇÃO

A solid green horizontal bar at the bottom of the slide.



SSL SERVER TEST



[Home](#) [Projects](#) [Qualys.com](#) [Contact](#)

You are here: [Home](#) > [Projects](#) > SSL Server Test

SSL Server Test

This free online service performs a deep analysis of the configuration of any SSL web server on the public Internet. **Please note that the information you submit here is used only to provide you the service. We don't use the domain names or the test results, and we never will.**

Hostname:

Submit

☐ Do not show the results on the boards

Recently Seen

[www.hypercache.pw](#)
[searx.ru](#)
[rco24.ru](#)
[www.webitech.co.uk](#)
[eldoom32.mamk.fi](#)

Recent Best

[yqs.ybzhao.com](#) A+
[api.wed-expert.com](#) A+
[www.idmobile.co.uk](#) A+
[www.playbor.com.br](#) A
[datanet.pl](#) A

Recent Worst

[westerfeld24.de](#) T
[www.e-rad.go.jp](#) F
[noz.de](#) T
[phoenix-dnr.ru](#) T
[webservices.waddell.com](#) F

Fonte: <https://www.ssllabs.com/ssltest/>



MOZILLA SSL CONFIGURATION GENERATOR

Mozilla SSL Configuration Generator

- ☒ Apache
- ☐ Nginx
- ☐ Lighttpd
- ☐ HAProxy
- ☐ AWS ELB

- ☐ Modern
- ☒ Intermediate
- ☐ Old

Server Version

OpenSSL Version

HSTS Enabled ☐

select your server version

select your server OpenSSL version

Which server is this for?

Oldest compatible browsers for this configuration.

apache 2.2.15 | intermediate profile | OpenSSL 1.0.1e
Compatible clients: Firefox 1, Chrome 1, IE 7, Opera 5, Safari 1, Windows XP IE8, Android 2.3

```
<VirtualHost *:443>
...
SSLEngine on
SSLCertificateFile      /path/to/signed_certificate
SSLCertificateChainFile /path/to/intermediate_certificate
SSLCertificateKeyFile   /path/to/private/key

# Uncomment the following directive when using client certificate authentication
#SSLCACertificateFile   /path/to/ca_certs_for_client_authentication

...
</VirtualHost>

# intermediate configuration, tweak to your needs
SSLProtocol              all -SSLv2 -SSLv3
SSLCipherSuite            ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-POLY1305:ECDHE-
```

Desafios

DESAFIOS E PROJETOS FUTUROS





Desafios

- Falta da cultura de Segurança da Informação
- Crescimento e Complexidade das Redes de Governo (computadores, celulares, *IoT*)



Projetos Futuros

- Guia de Boas Práticas
- Revisão de normas, padrões e processos
- Realização de Eventos



OBRIGADO!



<https://www.ctir.gov.br>

Alexandre Santos



INOC-DBA: 10954*810



ctir@ctir.gov.br

(notificação de incidentes)



Para comunicação através de um canal seguro, por favor utilize a seguinte chave PGP:

PGP Key ID: 0xAFBEDFCF

Fingerprint: 1E57 8A38 4834 6F1B 76BB 98C4 953E EB94 AFBE DFCF

PGP Public Key : www.ctir.gov.br/arquivos/certificados/ctir2009.asc



cgtir@presidencia.gov.br
(assuntos diversos)



www.linkedin.com/company/ctirgov/



@CtirGov