Resumo do artigo de Clark, 2013

**Siglas Importantes:**

CA: certificate authorities (autoridades de certificação)  
DV: domain validated (domínio validado)  
EV: extended validation (validação estendida)  
MITM: man-in-middle  
CRL: certificate revocation lists (listas de revogação de certificado)  
OCSP : online certificate status checking protocol (protocolo de verificação de status de certificado online)

**Cap 4: PROBLEMAS DE MODELO DE CONFIANÇA EM HTTPS**

**Certification -** Certificação

Um certificado da web vincula uma chave de assinatura pública a uma "identidade". A exatidão da vinculação é afirmada por meio de uma assinatura digital, por uma CA implicitamente que deve manter a precisão da vinculação ao longo do tempo.

O atributo essencial que todos os certificados de servidor HTTPS têm é um nome de domínio que o detentor do certificado controla. Se uma entidade solicitar um certificado para um nome de domínio, a CA normalmente desafia o solicitante a demonstrar controle sobre o domínio. Observe que isso pressupõe implicitamente que os nomes de domínio são mapeados para o servidor da web correto (endereço IP), um mapeamento realizado por meio do DNS. Esses certificados são chamados de certificados validados por domínio (DV).

Os certificados emitidos podem incluir informações adicionais verificadas pela CA, como nome da organização e endereço postal.

**Security Issues (Certification**) - Problemas de Segurança (Certificação)

Validação de nome de host (CAs): Os serviços de validação de domínio automatizados fornecidos por uma CA normalmente enviarão um e-mail de validação para um endereço de e-mail fixo associado ao domínio de nível superior do CN (por exemplo, admin @ domínio) ou um retirado do registro WhoIS do CN. Ambos os mecanismos dependem de informações de domínio precisas; assim, qualquer interrupção na capacidade do CA de receber registros DNS precisos pode resultar em um certificado emitido incorretamente.

Validação de nome de host (clientes): embora as plataformas de navegador atuais validem que um certificado de site recebido corresponde ao nome de host, alguns softwares que não sejam de navegador tiveram validação inadequada. CITA ALGUNS EXEMPLOS DE FALHAS OCORRIDAS.

Ataques de análise: Falhas relacionadas à análise permitem a emissão inadequada (análise incorreta de CA) e validação (análise incorreta do navegador) de certificados. Os pedidos de certificado contendo um caractere nulo (Ø) no CN podem ser mal interpretados.

Desclassificação de EV: Muitos dos problemas associados à validação de domínio automatizada são considerados frustrados por certificados EV. No entanto, um site que contém um certificado EV pode ser rebaixado para HTTPS normal por um ataque man-in-middle (MITM) com um certificado DV fraudulento.

**Anchoring Trust -** Ancorar confiança

Os fornecedores de software (por exemplo, Microsoft, Apple, Mozilla, Opera) configuram uma lista padrão de certificados de CA autoassinados em sistemas operacionais e / ou navegadores como âncoras de confiança. Cada site HTTPS cujo certificado de site o navegador aceita é, portanto, de fato confiável pelos usuários porque seu certificado foi garantido (direta ou indiretamente) por pelo menos uma das âncoras de confiança.

Em redes privadas, particularmente em ambientes corporativos, um certificado raiz para a organização pode ser configurado como uma âncora de confiança nas máquinas dos funcionários.

**Security Issues (Anchoring Trust) -** Problemas de segurança (Ancorar confiança)

Compromisso de CA: qualquer CA confiável pode emitir um certificado aceitável para navegador para qualquer site. Assim, um adversário pode visar a CA mais fraca para obter um certificado fraudulento e, assumindo que os clientes não notariam uma CA diferente, este certificado permite que o adversário evite a detecção em um ataque MITM.

Certificados obrigatórios: Também foram levantadas preocupações sobre a capacidade dos estados-nação de obrigar os certificados de uma CA aceita por navegador.

**Transitivity of Trust -** Transitividade de confiança

Dado que as âncoras de confiança podem emitir certificados CA intermediários, um certificado de site é aceitável para o navegador se o navegador puder construir uma cadeia de certificados que conduzam a uma âncora de confiança. Um estudo descobriu que 20% dos certificados válidos não exigiam nenhum intermediário e 38% usavam um.

**Security Issues (Transitivity of Trust) -** Problemas de segurança (transitividade de confiança)

Restrições básicas: a validação do caminho do certificado também deve verificar as restrições durante a validação, em particular se cada certificado CA intermediário tem CA: TRUE definido em basicConstraints. Se não estiver marcado, um certificado obtido para um servidor da web pode emitir certificados aceitáveis para navegador para qualquer outro site.

**Maintenance of Trust -** Manutenção da confiança

Outra função importante de uma CA é encerrar a validade de um certificado antes de sua data de expiração pré-configurada ao tomar conhecimento de certas circunstâncias. O status de revogação também deve estar disponível por meio da CA de emissão, ou seja, por listas de revogação de certificado (CRLs) ou respondentes do protocolo de verificação de status de certificado online (OCSP).

**Security Issues (Maintenance of Trust) -** Problemas de segurança (manutenção da confiança)

Revogação de bloqueio: Se um adversário conseguir obter um certificado fraudulento para um site que é posteriormente revogado, pode levar vários dias para que essa informação esteja disponível para os clientes, mesmo com OCSP, devido ao cache. Mesmo assim, os clientes podem não conseguir alcançar um respondente OCSP ou um ponto de distribuição de CRL.

**Indication and Interpretation of Trust** - Indicação e Interpretação de Confiança

Algumas proteções de segurança HTTPS dependem de um cuidado do usuário. Os usuários devem verificar o resultado de cada tentativa de conexão, normalmente indicada por uma dica visual na janela do navegador. Usuários mais cuidadosos podem verificar os detalhes do certificado. Por exemplo, que o nome do assunto - organização, endereço, país - corresponde às expectativas.

Dicas de segurança do navegador: os navegadores de desktop geralmente usam duas dicas principais para indicar que um site está sendo acessado por HTTPS:

(1) o URL na barra de endereço começa com **https: //**

(2) um ícone de cadeado é exibido em algum lugar no cromo do navegador, normalmente, clicar no ícone de cadeado exibirá informações sobre o certificado.

Avisos de segurança do navegador: os navegadores exibem avisos se uma conexão HTTPS falhar por determinados motivos. Um estudo foi feito em cima disso e se descobriu que a maioria das pessoas ignora os avisos dos navegadores.

Navegadores móveis: com o advento dos smartphones e tablets, os usuários também acessam sites HTTPS em navegadores móveis. Os navegadores móveis obedecem menos às diretrizes de interface do usuário HTTPS do que os navegadores de desktop, com menos suporte para exibir detalhes de certificado / conexão, distinguir certificados EV ou alertar os usuários sobre conteúdo misto.

**Security Issues (Indication and Interpretation of Trust)** - Problemas de segurança (indicação e interpretação de confiança)

Eliminando o TLS: devido à falta de atenção dos usuários aos indicadores e avisos de segurança HTTPS, um adversário MITM pode impedir o HTTPS de uma maneira tecnicamente detectável, mas improvável de ser notada.

Falsificação do Chrome do navegador: um aspecto importante dos indicadores de segurança é que eles são colocados no cromo do navegador, de modo que a sugestão exibida está sob o controle do navegador e não é influenciada pelo conteúdo da página da web exibida. Em um estudo, um site que implementou o último ataque foi classificado como legítimo por 63% dos usuários. Os navegadores de desktop de hoje normalmente forçam as janelas pop-up em novas guias, mantendo um cromo constante. Em muitos navegadores móveis, os sites podem posicionar a barra de endereço de forma que fique oculta, permitindo a falsificação de indicadores de segurança.