VOTANDO COM ASSINATURAS CEGAS
 (Voting with Blind Signatures)
Fonte: Applied Cryptography – Bruce Schneier
Cap. 6 – páginas 125-130

(1) Cada eleitor gera um conjuntos de mensagens, cada conjunto contendo um voto válido para cada resultado possível (por exemplo, se o voto é um sim ou não, cada conjunto contém dois votos, um para "Sim" e outro para "não"). Cada mensagem contém também um número de identificação gerado aleatoriamente, grande o suficiente para evitar duplicações com outros eleitores.

(2) Cada eleitor “cega” individualmente todas as mensagens (veja a Seção 5.3) e envia, com seus fatores de cegueira, ao CTF (Central de Apuração de Votos).

(3) O CTF verifica o seu banco de dados para garantir que o eleitor não apresentou seus votos “cegos”, assinados, anteriormente. CTF abre nove dos conjuntos para verificar se eles estão devidamente formados. Em seguida, CTF assina individualmente cada mensagem no conjunto. CTF envia-os de volta para o eleitor, armazenando o nome do eleitor em seu banco de dados.

(4) O eleitor “unblinds” (desfaz as assinaturas cegas das mensagens e fica com um conjunto de votos assinados pelo CTF. (Estes votos são assinados, mas não criptografados, para que o eleitor possa ver facilmente que voto é "sim" e que é "Não".)

(5) O eleitor escolhe um dos votos (ah!, a democracia) e criptografa com a chave pública do CTF.

(6) O eleitor envia seu voto ao CTF.

(7) A CTF decifra os votos, verifica as suas assinaturas e verifica o seu banco de dados para alguma duplicata da numeração de identificação, guarda o número de série e tabula os votos. Ela publica os resultados da eleição, juntamente com todos os números de série e seu voto associado.

COMENTANDO O PROTOCOLO

O eleitor malicioso, chamado de Mallory, não pode enganar o sistema. O protocolo garante assinatura se seus votos são únicos. Se Mallory tenta enviar o mesmo voto duas vezes, o CTF vai notar a duplicata número de série no passo (7) e jogar fora a segunda votação. Se ele tentar obter votos múltiplos assinados em passo (2), o CTF vai descobrir isso no passo (3). Mallory não pode gerar seus próprios votos, porque ele não sabe a chave privada do estabelecimento. Ele não pode interceptar e alterar votos de outras pessoas para a mesma razão.

O corte e a escolha do protocolo na etapa (3) é para garantir que os votos são únicos. Sem esse passo, Mallory poderia criar um conjunto de votos que são os mesmos, exceto para o número de identificação, e ter todos eles validados.

Um CTF malicioso não pode descobrir como as pessoas votaram. Uma vez que o protocolo de assinatura de ocultação impede a facilidade de ver os números de série dos votos, antes de serem lançados. A CTF não pode vincular o voto cego que ela assinou com o voto eventualmente lançado. A publicação de uma lista de números de série e seus votos associados permite aos eleitores confirmar em que o seu voto foi tabulados corretamente.

Existem ainda problemas. Se a etapa (6) não for anônima e a CTF puder registrar quem enviou num determinado voto, então a CTF pode descobrir quem votou em quem. No entanto, se receber votos em uma urna lacrada e, em seguida, tabulá-los mais tarde, ela não poderá. Além disso, enquanto a CTF pode não ser capaz de vincular votos a indivíduos, pode gerar um grande número de votos válidos, assinados, e fraudar submetendo aqueles votos a si própria. E se Alice descobre que o CTF mudou seu voto, ela não tem como provar isso. Um protocolo semelhante, que tenta corrigir esses problemas está em [1195, 1370] de Bruce Schneier.

------------------------------------------------------------------------------------------------------------------------------

VOTANDO COM DUAS CENTRAIS DE VOTAÇÃO
Fonte: Applied Cryptography – Bruce Schneier
Cap. 6 – páginas 125-130

Uma solução é dividir o CTF em dois. Nenhuma das partes teria o poder de enganar por conta própria.

O protocolo a seguir usa uma Agência Legitimação Central (CLA) para certificar os eleitores e um CTF separado, para contar votos [1373].

(1) Cada votante envia uma mensagem para o CLA pedindo um número de validação.

(2) O CLA ​​envia Ao eleitor, de volta, um número de validação aleatória. O CLA ​​mantém uma lista de números de validação. O CLA ​​também mantém uma lista de destinatários Dos números de validação, no caso alguém tentar votar duas vezes.

(3) O CLA ​​envia a lista de números de validação para o CTF.

(4) Cada eleitor escolhe um número de identificação (validação) aleatória. Ele gera uma mensagem com esse número, o número de validação que recebeu do CLA, e seu voto. Ele envia esta mensagem ao CTF.

(5) A CTF verifica o número de validação contra a lista que recebeu do CLA na etapa (3). Se o número de validação está lá, o CTF marca ele para evitar que alguém de vote duas vezes).
A CTF adiciona o número de identificação para a lista de pessoas que votaram para um determinado candidato e adiciona-o para registrar a contagem.

(6) Depois de todos os votos terem sido recebidos, a CVA publica o resultado, assim como as listas de números de identificação e os candidatos foram votados.

COMENTANDO O PROTOCOLO

Como o protocolo anterior, cada eleitor pode olhar para as listas de números de identificação e encontrar o seu, se possuir. Isto dá-lhe a prova de que o seu voto foi computado. Naturalmente, todas as mensagens que passam entre as partes do protocolo devem ser criptografadas e assinadas para impedir que alguém se passar por alguém ou interceptar transmissões.

A CTF não pode modificar votos porque cada eleitor vai verificar seu número de identificação. Se um eleitor não encontra sua seu número de identificação, ou encontra sua identificação em um registro diferente do que ele tenha votado, ele vai saber imediatamente se houve jogo sujo. A CTF não pode encher a urna porque ele está sendo vigiada pela CLA. O CLA ​​sabe quantos eleitores foram certificados e seus números de validação, e irá detectar qualquer modificação.

Mallory, que não é um eleitor, pode tentar enganar, por adivinhar um número de identificação válido. Este risco pode ser minimizado, tornando o número de possíveis números de identificação possíveis, muito maiores do que o número de os números de validação reais: números de 100 dígitos para um milhão de eleitores, por exemplo. Claro, os números de validação devem ser gerados aleatoriamente.

Apesar disso, o CLA ainda é uma autoridade confiável em alguns aspectos. Pode certificar eleitores inelegíveis. Pode certificar eleitores várias vezes. Este risco pode ser minimizado por ter o CLA publicar um lista de eleitores certificados (mas, não seus números de validação). Se o número de eleitores nessa lista é menos do que o número de votos tabulados, então algo está errado. No entanto, se mais eleitores foram certificados de votos tabulados, isso provavelmente significa que algumas pessoas certificadas não se incomodou de votação. Muitas pessoas que estão registrados para votar, não se preocuparam em votar.

Este protocolo é vulnerável ao “conluio” entre o CLA e o CTF. Se os dois podem correlacionar suas bases de dados e descobrir quem votou em quem.