Análise de Vulnerabilidade de Esquemas de Segredo Compartilhado Considerando um novo Modelo de Ameaça

Rick Lopes de Souza, Martin Vigil, Ricardo Felipe Custódio

[1]Universidade Federal de Santa Catarina (UFSC)
Florianópolis – SC – Brazil

Abstract. *Secret sharing schemes are cryptographic primitives used to distribute parts of a secret among a set of participants in such a way that only an authorized subset can rebuild the secret. Traditionally, most secret sharing schemes work with only two entity definitions: The Dealer and Participants. For these schemes, several threat models have been proposed considering only these two entities. However, in the literature it is not clear who should play the role of rebuilding the secret and who would be the keeper of the secret. These two new entities modify the existing threat models that consider: (i) the distributor initializes the system and splits and shares the secret, and (ii) the participants cooperate or not with the secret reconstruction. In this work we propose a new threat model considering the new entities that represent the roles involved in shared secret schemes. Considering this new model, we show that some of the best-known schemes are vulnerable. We make evaluations checking which points can be safely maintained and at which points vulnerabilities will emerge according to the new entities and new threat model.*

Resumo. *Esquemas de segredo compartilhado são primitivas criptográficas utilizadas para distribuir partes de um segredo entre um conjunto de participantes de tal forma que apenas um subconjunto autorizado consiga reconstruir o segredo. Tradicionalmente, grande parte dos esquemas de segredo compartilhado trabalham com apenas duas definições de entidades: Distribuidor e Participante. Para esses esquemas, diversos modelos de ameaça foram propostos considerando apenas essas duas entidades. Todavia, na literatura não está claro quem deveria exercer o papel de reconstruir o segredo e quem seria o detentor do segredo. Essas duas novas entidades modificam os modelos de ameaça existentes que consideram o Distribuidor a entidade responsável por inicializar o esquema, gerar parâmetros do sistema, gerar o segredo, criar as partes e distribuir, e Participantes que cooperam ou não com a reconstrução do segredo. Neste trabalho propomos um novo modelo de ameaça considerando as novas entidades que representam todos os papéis envolvidos em esquemas de segredo compartilhado. À luz desse novo modelo, alguns dos esquemas mais conhecidos mostram-se vulneráveis. Também são feitas avaliações verificando quais pontos consegue-se manter segurança e em quais pontos surgirão vulnerabilidades de acordo com as novas entidades e modelos de ameaça definidos.*

1. Introdução

Um esquema de segredo compartilhado é um método para distribuir um segredo para um conjunto de participantes dando para cada um apenas uma parte, de tal forma que

apenas um conjunto específico de participantes possa reconstruir o segredo reunindo as partes. Esquemas de segredo compartilhado são considerados serviços básicos em diversos protocolos criptográficos. Podem ser utilizados para procedimentos de autenticação, replicação de arquivos, contingência de dados sensíveis e computação distribuída.

Esses esquemas envolvem diferentes entidades que possuem funcionalidades específicas dependendo do uso. A literatura normalmente considera apenas duas entidades: Distribuidor e Participantes. O Distribuidor tem a responsabilidade de receber um segredo, quebrar em partes e distribuir de forma segura para um conjunto de Participantes. Os Participantes devem guardar de forma segura e seguir os protocolos honestamente para fornecer e reconstruir o segredo.

Partindo das entidades definidas anteriormente, os esquemas de segredo compartilhado clássicos como o de Shamir [Shamir 1979] consideram um modelo de ameaça tradicional, onde o Distribuidor é uma entidade confiável, que gera os parâmetros, o segredo e distribuir de forma segura para os Participantes. Os Participantes comportam-se de maneira polarizada. Ou seja, ou são completamente honestos (participam da reconstrução do segredo de forma correta) ou são maliciosos (não participam na reconstrução do segredo, atrapalhando o protocolo).

O modelo de ameaça mencionado anteriormente apresenta algumas premissas razoáveis para algumas situações, entretanto, não necessariamente reflete os diferentes cenários de aplicações existentes. Por isso, diversos outros trabalhos foram propostos descrevendo novos modelos de ameaças e novos esquemas de segredo compartilhado para garantir a segurança com essas variações.

Problema: Mesmo com diversos trabalhos propostos na literatura variando os modelos de ameaça, encontra-se uma limitação na definição das entidades. Refere-se na grande maioria que o Distribuidor é quem gera o segredo e os parâmetros, fazendo com que seja uma entidade parcialmente confiável. Mas sabe-se que esse nem sempre é o cenário encontrado nas aplicações, onde existe um Detentor do Segredo que deseja compartilhar um determinado segredo com mais participantes utilizando o protocolo de esquema compartilhado sem necessariamente confiar no Distribuidor. Além disso, em grande parte da literatura não se encontra de forma clara qual entidade deve ser responsável pela reconstrução do segredo.

Motivação: A confiabilidade de esquemas de segredo compartilhado dependem dos procedimentos de segurança que utilizam. Logo a avaliação dos modelos de ameaça nos protocolos de segredo compartilhado que são utilizados para os mais diversos motivos são essenciais. A literatura não comenta de forma mais específica sobre qual entidade deve ser responsável por reconstruir o segredo, assim como não comenta sobre qual entidade deveria gerar o segredo além do Distribuidor. A criação de definição de novas entidades muda alguns modelos de ameaça, fazendo com que alguns dos principais esquemas existentes possam não ser mais confiáveis em determinadas situações. Dessa forma, faz-se necessário uma avaliação desses esquemas em um novo modelo de ameaça para verificar se estariam seguros ou não.

A partir do problema e da motivação, conclui-se que é necessário um estudo nos esquemas de segredo compartilhado para avaliar qual seria o impacto da criação de uma novo modelo de ameaça baseado na criação de novas entidades.

Contribuição: Este artigo tem como principais contribuições:

1. Criação de uma nova entidade para os modelos de ameaça
2. Criação de um novo modelo de ameaça com a nova entidade
3. Avaliação do impacto nos protocolos de segredo compartilhado com base no novo modelo de ameaça
4. Possíveis correções e medidas de controle para os problemas encontrados a partir da avaliação feita

Este artigo está organizado da seguinte forma: primeiro alguns dos esquemas tradicionais de segredo compartilhado são introduzidos, depois as princpais entidades dos esquemas de segredo compartilhado são detalhadas. A partir disso, define-se o modelo de ameaça tradicional, assim como os modelos de ameaça não tradicionais. Como parte das contribuições do artigo, um novo modelo de ameaça é definido e avaliado. Ao final do trabalho estão as considerações finais.

2. Esquemas tradicionais de Segredo Compartilhado

Esquemas de segredo compartilhado são considerados serviços básicos em determinados protocolos criptográficos. Podem ser utilizados para procedimentos de autenticação, replicação de arquivos, contingência de dados sensíveis e etc.

Esses esquemas normalmente definem duas entidades: Distribuidor e Participantes. Os Distribuidores tem como principal função a geração dos parâmetros, quebrar o segredo em partes e distribuí-los para os Participantes. Os Participantes então devem guardar em segurança e cooperar no momento da reconstrução.

Os Participantes fazem parte de um conjunto chamado Estrutura de Acesso do esquema de segredo compartilhado. Beimel [Beimel 2011] provê uma definição formal das Estruturas de Acesso:

Definição 2.1 (Estrutura de Acesso)**.** Seja $P = \{p_1, \ldots, p_n\}$ um conjunto de participantes. Uma coleção $\mathcal{A} \subseteq 2^{\{p_1,\ldots,p_n\}}$ é monotônica se $B \in \mathcal{A}$ e $B \subseteq C$ implica que $C \in \mathcal{A}$. Uma estrutura de acesso é uma coleção monotônica $\mathcal{A} \subseteq 2^{\{p_1,\ldots,p_n\}}$ de subconjuntos não vazios de $\{p_1, \ldots, p_n\}$. Conjuntos pertencentes a $\mathcal{A}$ são chamados autorizados e conjuntos não pertencentes a $\mathcal{A}$ são chamados não autorizados.

As duas principais propriedades de um esquema de segredo compartilhado podem ser definidas da seguinte forma. Seja P um conjunto de participantes, seja $\mathcal{A}$ a estrutura de acesso monotônica em P, seja K o conjunto de possíveis segredos. Dessa forma, os esquemas devem possuir as duas seguintes propriedades:

1. **Corretude**. Qualquer subconjunto autorizado consegue reconstruir o segredo.
2. **Privacidade Perfeita**. Qualquer subconjunto não autorizado não consegue obter nenhuma informação a respeito do segredo.

Existem diferentes construções de esquemas de segredo compartilhado ([Beimel 2011] para um survey). Um dos mais importantes esquemas já propostos é o de Shamir [Shamir 1979] descrito a seguir.

O esquema clássico de Shamir possui as propriedades de Corretude e Privacidade Perfeita como estabelecida na definição (referenciar definição). O esquema estabelece

dois parâmetros t e n, tal que $t, n \in \mathbb{Z}$, onde $0 < t \leq n$. O segredo $k \in \mathbb{Z}_p$, onde $\mathbb{Z}_p$ é um anel com p primo, é dividido em n partes de tal forma que ao menos t é possível reconstruir o segredo. O esquema é baseado em interpolação de polinômios, onde dado t diferentes pontos $(x_1, y_1), \ldots, (x_t, y_t)$, existe apenas um único polinômio $Q(x)$ de grau $t-1$ onde $Q(0) = k$.

O esquema funciona como descrito a seguir. Dados t, n e um segredo $k \in \mathbb{Z}_p$, a entidade chamada Distribuidor precisa escolher um polinômio $Q(x) = a_0 + a_1 x + ... + a_{t-1}x^{t-1}$ tal que $a_0 = k$ e $a_1, \ldots, a_{t-1} \in \mathbb{Z}_p$ são coeficientes escolhidos de forma aleatória utilizando uma distribuição uniforme.

As partes são compostas por (x_i, y_i), para $i = (1, 2, \ldots, n)$, onde x_i é gerado aleatoriamente e cada avaliação $y_i = Q(x_i)$ é calculada. Após esta etapa, diferentes partes são distribuídas para cada Participante. Recebendo quaisquer t ou mais partes, o Reconstrutor pode encontrar o polinômio $Q(x)$ por meio de interpolação e então recuperar o segredo com a operação $k = Q(0)$.

3. Entidades

O esquema de segredo compartilhado depende de algumas entidades para funcionar de maneira correta. Isto significa que cada entidade deve ter suas funções corretamente definidas, assim como suas limitações. Não se encontra na literatura definições muito concretas sobre cada entidade, assim como suas limitações. Na grande maioria dos casos nota-se falta de informação sobre a entidade que gera o segredo e a entidade que reconstrói o segredo. Abordaremos aqui todas as possíveis entidades envolvidas em um esquema de segredo compartilhado.

1. **Detentor do Segredo:** O Detentor do Segredo é uma entidade que gera o segredo e tem como principal função gerar um segredo de forma aleatória e segura. Após essa geração, deve-se repassar o mesmo para que uma outra entidade possa quebrar e compartilhar com outras entidades. Partimos da premissa que o Detentor do Segredo deve ser sempre confiável, pois ele é o Detentor do Segredo que quer compartilhando utilizando algum esquema de compartilhamento.
   Opcionais:
   (a) *Quebrar o segredo e distribuir:* O Detentor do Segredo pode também ser um Distribuidor (que será apresentado a seguir). Esta entidade irá quebrar o segredo e compartilhar com os participantes de forma segura.
   (b) *Confiável:* O Detentor do Segredo é confiável. Ou seja, o mesmo sempre gerará o segredo de uma forma aleatória seguindo alguma distribuição uniforme e entregará ao Distribuidor utilizando um canal de comunicação seguro.
2. **Distribuidor:** O Distribuidor é uma entidade que tem como principal função receber o segredo de um participante ou uma terceira parte, quebrá-lo e distribuí-lo para os participantes por meio de um canal seguro. **Opcionais:**
   (a) *Gerar o segredo* - Dado um conjunto de possíveis segredos K, irá sortear de forma aleatória um segredo $k \in K$.
   (b) *Gerar os parâmetros do sistema* - Em determinados tipos de esquemas de segredo compartilhado, deve-se gerar os parâmetros para o compartilhamento. Entre eles:

- Tamanho total do grupo
- Tamanho do limiar
- Quantidade de níveis do esquema

(c) *Confiável:* O Distribuidor é completamente honesto. Ou seja, não pode ser corrompido por ninguém e seguirá corretamente os protocolos e regras.

(d) *Malicioso:* Esta entidade irá se comportar de forma maliciosa. Ou seja, irá gerar partes falsas que não deixarão recuperar o segredo. Poderá também manipular a geração de partes tal que menos participantes consigam recuperar o segredo. O Distribuidor irá se comportar como mencionado na definição 2 com os opcionais 1 e 2.

3. **Participante:** Um participante é um membro que pertence a uma estrutura de acesso do esquema de segredo compartilhado. Este membro recebe uma parte do segredo e tem como principal função guardá-lo de forma segura. Deve também seguir os protocolos de maneira honesta na reconstrução do segredo.
   Opcionais:
   (a) *Agir como um Distribuidor* - Agindo como um Distribuidor, o participante pode receber o segredo de uma terceira entidade ou gerá-lo sozinho. O participante então quebra esse segredo e distribui para os outros participantes.
   (b) *Agir como um Reconstrutor* - O participante consegue receber um conjunto de partes dos participantes para reconstruir o segredo.
   (c) *Confiável:* Os participantes irão executar os protocolos de maneira correta. Ou seja, recebem suas partes, mantém em segurança e participam do processo de reconstrução quando necessário.
   (d) *Malicioso:* O participante pode ser comprometido por um adversário e tentará subverter o protocolo.
4. **Reconstrutor:** Um reconstrutor tem como principal função receber as partes dos participantes e reconstruir o segredo. Este segredo será então utilizado para o seu propósito final.
   Opcionais:
   (a) *O Reconstrutor é também um Distribuidor* - Em determinadas situações necessita-se que exista apenas uma entidade que distribua e receba as partes. Neste caso, centraliza-se a segurança do esquema em apenas uma entidade que possui dois papéis.
   (b) *O Reconstrutor é também um Participante* - Existem casos onde é necessário que um dos participantes assuma o papel de reconstrutor. Ou seja, todos as partes serão reveladas para esta entidade reconstruir o segredo.
   (c) *O reconstrutor é uma terceira parte* - Uma terceira parte, que não é o Distribuidor ou Participantes, pode agir como um reconstrutor para receber as partes e reconstruir o segredo.
   (d) *Confiável:* O Reconstrutor é confiável e recebe todos as partes necessárias para reconstruir o segredo. Após a reconstrução, o reconstrutor deve encaminhar o segredo para a entidade Detentor do Segredo e destruir o segredo reconstruído localmente.
   (e) *Malicioso:* O reconstrutor é malicioso e pode querer corromper o esquema enviando o segredo recuperado para um adversário.

5. **Adversário:** Um adversário tem como principal objetivo obter informação a respeito do segredo. Ou seja, esta entidade quer de alguma forma atrapalhar o protocolo estabelecido para ganhar acesso ao segredo. Isto pode ser feito de diversas formas, dependendo do tipo de papel que o adversário tem no esquema.
   Opcionais:
   (a) *O adversário é o Distribuidor - Um Distribuidor malicioso pode ser o adversário do esquema. Tal entidade pode gerar parâmetros errados, assim como partes incorretas ou inserir dados suspeitos na criação dos esquemas. Caso tais informações não sejam geradas seguindo de forma correta os protocolos, o esquema pode ser comprometido.*
   (b) *O adversário é um Participante* - Um participante pode ser um adversário para o esquema. Tal participante pode ter sido comprado por uma entidade externa ao esquema e tentar prejudicar a recuperação do segredo. Assim como pode também tentar descobrir o segredo sem a autorização do resto do grupo.
   (c) *O adversário é uma Terceira Parte* - Uma terceira parte é uma entidade que não faz parte do esquema ou da estrutura de acesso, mas pode tentar obter alguma informação sobre as partes ou do segredo.
   (d) *Passivo:* Um adversário pode capturar as partes, entretanto, o protocolo é executado de forma correta e as partes não são corrompidas.
   (e) *Ativo:* Pode tomar a forma de um participante e submeter uma parte falsa durante o processo de reconstrução. Isso previne os participantes de conseguir reconstruir o segredo correto.

4. Modelo de Ameaça Tradicional

Para melhor entender os esquemas, precisa-se primeiramente especificar o modelo de ameaça tradicional. Após essa especificação, pode-se então especificar os modelos de ameaça diferentes e que não estão bem documentados na literatura.

O modelo de ameaça tradicional é o esquema em que todas as entidades se comportam de maneira honesta [Martin 2008]. Ou seja, todos irão gerar seus dados de forma aleatória utilizando uma distribuição uniforme e vão seguir os protocolos de maneira correta. Existem adversários que vão tentar obter as partes buscando por falhas de segurança nas comunicações ou vão tentar comprometer algum participante para subverter o protocolo. O Distribuidor se comporta de forma honesta, gera os parâmetros, segredo e distribui as partes para os Participantes. Os Participantes se comportam de maneira polarizada. Ou seja, recebem as partes, guardam de maneira segura e participam ou não no processo de reconstrução. O Reconstrutor não é bem definido pelo modelo, ficando aberto se um dos participantes poderia assumir esse papel ou uma terceira parte confiável. A tabela 1 ilustra a relação do modelo de ameaça tradicional com as entidades envolvidas.

Tabela 1. Modelo de Ameaça Tradicional

	Confiável	**Malicioso**	**Passivo**	**Ativo**
Distribuidor	✓			
Participante	✓			
Reconstrutor	✓			
Adversário			✓	

Os esquemas tradicionais de Shamir [Shamir 1979] e Blakley [Blakley 1979] suportam esse modelo de ameaça e conseguem garantir segurança nos protocolos. Ambos protocolos definem como premissas que as entidades são confiáveis e que todo o protocolo funcionará de maneira correta, sem interferências.

5. Modelos de Ameaça Não Tradicionais

Sabemos que o modelo de ameaça tradicional não é sempre possível devido às diferentes circunstâncias de uso dos esquemas de segredo compartilhado. Nem sempre é possível garantir total segurança em todas as etapas em cenários reais. Um dos primeiros ataques publicados na literatura, um adversário passa a ter um comportamento ativo para explorar o modelo de ameaça tradicional do esquema de Shamir [Tompa and Woll 1989]. Esse ataque explora a ação de um adversário tomar a forma de um Participante que maliciosamente submete partes falsas no processo de reconstrução do segredo. Após a mudança no modelo de ameaça, algumas perguntas surgem e que precisam ser respondidas:

1. Quem reconstrói o segredo?
2. As partes são reveladas durante o processo de reconstrução?
3. Os adversários são estáticos ou dinâmicos?
4. Quais são os objetivos dos adversários?

Portanto, necessita-se descrever diferentes modelos de ameaça para se adequar aos novos cenários de uso e tentar responder essas perguntas. Descreve-se a seguir os modelos de ameaças alternativos encontrados na literatura.

5.1. Modelo de Ameaça Alternativo 1 - Distribuidor Malicioso

Este modelo considera que os Participantes são honestos (que vão seguir os protocolos de maneira correta) e que o Distribuidor é malicioso de forma limitada. Definimos aqui que existe algum tipo de acordo entre o Distribuidor malicioso e um adversário externo. Devemos ressaltar que o Distribuidor não é uma entidade ”toda poderosa”, onde poderia fazer qualquer coisa. Existem limites que precisamos definir. O Distribuidor malicioso gerará os parâmetros, sorteará um segredo e o enviará as partes para os Participantes. Entretanto, o Distribuidor malicioso terá como um dos principais objetivos prejudicar a reconstrução do segredo distribuindo de forma proposital partes que não pertencem ao esquema. Outra ameaça do Distribuidor é tentar de alguma forma alterar a geração do polinômio, não sendo completamente aleatório como os protocolos tradicionais recomendam. Esses detalhes podem comprometer o segredo no momento da reconstrução, inviabilizando a obtenção correta do parte ou fazendo com que determinados pontos possam ser favorecidos. Os Participantes receberão as partes, guardarão de forma segura e irão participar de forma honesta na reconstrução do segredo enviando de forma segura as partes para o Reconstrutor. Não fica claro quem deve assumir o papel do Reconstrutor, mas o mesmo irá reunir as partes para finalmente reconstruir o segredo. Caso o Reconstrutor seja uma terceira parte, as partes do segredo não são reveladas, caso seja um dos participantes, as partes são reveladas, o segredo é reconstruído, utilizado e então as partes devem ser descartadas. A tabela 2 ilustra a relação do modelo de ameaça alternativo 1 com as entidades.

Tabela 2. Modelo de Ameaça 1 - Distribuidor Malicioso

	Confiável	Malicioso	Passivo	Ativo
Distribuidor		✓		
Participante	✓			
Reconstrutor	✓			
Adversário				✓

5.1.1. Esquemas Seguros para este Modelo

Os esquemas de segredo compartilhado verificáveis (SCV) de Pedersen [Pedersen et al. 1991] e Feldman [Feldman 1987], que são baseados no esquema de Shamir e criptografia homomórfica, são protocolos que conseguem manter segurança nesse tipo de modelo de ameaça. Esses protocolos necessitam de um algoritmo chamado "Verificar"que permite aos Participantes verificar a validade de suas partes (antes de tentar qualquer reconstrução). Ao final do algoritmo, cada participante decide se aceita ou rejeita sua parte. O algoritmo precisa verificar: Consistência: um subgrupo autorizado de participantes que aceita suas partes poderá reconstruir o segredo k. Corretude: Se o Distribuidor for honesto, então o valor k de segredo é genuíno.

5.2. Modelo de Ameaça Alternativo 2 - Participante Malicioso

Este modelo de ameaça considera que um adversário pode tomar a forma de um participante e começar a atuar de forma ativa. Ou seja, o participante tentará de alguma forma comprometer o esquema submetendo partes incorretas no momento da reconstrução, fazendo com que os participantes honestos não consigam reconstruir o segredo e também falha em alertar os outros participantes que eles não reconstruíram o segredo correto. Considera-se aqui o Distribuidor uma entidade honesta que gera os parâmetros, o segredo e distribui as partes de forma segura para os Participantes. Não fica claro quem deve ser o Reconstrutor, entretanto, o modelo de ameaça deixa em aberto que um Participante malicioso poderia assumir esse papel. Ou seja, uma entidade não confiável pode prejudicar a reconstrução do segredo. A tabela 3 ilustra a relação do modelo de ameaça alternativo 2 com as entidades.

Tabela 3. Modelo de Ameaça 2 - Participante Malicioso

	Confiável	Malicioso	Passivo	Ativo
Distribuidor	✓			
Participante		✓		
Reconstrutor	✓			
Adversário				✓

5.2.1. Esquemas Seguros para este Modelo

Considerando o modelo de ameaça 2, onde um participante pode ser malicioso, o esquema de Bellare e Rogaway [Rogaway and Bellare 2007] propõe um framework para esquemas

de segredo compartilhado que mantém um Distribuidor confiável e participantes polarizados, ou seja, existem participantes honestos e maliciosos. O framework consegue garantir a segurança nesse modelo de ameaça propondo um protocolo chamado HK2, redefinindo o esquema de Krawczyk's. O framework estende a ideia de adversários classificando como poderiam comprometer as partes. Esses adversários são classificados da seguinte forma:

- Erasure (0): Adversário não consegue corromper as partes (apenas visualizar e prevenir o uso no processo de reconstrução).
- Recoverability (1): Adversário pode corromper todas as partes, exceto uma (isso corresponde o caso onde o Reconstrutor é um participante honesto).
- Recoverability (2): Um adversário pode corromper todas as partes (isso corresponde ao caso onde o reconstrutor é uma terceira parte).

Outros esquemas que também tentam garantir segurança contra Participantes maliciosos são os trabalhos de Carpentieri [Carpentieri 1995] e Rabin e Ben-Or [Rabin and Ben-Or 1989], onde propõe um esquema que os Participantes possuem canais de comunicação segura entre eles para troca de mensagens. Esses participantes podem se comunicar secretamente que podem verificar as partes com uma maioria honesta.

Dado um conjunto total de participantes n, sendo necessário no mínimo t para reconstruir o segredo, o protocolo se baseia em um Distribuidor confiável que gerará um segredo k, partes $s_1, \ldots, s_n$ que serão distribuídos para os Participantes. Além desses valores, o Distribuidor enviará também um vetor para verificação v_i para cada Participante i. Ao final do processo, os Participantes devem se reunir para tentar recuperar o segredo com o Reconstrutor obtendo novamente um valor y. Os Participantes devem então verificar esse valor utilizando suas partes s_i juntamente com o vetor v. Cada um ao final da operação de verificação deverá obter um valor que seria o segredo k. Caso uma maioria honesta consiga obter o valor y, isso significa que $y = k$ e recuperaram de forma correta o segredo inicial.

6. Novo Modelo de Ameaça

O novo modelo de ameaça descrito neste trabalho consiste no uso de mais uma entidade definida na seção 3 chamada de Detentor do Segredo. Além disso, este trabalho definirá o Reconstrutor como uma terceira parte. Ou seja, será uma entidade que não exerce o papel de Participante, podendo ser tanto o Distribuidor quanto uma terceira parte exercendo exclusivamente este papel.

Neste modelo de ameaça, o Detentor do Segredo honesto cria um determinado segredo k de acordo com suas regras locais, cria os parâmetros de limiar (n, m) e envia de maneira segura para o Distribuidor. O Distribuidor malicioso então gerará as partes e distribuirá para os Participantes. Essa geração das partes pode estar comprometida, pois o Distribuidor pode gerar partes falsas com o objetivo de atrapalhar a reconstrução do segredo ou gerar as partes de tal forma que comprometa a segurança do sistema, possibilitando que menos partes poderiam ser utilizadas para recuperar o segredo. Além disso, a distribuição pode não ser feita de maneira segura para os Participantes, pois não se sabe como essa comunicação é feita. Os Participantes são considerados honestos, pois guardarão suas partes com segurança e participarão de maneira correta do momento de

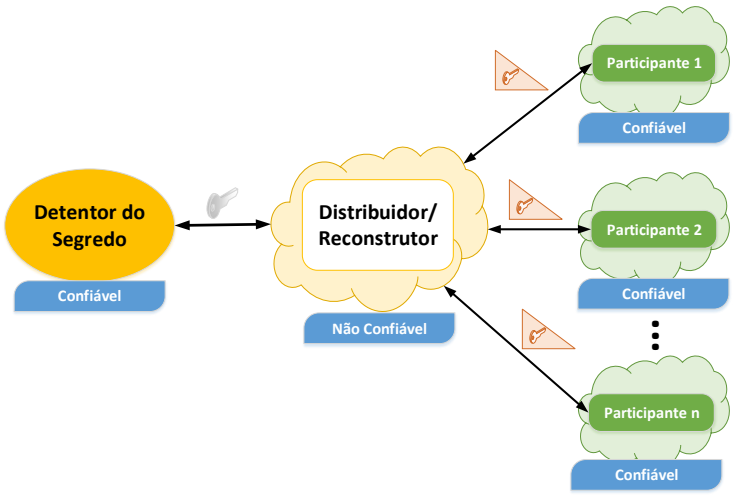

Figura 1. Ilustração de um exemplo do novo modelo de ameaça a esquemas de segredo compartilhado.

reconstrução. O Reconstrutor é uma terceira entidade ou o próprio Distribuidor e se comporta de maneira maliciosa. Ou seja, o mesmo pode não recuperar o segredo de maneira deliberada ou pode tentar divulgar o segredo e as partes sem a permissão do Detentor do Segredo.

Um exemplo seria uma aplicação que gera parâmetros secretos e deseja utilizar um dispositivo criptográfico disponibilizado em nuvem para replicar os dados de maneira segura e tentar garantir disponibilidade desses dados. O Detentor do segredo (que seria a aplicação local) utilizaria uma terceira parte não confiável para como Distribuidor e Reconstrutor para distribuir e reconstruir as partes antes de obter novamente o segredo. Essas partes seriam enviadas para outros provedores de nuvens separados para garantir segurança e disponibilidade. Dessa forma, seria interessante que apenas o Detentor do Segredo tivesse posse do Segredo em claro para garantir a segurança em todo o processo. A figura 1 ilustra o exemplo aqui comentado. A tabela 4 ilustra a relação do novo modelo de ameaça com as entidades.

Tabela 4. Novo Modelo de Ameaça - Distribuidor e Reconstrutor Maliciosos

	Confiável	Malicioso	Passivo	Ativo
Detentor do Segredo	✓			
Distribuidor		✓		
Participante	✓			
Reconstrutor		✓		
Adversário				✓

7. Avaliação Novo Modelo de Ameaça

Para realizar a avaliação dos esquemas no novo modelo de ameaça vamos seguir as etapas:

1. Mostrar um protocolo de segredo compartilhado com a entidade Detentor do Segredo.

2. Analisar quais seriam os pontos de vulnerabilidade considerando o Novo Modelo de Ameaça.
3. Criar uma tabela comparativa mostrando a vulnerabilidade de diferentes esquemas de segredo compartilhado frente à algumas das principais ameaças.
4. Criar uma tabela mostrando quais esquemas de segredo compartilhado ainda estão vulneráveis para os diferentes modelos de ameaça.
5. Propor uma possível solução para contornar o problema de segurança encontrado.

O seguinte protocolo ilustra um exemplo de como fica um esquema de segredo compartilhado com uma nova entidade. A partir disso, pode-se avaliar o conhecimento de cada entidade e verificar a segurança conforme o modelo de ameaça adotado.

$$
\begin{array}{llcll}
M_1 & Dt & \xrightarrow[\text{interna}]{} & Dt & : \; k, t, n \\
M_2 & Dt & \xrightarrow[\text{externa}]{} & D & : \; k, t, n \\
M_3 & D & \xrightarrow[\text{externa}]{} & P_1 \dots P_n & : \; (s_1, \dots, s_n) \\
M_4 & P_1 \dots P_n & \xrightarrow[\text{externa}]{} & R & : \; (s_1, \dots, s_n) \\
M_5 & R & \xrightarrow[\text{interna}]{} & R & : \; k \\
M_6 & R & \xrightarrow[\text{externa}]{} & Dt & : \; k
\end{array}
$$

Considerando Dt como Detentor do segredo, D como o Distribuidor malicioso, P_i tal que $i \in \{1, \dots, n\}$ são Participantes, R é o Reconstrutor malicioso, a seta $\rightarrow$ representa a comunicação entre Entidades, podendo ser $interna$ ou $externa$ (ou seja, mensagens para criação própria de parâmetros ou mensagens para outras entidades com ações do esquema), s_i tal que $i \in \{1, \dots, n\}$ são partes do segredo, k é o segredo original gerado a partir de partes enviadas pelos participantes.

A análise do esquema é o seguinte: No protocolo anterior, a mensagem M_1 que o Detentor do segredo gera os parâmetros k, t, n, sendo esses os necessários para fazer o esquema funcionar. Os mesmos são então repassados de maneira segura para o Distribuidor na mensagem M_2. A partir deste momento, o Distribuidor tem conhecimento do segredo e pode tomar atitudes suspeitas como a divulgação do segredo ou alteração dos parâmetros, não gerando de forma correta e honesta. Considerando que o mesmo seja malicioso, o esquema estará parcialmente comprometido a partir dessa mensagem M_2. A mensagem M_3 é o envio seguro das partes para todos os Participantes do esquema. Esses Participantes são honestos e não subverterão o protocolo. Participarão de forma honesta na reconstrução do segredo. A mensagem M_4 é o processo de recuperação do segredo, onde os Participantes enviam suas partes para o Reconstrutor de forma segura. A mensagem M_5 é o processo onde o Reconstrutor recupera o segredo e pode tomar atitudes suspeitas, como a divulgação do mesmo. A mensagem M_6 é onde o Reconstrutor envia de volta o segredo para o Detentor do Segredo.

Ao avaliar o protocolo anterior, existem diversas partes onde entidades maliciosas podem tomar atitudes suspeitas como a divulgação do segredo, mudança nas partes e mudança no segredo. A tabela 5 ilustra a quais ameaças estão expostas cada um dos principais esquemas de segredo compartilhado.

Na tabela 5, as ameaças são descritas a seguir:

Tabela 5. Ameaças aos quais cada esquema de segredo compartilhado está exposta.

	A_1	A_2	A_3	A_4	A_5
[Shamir 1979]	✓	✓	✓	✓	✓
[Feldman 1987]	✓	✓			
[Pedersen et al. 1991]	✓	✓			
[Rabin and Ben-Or 1989]	✓	✓			
[Rogaway and Bellare 2007]	✓	✓			

- A_1- **Divulgar Segredo:** Quando o Distribuidor não é totalmente confiável, o segredo que é repassado para ele não cifrado pode ser divulgado sem a autorização do Detentor do Segredo para um adversário. Esse adversário pode ser uma terceira parte fora do esquema ou para algum Participante malicioso.
- A_2- **Alteração dos Parâmetros:** Ao utilizar um Distribuidor malicioso como gerador de parâmetros do esquema de segredo compartilhado, pode-se ter alterações nos parâmetros originais que foram repassados por um Detentor de Segredo ou uma terceira parte confiável. Essa alteração pode consistir em:
  1. Não utilizar um gerador de números aleatórios confiável
  2. Gerar propositadamente parâmetros fracos
  3. Não utilizar os parâmetros corretos e possibilitar a recuperação com menos partes do que o necessário
- A_3- **Alterar Partes:** Participantes podem receber corretamente suas partes, entretanto, no momento da reconstrução, Participantes maliciosos podem enviar partes incorretas para prevenir a geração correta do segredo.
- A_4- **Subverter Protocolo:** Podem existir Participantes maliciosos que tentarão atrapalhar o protocolo enviando partes erradas ou simplesmente não participando das reconstruções. Essas atitudes podem comprometer a reconstrução do segredo, evitando que saibam quem realizou os ataques.
- A_5- **Partes Reveladas na Reconstrução:** Esse tipo de ameaça depende do tipo do modelo de ameaça e da entidade Reconstrutor. Se essa entidade é uma terceira parte confiável, as partes normalmente não são reveladas, entretanto, ao colocar um participante, deve-se revelar as partes e descartar após o procedimento de reconstrução. Caso o reconstrutor seja uma entidade maliciosa, o mesmo pode querer divulgar as partes para adversários.

A tabela 6 faz um comparativo dos diferentes esquemas de segredo compartilhado e para quais modelos de ameaça são vulneráveis. Nota-se que para o novo modelo todos estariam vulneráveis.

Tabela 6. Quais esquemas de segredo compartilhado estão vulneráveis para diferentes modelos de ameaça.

	Tradicional	Modelo 1	Modelo 2	Novo Modelo
[Shamir 1979]	✓			✓
[Feldman 1987]				✓
[Pedersen et al. 1991]				✓
[Rabin and Ben-Or 1989]				✓
[Rogaway and Bellare 2007]				✓

7.1. Possível Solução

Ao analisar o novo modelo de ameaça aqui proposto, nota-se que existem diversos pontos de falha, como a divulgação do segredo e alteração dos parâmetros. Para que essas propriedades sejam protegidas, o Detentor do Segredo pode tomar algumas providências iniciais para garantir uma maior segurança.

Uma das atitudes iniciais é considerar que existe essa entidade a mais, fazendo com que o Distribuidor não seja uma entidade totalmente confiável. Partindo dessa premissa, pode-se então cifrar o segredo antes de enviar para o Distribuidor com uma chave simétrica Ks. O seguinte protocolo ilustra essa possível solução.

$$
\begin{array}{llcll}
M_1 & Dt & \xrightarrow[\text{interna}]{} & Dt & : \; k, t, n, Ks \\
M_2 & Dt & \xrightarrow[\text{interna}]{} & Dt & : \; E(k)_{Ks} \\
M_3 & Dt & \xrightarrow[\text{externa}]{} & D & : \; (k)_{Ks}, t, n \\
M_4 & D & \xrightarrow[\text{externa}]{} & P_1 \dots P_n & : \; (s_1, \dots, s_n) \\
M_5 & P_1 \dots P_n & \xrightarrow[\text{externa}]{} & R & : \; (s_1, \dots, s_n) \\
M_6 & R & \xrightarrow[\text{interna}]{} & R & : \; (k)_{Ks} \\
M_7 & R & \xrightarrow[\text{externa}]{} & Dt & : \; (k)_{Ks} \\
M_8 & Dt & \xrightarrow[\text{interna}]{} & Dt & : \; D(k)_{Ks}
\end{array}
$$

Considerando Dt como Detentor do segredo, D como o Distribuidor malicioso, P_i tal que $i \in \{1, \dots, n\}$ são Participantes, R é o Reconstrutor malicioso, a seta $\rightarrow$ representa a comunicação entre Entidades, podendo ser $interna$ ou $externa$ (ou seja, mensagens para criação própria de parâmetros ou mensagens para outras entidades com ações do esquema), s_i tal que $i \in \{1, \dots, n\}$ são partes do segredo, k é o segredo original gerado a partir de partes enviadas pelos participantes.

Neste protocolo pode-se ver que na mensagem M_1 além de criar os parâmetros, o Detentor do Segredo agora também cria uma chave simétrica Ks para cifrar o segredo. A mensagem M_2 ilustra o procedimento de cifragem do segredo k com a chave Ks. A partir da mensagem M_3 até a mensagem M_7 é feita da mesma forma como o protocolo anterior, com a diferença de que as outras entidades tem conhecimento apenas do segredo cifrado. Na mensagem M_8 o segredo é então decifrado pelo Detentor do Segredo.

8. Considerações Finais

Com a análise feita nos modelos de ameaças tradicionais e alternativos, pode-se detectar que esses modelos não refletem a realidade de muitas aplicações utilizadas. Grande parte das aplicações utilizam uma entidade separada para gerar o segredo e os parâmetros utilizando o Distribuidor somente para quebrar o segredo e compartilhar as partes. Dessa forma, este trabalho propôs a criação de uma nova entidade chamada Detentor do Segredo. Após a criação dessa nova entidade, os modelos de ameaça mudam e precisam ser novamente analisados. Por isso, um novo modelo de ameaça também foi proposto para analisar os principais esquemas de segredo compartilhado.

Após o levantamento dos principais esquemas de segredo compartilhado na literatura para os diferentes modelos de ameaças, atingiu-se o objetivo de detectar vulnerabilidades para esses esquemas utilizando o novo modelo de ameaça aqui proposto. A análise foi baseada na avaliação do protocolo tradicional de segredo compartilhado, utilizando as entidades normalmente encontradas na literatura. Com isso, observou-se alguns pontos de falhas para algumas ameaças aqui citadas. Com essas novas ameaças, este trabalho também propôs uma possível solução para contornar as vulnerabilidades encontradas.

Como trabalho futuro, pretende-se aplicar o novo modelo de ameaça descrito neste trabalho para introduzir um novo assunto chamado de estruturas de acesso escondidas. Essas estruturas de acesso escondidas tem como uma das premissas o uso de Distribuidores maliciosos e diferentes modelos de ameaça de tal forma que seja possível recuperar o segredo com menos partes que o liminar definido no protocolo de Shamir.

Referências

Beimel, A. (2011). Secret-sharing schemes: a survey. In *Coding and cryptology*, pages 11–46. Springer.

Blakley, G. R. (1979). Safeguarding cryptographic keys. In *Proc. AFIPS 1979 National Computer Conference*, pages 313–317.

Carpentieri, M. (1995). A perfect threshold secret sharing scheme to identify cheaters. *Designs, Codes and Cryptography*, 5(3):183–187.

Feldman, P. (1987). A practical scheme for non-interactive verifiable secret sharing. In *Foundations of Computer Science, 1987., 28th Annual Symposium on*, pages 427–438. IEEE.

Martin, K. M. (2008). Challenging the adversary model in secret sharing schemes. *Coding and Cryptography II, Proceedings of the Royal Flemish Academy of Belgium for Science and the Arts*, pages 45–63.

Pedersen, T. P. et al. (1991). Non-interactive and information-theoretic secure verifiable secret sharing. In *Crypto*, volume 91, pages 129–140. Springer.

Rabin, T. and Ben-Or, M. (1989). Verifiable secret sharing and multiparty protocols with honest majority. In *Proceedings of the twenty-first annual ACM symposium on Theory of computing*, pages 73–85. ACM.

Rogaway, P. and Bellare, M. (2007). Robust computational secret sharing and a unified account of classical secret-sharing goals. In *Proceedings of the 14th ACM conference on Computer and communications security*, pages 172–184. ACM.

Shamir, A. (1979). How to share a secret. *Communications of the ACM*, 22(11):612–613.

Tompa, M. and Woll, H. (1989). How to share a secret with cheaters. *journal of Cryptology*, 1(3):133–138.

