Um sistema de pagamento eletrônico com garantia de privacidade baseado no algoritmo criptográfico RSA

Gustavo Gattino
E-mail: <gustavo.gattino@gmail.com>.
Universidade do Vale do Rio dos Sinos - Unisinos

Marcelo Danesi
E-mail: <mdanesi@unisinos.br>.
Universidade do Vale do Rio dos Sinos - Unisinos

Luciano Ignaczak
E-mail: <lignaczak@unisinos.br>.
Universidade do Vale do Rio dos Sinos - Unisinos

Resumo

A exposição dos dados do cliente a diferentes entidades durante o processo de compra pode levar a mapeamento de perfil e situações constrangedoras dependendo da natureza dos produtos adquiridos. Para solucionar esse problema, um sistema para realização de transações de comércio eletrônico garantindo a privacidade da parte compradora é implementado. Através dele, o usuário tem a garantia de que a privacidade de suas informações estão seguras para com as demais entidades envolvidas no processo. Esse sistema utiliza um modelo com três entidades — cliente, loja virtual e processador de pagamento — as quais não conseguem associar a compra realizada ao cliente comprador. Experimentos foram realizados avaliando o sistema quanto a colisões na geração de tickets e sua resistência a ataques de fabricação. Foi possível perceber um aumento na ocorrência de colisões a medida que a quantidade de usuários cresce, indicando que a proporção de usuários e valores disponíveis para a geração dos tickets deve ser de 1 para 100, reduzindo as chances de colisão para 0,01%. O mesmo ocorre no experimento de fabricação: à medida que mais valores são aceitos, maior é a taxa de sucesso.[1]
Palavras-chave: Privacidade, Comércio Eletrônico, RSA.

Recentemente as pessoas tornaram-se mais sensíveis em relação a sua privacidade *on-line* — o direito de controlar ou influenciar quais informações sobre elas podem ser coletadas, armazenadas e divulgadas (ISO 7498-2, 1989) — percebendo que deixam todos os tipos de rastros ao navegar (Souza, 2013). Casos como o monitoramento de pagamentos internacionais, bancos e transações de cartão de crédito tornaram usuários de serviços de pagamento *on-line* mais preocupados com quem acessa seus dados (Spiegel, 2013).

A criptografia fornece meios de proteção à privacidade com relação a terceiros, de modo a dificultar a espionagem. No entanto, existem situações em que a proteção da privacidade deve ir ainda mais longe e é neste momento em que a identidade do usuário passa a ser o ponto mais importante nas trocas de informações.

1 Artigo publicado na 13ª Escola Regional de Redes de Computadores - 2015.

DOI: 10.18256/2359-3539/reit-imed.v2n2p44-54

O principal problema com pagamentos digitais é que o cliente é obrigado a passar as suas informações de identificação e pagamento ao vendedor, sendo essa falta de privacidade uma das principais razões que impedem o crescimento do comércio eletrônico, uma vez que limita a confiança de potenciais clientes (Grudzinski, 2013) (Thomasso, 2013). A demanda pela omissão da identidade *on-line* é completamente justificável, uma vez que muitas situações da vida *off-line* são anônimas: lojas físicas oferecem um certo grau de anonimato para seus clientes se esses pagarem com dinheiro.

Diante do problema levantado, o objetivo deste trabalho é elaborar um sistema de pagamento que garanta a privacidade das informações de pagamento do comprador e a não vinculabilidade entre as compras realizadas. Através desse sistema, o usuário terá a garantia de que a privacidade de suas informações de transação estarão seguras para com as demais entidades envolvidas no processo de pagamento. O sistema define um modelo com três entidades: cliente, loja virtual e processador de pagamento. Entre elas, apenas o processador de pagamento conhece a identidade do cliente, no entanto nenhuma consegue associar a compra realizada ao comprador.

A principal contribuição gerada por este trabalho é a construção do sistema de pagamento digital que faz uso da função criptográfica RSA, amplamente utilizada para garantir autenticidade e confidencialidade, como forma de garantir a não vinculabilidade entre uma compra realizada e o seu comprador. Essa garantia é possível através da utilização das propriedades de injeção e não sobrejeção que a função possui.

Fundamentação Teórica

Privacidade

No que diz respeito a dados, a privacidade geralmente é um conceito aplicado a "dados pessoais" (informações relativas a uma pessoa singular identificada ou identificável) (Pfitzmann & Hansen, 2010) (Cooper et al., 2013) e "o direito dos indivíduos de controlar ou influenciar quais informações relacionadas a eles podem ser coletadas e armazenadas, por quem e para quem essa informação pode ser divulgada" (ISO 7498-2, 1989, p. 4).

Ao longo das últimas décadas, os trabalhos na área de privacidade e proteção de privacidade têm enfocado a ideia de minimização dos dados, a qual faz uso de terminologias como anonimato, pseudonimato e não vinculabilidade. A ideia principal por trás da minimização de dados está na habilidade de incapacitar o recolhimento de dados pessoais de um sujeito ou na redução de dados recolhidos (Pfitzmann & Hansen, 2010) (Cooper et al., 2013).

O uso da minimização dos dados é a única estratégia que aumenta a privacidade de um indivíduo caso dados pessoais sejam usados, uma vez que eles inerentemente fornecem algum tipo de associação a pessoa. Outras técnicas têm sido propostas e implementadas visando aumentar a privacidade através do envio de informações erradas ou desinformação (Pfitzmann & Hansen, 2010).

Anonimato

O anonimato descreve a condição de uma identidade em ser desconhecida ou oculta e que as suas ações não podem ser rastreadas até a sua origem (ISO/IEC 15408-2, 2008). Para isso, a existência do anonimato depende de um conjunto de usuários com atributos parecidos. O conjunto de todos estes possíveis usuários, os quais podem variar ao longo do tempo, é conhecido como o conjunto de anonimato (Chaum, 1988) (Pfitzmann & Hansen, 2010).

O conjunto de possíveis usuários depende do conhecimento que um observador tem sobre eles, sendo assim o anonimato relativo em relação ao observador. Portanto, por exemplo, um comprador pode ser anônimo somente dentro de um conjunto de potenciais compradores — o seu conjunto de anonimato — o que em si pode ser um subconjunto de todos os usuários que podem fazer uma compra. Da mesma forma, o vendedor pode ser anônimo apenas dentro de um conjunto de potenciais vendedores. Ambos os conjuntos de anonimato podem ser separados, sobrepostos ou até mesmo ser o mesmo conjunto (Pfitzmann & Hansen, 2010).

Pseudonimato

Uma das formas de ocultar a verdadeira identidade de uma entidade é através da utilização de pseudônimos. O pseudonimato garante que o usuário possa usar um recurso ou serviço sem revelar a sua identidade, sem que a responsabilidade do uso desse recurso seja negada. Este pode ser diretamente responsabilizado pelos seus atos por es-

tar relacionado a uma referência (pseudônimo) no sistema (ISO/IEC 15408-2, 2008). Os nomes reais dos clientes não podem ser facilmente determinados através da simples observação das ações, mas é possível que o pseudônimo seja correlacionado a uma identidade real (Shirey, 2007).

Em vários aspectos o pseudonimato se assemelha ao anonimato, por ambos protegerem a identidade do utilizador. Contudo, o pseudonimato difere por não ser completamente indetectável: no pseudonimato uma referência a identidade do utilizador é mantida para fins de contabilização dentro do sistema, mas sua identidade é anônima para entidades externas ao sistema. De forma geral, a identidade do usuário só precisa ser resgatada em condições específicas, como por exemplo, em um ambiente de pagamentos, no qual é vantajoso ser capaz de detectar a identidade de um pagador quando um mesmo cheque é emitido várias vezes (fraude) (Shirey, 2007) (ISO/IEC 15408-2, 2008).

O uso de pseudônimos é uma solução clássica para o fornecimento de anonimato, quando nem a relação entre pseudônimo e sujeito, nem a relação entre diferentes pseudônimos é revelada a um observador. Mudando pseudônimos entre contextos, um sujeito pode tornar impossível a ligação entre identidades em diferentes esferas de contexto. Um exemplo simples é o uso de diferentes endereços eletrônicos como pseudônimos para fornecer não vinculabilidade entre comunicação de negócios e pessoal (Gerlach, 2006; Eichler, 2007).

O pseudonimato garante privacidade?

É uma crença geral que o uso adequado do anonimato ou pseudonimato é suficiente para combater as ameaças à privacidade. Todavia, o foco atual em esconder informações explícitas de identidade não é suficiente. Há ainda uma considerável quantia de informações de identificação que são expostas à medida que usamos um sistema: nosso padrão de comportamento. O modo como agimos e navegamos é suficiente para que um atacante deduza a identidade de um usuário quando uma quantidade suficiente de comunicação é analisada (Rao & Rohatgi, 2000).

No contexto de pagamentos eletrônicos, o mesmo pode ocorrer ao comparar o comportamento de gastos e acessos de um usuário (Pfitzmann & Waidner, 1992). Por exemplo, se um usuário faz pagamentos a diferentes entidades e a sua identidade é conhecida por uma delas, estas entidades podem simplesmente juntar suas informações e identificá-lo, caso os pagamentos possam ser vinculados entre si.

Ainda assim, mesmo que este usuário não seja conhecido por nenhuma das entidades, é possível identificá-lo através da comparação das informações sobre o comportamento dos gastos dos indivíduos dentro do sistema bancário, como quando e quanto dinheiro cada pessoa retirou, e possibilitar a vinculação entre ações para quebrar o anonimato desse sistema (Pfitzmann & Waidner, 1992).

Não vinculabilidade

Não vinculabilidade, termo adaptado do inglês *unlinkability*, dentro de um determinado conjunto de informações, assegura que um usuário possa fazer múltiplos usos dos recursos ou serviços de um sistema sem que um observador possa distinguir, com um grau de probabilidade elevado o suficiente para ser útil, se duas ou mais dessas ações estão relacionadas ou não (ISO/IEC 15408-2, 2008) (Pfitzmann & Hansen, 2010) (Cooper et al., 2013).

Como resultado, um de seus requisitos implica que a identidade do usuário de uma operação seja protegida. Caso contrário, essa informação pode ser usada para associar as demais operações. Contudo, pseudonimato e não vinculabilidade não propõem a mesma característica ao usuário, pois, embora no pseudonimato a identidade do usuário também seja desconhecida, as relações entre diferentes ações ainda podem ser identificadas (ISO/IEC 15408-2, 2008). Enquanto o anonimato refere-se à relação entre emissores/receptores e dados, não vinculabilidade descreve a relação entre os itens com relação a alguma característica comum a eles (Pfitzmann & Hansen, 2010).

A não vinculabilidade requer que operações diferentes não possam ser relacionadas. Esta relação pode assumir várias formas, pois um modelo pode especificar quais tipo de relações devem ser combatidas: alguns modelos incluem a capacidade de fazer uso de múltiplos pseudônimos, por exemplo, para que não seja possível a criação de um padrão de uso que revele a identidade do usuário (ISO/IEC 15408-2, 2008).

Proof-of-Work

Em muitos protocolos criptográficos, um usuário procura convencer um verificador que possui conhecimento de um segredo ou que uma determinada relação matemática é válida. Por outro lado, em um *proof-of-work* (PoW), um usuário demonstra a um verificador que este passou por uma certa quantidade de trabalho computacional em um intervalo de tempo especificado (Jakobsson & Juels, 1999). Uma propriedade importante de todos os PoWs é que eles são muito custosos para resolução, porém comparativamente baratos para validação (Laurie & Clayton, 2004).

Atualmente, o sistema mais conhecido de PoW é o Hashcash, sendo principalmente utilizado para impedir o envio de *spam*. Este algoritmo exige que um usuário produza uma *string* cujo *hash* criptográfico comece com um determinado número de zeros para ser aceito (Laurie & Clayton, 2004).

Trabalhos relacionados

Trabalhos anteriores mostram a dificuldade de manter a privacidade de um usuário no contexto de dados em rede e serviços *on-line* que expõem informações parciais do seu comportamento. (Backstrom, Dwork, & Kleinberg, 2007) consideraram ataques à privacidade dos usuários, identificando-os através da estrutura de rede que os cercam e discutiram a dificuldade de garantir o anonimato do usuário quando há presença de dados na rede que os identificam. (Crandall et al., 2010) correlacionam laços sociais entre usuários, em que nenhuma correlação foi explicitamente declarada, apenas ao identificar padrões *off-line*: tendo em conta que duas pessoas estão aproximadamente na mesma localidade geográfica, aproximadamente ao mesmo tempo e em diversas ocasiões, estas, provavelmente, estão relacionadas. (Narayanan & Shmatikov, 2008) quebraram o anonimato do *dataset* do algoritmo Netflix Prize usando informações do IMDB2, a qual tinha conteúdos de usuário similar, mostrando que a correlação estatística entre diferentes, mas relacionados, conjuntos de dados podem ser usados para atacar a privacidade. (Puzis, Yagil, Elovici, & Braha, 2009) simularam o monitoramento de uma rede de comunicações usando nós de monitoramento localizados em pontos estratégicos da rede, mostrando que, ao usar topologias de rede do mundo real, um número relativamente pequeno de nós pode representar uma ameaça significativa para a privacidade.

(Rennhard, Rafaeli, Mathy, Plattner, & Hutchison, 2004) apresentam novos componentes que permitem um comércio eletrônico seguro baseado em pseudônimos. De um lado, estes componentes permitem que clientes possam navegar através de um loja virtual, selecionar seus bens e pagá-los com seu cartão de crédito de tal forma que nem a loja, nem o emissor do cartão de crédito, nem um intruso serão capazes de obter qualquer informações sobre a identidade do cliente. Por outro lado, é garantido que nenhuma das partes envolvidas é capaz de atuar desonestamente durante o pagamento.

(Konidala et al., 2012) propõe um modelo de pagamento *mobile* pré-pago baseado em HTTPS, no qual o cliente obtém informações sobre a conta bancária do comerciante e instrui seu banco a transferir dinheiro para essa conta, no momento do pagamento. O protocolo de comunicação NFC é utilizado através do *smartphone* do cliente para obter informações sobre a conta bancária. O modelo também faz uso do esquema de assinatura parcialmente cega para esconder a identidade dos clientes do banco e do comerciante. Este modelo provê ao cliente um maior controle sobre seus pagamentos e proteção de sua privacidade em relação ao banco e comerciante.

(Nakanishi & Sugiyama, 2005) propõem um sistema de moeda eletrônica *on-line* anônimo com pagamentos exatos não vinculáveis, no qual a não vinculabilidade é alcançada sem perda de eficiência. Neste modelo, a moeda eletrônica é uma assinatura digital do banco assinada de forma cega e ocultada através de criptografia e técnicas de *zero-knowledge* durante o pagamento, impossibilitando a ligação entre transações. O modelo possui funcionalidades de revogação do anonimato, a fim de constranger a sua utilização para fins ilícitos.

Sistema de pagamento eletrônico

Este artigo define um sistema para realização de transações de comércio eletrônico garantindo a privacidade da parte compradora. Através dele, o usuário tem a sua privacidade assegurada du-

rante o processo de compra. Essa segurança se dá através do uso de pseudônimos na compra com a loja virtual e da ofuscação do *ticket* escolhido pelo usuário com o processador de pagamento. Através desses dois elementos, o anonimato da compra é alcançado, garantindo a não vinculabilidade entre uma ou mais compras realizadas através do sistema e as identidades utilizadas para a compra. O sistema utiliza um modelo com três entidades — cliente, loja virtual e processador de pagamento.

Funcionamento do Sistema

O sistema utiliza oito etapas para a realização da compra, conforme mostrado na Figura 1, as quais são descritas a seguir.

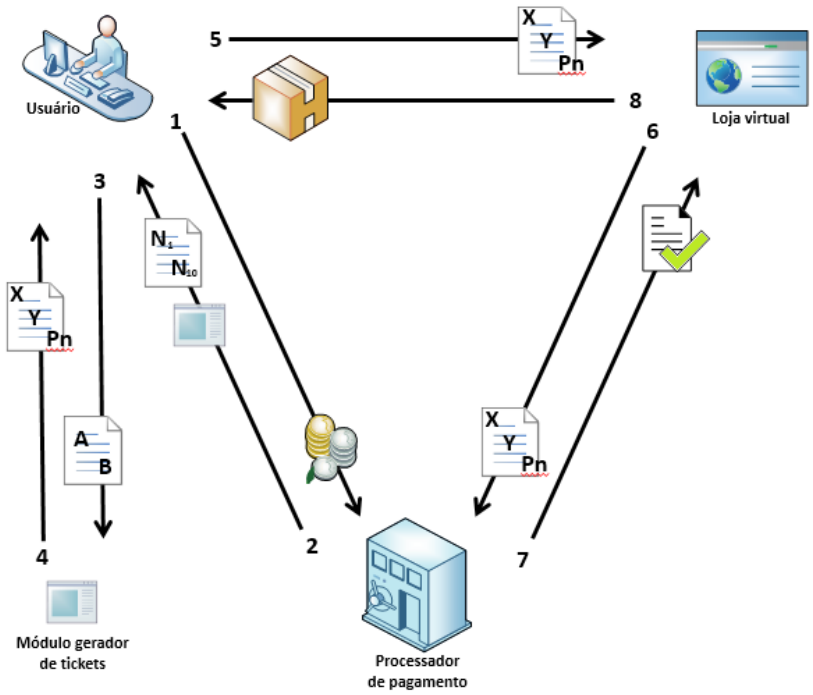

Figura 1. Processo de compra do sistema de pagamento proposto.

No início do processo de compra, o cliente entra em contato com o processador de pagamento solicitando a aquisição de um *ticket* de pagamento. Nesse momento, para adquirir o *ticket*, o cliente realiza um pagamento digital amplamente adotado (1) — este pagamento pode ocorrer através de cartão de crédito, boleto bancário, Paypal, etc.

Após concluída a transação, o processador de pagamento envia ao cliente o módulo de geração de *tickets* e um conjunto de *n* valores (2). O módulo e os valores enviados são utilizados para a geração do *ticket* do usuário. A partir do momento em que esses dados são recebidos, o usuário tem um espaço de tempo *t* para geração e gasto do seu *ticket*.

Ao receber os dois componentes, o usuário escolhe um par de valores dentre os *n* recebidos — os dois valores escolhidos serão representados por *A* e *B* — e submete-os ao módulo de geração (3). O módulo de geração deriva matematicamente os valores *A* e *B* em dois novos valores distintos, representados por *X* e *Y*, usando o algoritmo criptográfico RSA. Esses dois novos valores não podem ser vinculados aos valores originais, porém o processador de pagamento consegue verificar a sua autenticidade. A relação matemática entre *A* e *B* e *X* e *Y* é usada como autenticação.

Após a derivação, o módulo de geração utiliza os valores resultantes em uma função *Proof-of-Work*. Sua execução exige (*t*/2) + 1 minutos para conclusão (visando impedir a utilização de mais do que dois dos valores enviados — *double spending*). Após concluído o PoW, o módulo de geração retorna ao usuário o *ticket*: uma *string* que concatena os valores *X* e *Y* e o valor utilizado pelo PoW como *nounce* (4). Após a execução do módulo gerador, o usuário tem em torno (*t*/2) – 1 minutos para realizar a compra.

De posse do *ticket*, o usuário já pode realizar a sua compra virtual. Para isso, o usuário envia-o à loja virtual (5) que, por sua vez, valida sua autenticidade junto ao processador de pagamento (6). O processador de pagamento comprova a validade do *ticket* através de um verificador de PoW e confere se o valor recebido já não consta em seu banco de dados de *tickets* recebidos (7).

Validado o *ticket*, a loja virtual libera o produto ao comprador (8). A compra realizada não pode ser vinculada ao usuário, pois o processador de pagamento não sabe qual *A* e *B* o usuário escolheu para gerar *X* e *Y* e o mesmo não enviou seus dados reais.

O funcionamento correto do sistema depende do atendimento de alguns requisitos obrigatórios, os quais definem limites no escopo do seu uso.

1. Limite de instâncias do módulo gerador de *tickets*: O usuário deve ser incapaz de executar duas ou mais instâncias do módulo de geração de *tickets* de forma paralela.
2. Definição do processador de pagamento como entidade de confiança: O processador de pagamento deve ser uma entidade confiável e não vincula os números enviados a clientes com seus valores derivados finais através da submissão desses ao módulo gerador de *tickets*.
3. Definição do usuário como entidade anônima na rede: O usuário faz uso de tecnologias que o qualificam como anônimo na rede ao comunicar-se com as outras entidades envolvidas no processo de compra.

Discussão de Segurança

Nesta seção é abordada a forma como o modelo proposto resolve possíveis falhas e questões de segurança decorrentes de sua utilização.

Gasto duplicado

É possível que um *ticket* seja utilizado de forma repetida se um controle de utilização não for implementado. Essa falha de segurança, na qual um usuário gasta um mesmo *ticket* duas ou mais vezes, é chamada de *double-spending*.

No modelo proposto, o provedor de pagamento mantém uma listagem de todos os *tickets* válidos e não expirados. Ao receber um *ticket* de uma loja virtual, seu banco de dados de *tickets* gastos é atualizado, adicionando este novo valor. Com isso, gastos duplos são impedidos pelo sistema, sendo negados pelo serviço ao serem recebidos da loja virtual. Embora o reuso possa ser detectado e evitado, este processo não permite identificar a identidade do utilizador.

O sistema também impossibilita que seja gasto mais do que foi pago, pois a geração dos *tickets* leva em torno da metade do tempo de sua expiração para ser concluída, impedindo que o usuário gere mais de um *ticket*.

Comprometimento da identidade do cliente na loja virtual

A identidade do cliente é comprometida à medida que este faz uso de dados pessoais válidos para realização da compra, uma vez que todos os dados pessoais válidos inerentemente fornecem algum tipo de vinculação a uma identidade.

O *ticket* utilizado no modelo, gerado pelo usuário, não possui qualquer tipo de informação que possa identificá-lo, impedindo que a loja vincule sua identidade a compra.

Relação entre compra e identidade do cliente

A comunicação do usuário em relação ao processador de pagamento não pode ser anônima, uma vez que este deve informar dados pessoais para a realização da compra dos *tickets*.

Para garantir a privacidade do cliente, o processador de pagamento é impedido de vincular uma compra realizada a um *ticket* gerado. Esta propriedade é assegurada pela utilização da variação matemática nos números escolhidos pelo comprador, a qual só é conhecida pelo processador de pagamento em sua forma final que não pode ser relacionada ao seu número de origem.

Colisão na seleção de números

Os conjunto de números enviados aos usuários para a escolha e variação podem ser enviados de forma repetida. Esta definição pode acarretar em colisão na escolha dos números — dois usuários diferentes escolhem o mesmo par de números.

Para mitigar esta possibilidade, o modelo faz uso da mesma técnica utilizada por consagrados métodos criptográficos de chave pública, no qual o conjunto de possibilidades disponíveis para escolha do usuário é grande o suficiente para que a probabilidade de que estes escolham o mesmo número seja mínima. No modelo, testes foram realizados identificando o número necessários de valores a serem disponibilizados para que a chance de colisão seja mínima.

Fabricação de um *ticket*

É possível que um *ticket* válido possa ser fabricado através de um ataque de força bruta, informando uma *string* gerada de forma aleatória à loja virtual.

Este tipo de ação é impedida através da necessidade de conhecimento de um A e B válidos e a validação desses valores através de um *proof-of-work* com um *nounce* válido. É possível que um atacante faça uso do módulo gerador de *tickets* para a fabricação, a fim de facilitar a validação do *nounce*. Entretanto, este tipo de abordagem é desencorajada devido ao tempo gasto utilizado na geração do *nounce*, já que este poderá ser válido para um par de valores não aceitos pelo validador.

Implementação

Para a realização de experimentos foi necessário o desenvolvimento de um protótipo para realizar testes de segurança das funcionalidades do sistema proposto. A implementação contemplou o módulo de geração de *tickets*, utilizado pelo comprador, e o módulo de validação dos *tickets*, presente no sistema de processamento de pagamentos. Os dois módulos foram desenvolvidos usando a linguagem de programação Python 3.3.

O módulo de geração de *tickets* recebe o par de valores selecionados pelo usuário e aplica-os na função m^e mod N do algoritmo RSA. Os valores de e e N são fixados pelo processador de pagamento de forma que sejam co-primos para que o resultado da função seja sempre único. Os valores resultantes da função são utilizados no PoW baseado em Hashcash onde, concatenados a um *nounce*, são submetidos a uma função *hash* SHA-1. O resultado desse *hash* é convertido para a base hexadecimal e tem seus dígitos iniciais analisados a procura de uma quantidade de zeros. Para que o *ticket* seja informado ao usuário, a quantidade de zeros presentes nos dígitos iniciais do resultado do *hash* deverá ser maior ou igual a z. Caso a quantidade não seja suficiente, o processo é reiniciado informando um novo *nounce* até que esse requisito seja atendido. O número de zeros hexadecimais a serem gerados pelo PoW são escolhidos com base na velocidade de criação de *tickets* que se deseja alcançar. Ao fim do processamento, o módulo apresenta ao usuário o *ticket* de pagamento, formado pela concatenação do último *nounce* utilizado e os dois números resultantes da função m^e mod N.

O módulo validador recebe o *ticket* enviado pela loja virtual, identificando se ele foi gerado através do módulo gerador e se o par de valores usados são válidos para a compra. O *ticket* recebido é aplicado a uma função *hash* SHA-1 e tem seu valor resultante convertido para a base hexadecimal. O valor convertido é analisado verificando se a quantidade de zeros aceitos configurados no PoW está correta. Se a quantidade mínima de zeros iniciais for identificada, então o módulo verifica se o par de valores passados está presente no banco de dados de *tickets* válidos. Caso os critérios sejam atendidos, o módulo classifica o *ticket* recebido como válido.

Experimentos

Para analisar a segurança do sistema a respeito de colisões na escolha dos valores enviados aos compradores e a resistência do sistema a ataques de força bruta de fabricação de *tickets* foi necessário implementar novas aplicações.

Para a realização dos testes de colisão e ataques de fabricação através do método de força bruta, foram utilizados três conjuntos de anonimato contendo uma quantidade de 100, 250 e 500 participantes. Além disso, os testes consideraram três quantidades de valores para a geração do *ticket*, sendo eles 1.000, 5.000 e 10.000. Esses valores foram escolhidos pelo autor com o objetivo de validar diferentes proporções na relação usuários e valores, uma vez que não foram encontradas referências abordando o assunto.

Para a análise das colisões na seleção de valores foi implementado um aplicativo capaz de gerar o par de valores pseudoaleatórios para cada usuário do teste, comparando-os à procura de colisões. O experimento fez uso de nove cenários de teste — 2 fatores com 3 níveis cada — no qual 100, 250 e 500 usuários escolhem um par de valores contidos em uma listagem de 1.000, 5.000 e 10.000 valores disponíveis. O número total de colisões geradas para cada uma das replicações foi utilizado como variável de resposta.

Para a avaliação da resistência a um ataque de força bruta foi implementado um aplicativo capaz de gerar aleatoriamente um par de valores pseudoaleatórios, submetê-los no módulo gerador de *tickets* e comparar os valores gerados com

uma listagem de valores aceitos pelo processador de pagamento. A avaliação fez uso de três cenários de teste, nos quais um par de valores é escolhido de forma pseudoaleatória, submetido ao módulo gerador de *tickets* e é comparado a uma listagem de 1.000, 5.000 e 10.000 valores válidos. O número total de *tickets* válidos aceitos pelo processador de pagamento após a ocorrência de 100.000 tentativas foi utilizado como variável de resposta. Um total de 30 replicações foi utilizado para cada nível do fator primário.

Resultados

Nesta seção são apresentados e analisados os resultados provenientes dos experimentos identificados na seção Experimentos, os quais computaram 62 milhões de tentativas de colisão na escolha de valores para variação e 9 milhões de tentativas de fabricação de *tickets* através do modulo gerador de *tickets*. Visando uma melhor compreensão, a análise dos resultados foi dividida em subseções distintas para cada teste realizado.

Colisão na seleção dos valores a serem variados

Inicialmente foram coletados o número total de colisões geradas para cada um dos três grupos de usuários e suas diferentes quantidades de valores disponíveis. Na Tabela 1, são identificados os resultados do teste para cada fator e seus níveis. A coluna "colisões" representa o total de ocorrências em que um par de valores foi escolhido duas ou mais vezes em uma mesma execução do teste.

Tabela 1. Resultados do teste de colisão na escolha dos pares

Usuários	Valores	Repetições	Colisões	% de colisão
100	1.000	499.500	106	0,021 %
250	1.000	499.500	30.245	6,055 %
500	1.000	499.500	110.948	22,212 %
100	5.000	12.497.500	2.092	0,017 %
250	5.000	12.497.500	31.163	0,249 %
500	5.000	12.497.500	124.099	0,99 3%
100	10.000	49.995.000	4.918	0,01 %
250	10.000	49.995.000	30.941	0,062 %
500	10.000	49.995.000	124.346	0,249 %

Através da observação da Tabela 1 é possível perceber o aumento no número de colisões à medida que a quantidade de usuários cresce. Essa característica fica evidente, por exemplo, nos resultados dos níveis de 10 mil valores, os quais a duplicação da quantidade de usuários praticamente quadruplica a taxa de colisões — à medida que 250 usuários geram, aproximadamente, 30 mil colisões, 500 usuários aumentam a ocorrência para, aproximadamente, 124 mil.

Para identificar a relação entre o número de valores disponíveis para a escolha e taxa de colisões, um cálculo de probabilidade foi realizado, conforme apresentado na coluna "% de colisão". O resultado desse cálculo representa a chance de ocorrência de colisão para cada vez que os usuários devem escolher um par de números.

É possível observar que a probabilidade de ocorrência de colisão diminui à medida que mais valores para escolha são adicionados. Essa característica fica clara ao comparar as chances de colisão para 500 usuários, ao qual dispondo de mil valores para a escolha resulta em uma chance de 22% de colisão por rodada, porém o valor é reduzido assim que 5 mil valores são disponibilizados, diminuindo as chances para menos de 1%.

Após a análise dos dados, fica claro que nos dois diferentes fatores testados há um aumento na ocorrência de colisões, conforme a quantidade de usuários cresce. Essa condição independe da quantidade de valores disponíveis para escolha. A análise permite concluir que a proporção mínima adequada deve ser de 1 usuário para 100 valores, para que as chances de colisão fiquem abaixo de 0,01%.

Fabricação de *tickets* através de força bruta

Inicialmente, para a realização do experimento de fabricação através de força bruta, foi

coletado o número total de *tickets* válidos gerados em cada um dos três níveis de valores. Na Tabela 2, são apresentados os resultados dos testes. A coluna "sucessos" identifica a quantidade total de *tickets* de pagamento válidos gerados.

Tabela 2. Resultados do teste de fabricação de *tickets* através de força bruta

Valores Válidos	Repetições	Replicações	Sucessos
1.000	100.000	30	76
5.000	100.000	30	1.859
10.000	100.000	30	7.422

Após a coleta dos dados, os resultados do experimento foram analisados relacionando a quantidade de sucessos na geração dos *tickets* com a quantidade de valores aceitos pelo processador de pagamento. É possível perceber um crescimento da taxa de sucesso de criação de *tickets* válidos a medida que mais valores aceitos são disponibilizados para validação. Esse ponto apresenta uma relação inversa com a quantidade de valores disponíveis comparado aos dados apresentados pelo teste de colisão.

No pior cenário, em que 10 mil valores estão disponíveis para validação, a taxa de fabricação de *tickets* é de 404 tentativas por sucesso. Ao considerar uma implementação do sistema configurado para que a aceitação do PoW exija 6 zeros de validação, um atacante gastará um tempo de 40 horas[1] para obter sucesso na criação de um *ticket*. Todavia, apesar do aumento na taxa de sucesso na fabricação dos *tickets*, em virtude da funcionalidade de expiração dos valores enviados aos usuários, esse indicador não apresenta risco para o sistema caso uma grande quantidade de valores para escolha seja utilizada.

Considerações finais

Neste trabalho, foi elaborado um sistema para realização de transações de comércio eletrônico que assegura a privacidade do comprador durante o processo de pagamento da compra. Ela é garantida através do uso de pseudônimos no momento da compra com a loja virtual e da quebra de relação do *ticket* final utilizado para compra com os itens fornecidos pelo processador de pagamento para a sua geração. Através desses dois elementos, o anonimato da compra é alcançado, garantindo a não vinculabilidade entre uma ou mais compras realizadas através do sistema e as identidades utilizadas para a compra.

Dentre os itens enviados pelo processador de pagamento, o mais sensível é o conjunto de valores para a escolha do comprador, pois ele deve ser encaminhado a diferentes compradores para que o conjunto de anonimato do pagamento não permita ao processador de pagamento identificar qual usuário escolheu qual par de valores. Essa definição pode acarretar em colisão na escolha dos números e para tratar essa possibilidade, o sistema faz uso da mesma técnica utilizada pelos algoritmos criptográficos de chave pública: o conjunto de valores disponíveis para escolha é grande o suficiente para que a probabilidade de colisão seja mínima. No sistema, testes foram realizados identificando a necessidade de proporção de, pelo menos, 1 usuário para cada 100 valores disponíveis, fazendo com que as chances de colisão fiquem abaixo de 0,01%.

Além disso, o sistema é resistente a cenários nos quais um usuário mal-intencionado realize tentativas de fabricação de *tickets* válidos através de força bruta. Sua resistência a este tipo de ação ocorre através do uso do *proof-of-work*, o qual, além de exigir um *nounce* válido para o processamento do *ticket*, torna o processo de fabricação desinteressante a medida que seu processamento fica muito custoso. Mesmo assim, testes foram realizados simulando um cenário de ataque, os quais identificaram que com o poder computacional utilizado no ambiente de teste, mesmo no pior cenário, um atacante não poderia fabricar um *ticket* rápido o suficiente para vencer a expiração dos valores disponibilizados para escolha. Contudo, os tempos de fabricação podem variar de acordo com poder computacional utilizado, sendo possível impactar as questões de segurança do modelo.

Referências

Backstrom, L., Dwork, C., & Kleinberg, J. (2007). Wherefore art thou r3579x?: anonymized social networks, hidden patterns, and structural steganography. *16th international conference on World Wide Web* (pp. 181-190). Banff: ACM.

1 O tempo de fabricação do ticket está diretamente relacionado ao poder computacional utilizado no ambiente de testes, podendo seu tempo de fabricação variar em outros ambientes.

Chaum, D. (1988). The dining cryptographers problem: Unconditional sender and recipient untraceability. *Journal of Cryptology*, 65-75.

Cooper, A., Tschofenig, H., Aboba, B., Peterson, J., Morris, J., Hansen, M., & Smith, R. (2013). *Privacy Considerations for Internet Protocols.* Internet Engineering Task. IETF. Fonte: tools.ietf.org/rfc/rfc6973.txt

Crandall, D., Backstrom, L., Cosley, D., Suri, S., Huttenlocher, D., & Kleinberg, J. (2010). Inferring social ties from geographic coincidences. *National Academy of Sciences* (pp. 22436-22441). National Acad Sciences.

Eichler, S. (2007). Strategies for Pseudonym Changes in Vehicular Ad Hoc Networks depending on Node Mobility. *Intelligent Vehicles Symposium*, 541-546.

Gerlach, M. (2006). Assessing and improving privacy in VANETs. *ESCAR, Embedded Security in Cars.*

Grudzinski, G. (24 de Outubro de 2013). *Do online shoppers care about privacy?* Fonte: InternetRetailer: https://www.internetretailer.com/commentary/2013/10/24/do-online-shoppers-care-about-privacy

ISO 7498-2. (1989). *Information processing systems -- Open Systems Interconnection -- Basic Reference Model -- Part 2: Security Architecture.* International Electrotechnical Commission.

ISO/IEC 15408-2. (2008). *Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 2: Security functional components.* International Electrotechnical Commission.

Jakobsson, M., & Juels, A. (1999). Secure Information Networks. *Proofs of Work and Bread Pudding Protocols(Extended Abstract), 23*, 258-272. (B. Preneel, Ed.) Springer. doi:10.1007/978-0-387-35568-9_18

Konidala, D. M., Dwijaksara, M. H., Kim, K., Lee, D., Lee, B., Kim, D., & Kim, S. (2012). Resuscitating privacy-preserving mobile payment with customer in complete control. *Personal and Ubiquitous Computing, 16*, 643-654.

Laurie, B., & Clayton, R. (2004). "Proof-of-Work" proves not to work; version 0.2. *Workshop on Economics and Information, Security.* Fonte: www.cl.cam.ac.uk/~rnc1/proofwork2.pdf

Nakanishi, T., & Sugiyama, Y. (2005). An efficient on-line electronic cash with unlinkable exact payments. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 88*, 2769-2777.

Narayanan, A., & Shmatikov, V. (2008). Robust de-anonymization of large sparse datasets. *IEEE Symposium on Security and Privacy* (pp. 111-125). IEEE.

Pfitzmann, A., & Hansen, M. (2010). A terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management. Fonte: dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.34.pdf

Pfitzmann, B., & Waidner, M. (1992). How to break and repair a "provably secure" untraceable payment system. *Advances in Cryptology* (pp. 338-350). Springer.

Puzis, R., Yagil, D., Elovici, Y., & Braha, D. (2009). Collaborative attack on Internet users' anonymity. *Internet Research, 19*(1), 60-77.

Rao, J. R., & Rohatgi, P. (2000). Can pseudonymity really guarantee privacy? *USENIX Security Symposium* (pp. 85-96). Denver: USENIX Association.

Rennhard, M., Rafaeli, S., Mathy, L., Plattner, B., & Hutchison, D. (2004). Towards pseudonymous e-commerce. *Electronic Commerce Research, 4*, 83-111.

Shirey, R. (2007). *Internet Security Glossary, Version 2.* Internet Engineering Task Force. IETF. Fonte: tools.ietf.org/rfc/rfc4949.txt

Souza, E. A. (13 de Novembro de 2013). *A privacidade como diferencial.* Fonte: MidiaNews: http://www.midianews.com.br/conteudo.php?sid=262&cid=179125

Spiegel, D. (15 de Stembro de 2013). *'Follow the Money': NSA Spies on International Payments.* Fonte: Spiegel Online: http://www.spiegel.de/international/world/spiegel-exclusive-nsa-spies-on-international-bank-transactions-a-922276.html

Thomasso, E. (15 de Novembro de 2013). *Big Retailer is watching you: stores seek to match online savvy.* Fonte: Reuters: http://www.reuters.com/article/2013/11/15/net-us-retail-tracking-idUSBRE9AE05R20131115

Abstract

The exposure of customer's data can lead to profile mapping and unpleasant situations depending on the nature of the goods purchased. To solve this problem, a system to execute e-commerce transactions assuring the privacy of the customer is implemented. Through it, the customer is assured that the privacy of your information is secured toward the other entities involved in the process. The system uses a model with three entities — customer, shop and payment processor — which none of them can associate the purchase to the buyer. Experiments were conducted to evaluate the security of the model regarding collisions in legitimate tickets generation and its resistance to fabrications attacks. An increase is noticed in the occurrence of collisions as the number of users grows, indicating that the proportion of users and amounts available for the generation of the tickets should be 1 to 100, respectively, reducing the chances of collision to 0.1 %. The same occurs in the experiment of fabrication: as more values are accepted, the higher the success rate.
Keywords: Privacy, E-commerce, RSA.