Uma Análise Formal Automatizada dos Protocolos de Envio e Confirmação de Processamento da Nota Fiscal Eletrônica Brasileira

Jean Everson Martina[1]*, **Luiz Augusto Chaves Boal**[2]

[1] University of Cambridge
Computer Laboratory
William Gates Building
15 JJ Thomson Avenue
Cambridge – CB3 0FD – United Kingdom

[2]DF-e Tecnologia
Florianópolis
Santa Catarina - Brazil

Jean.Martina@cl.cam.ac.uk,luizboal@dfe.com.br

Abstract. *The Brazilian Electronic Bill of Sale(NF-e) is a taxing legislation that establishes an electronic system to replace the actual paper-based goods taxing system. It is used to declare to the government operations related with buying and selling goods between companies in real time, replacing the actual paperwork. This paper aims to formalise and analise the message exchange protocols established by the legislation. We formalise the messages of sending and confirmation sub-protocols, then we use a consolidated method to automatically analise security protocols. A conceptual problem is found. We then evaluate the impact and propose modifications in the protocols to avoid this problem.*

Resumo. *A Nota Fiscal Eletrônica Nacional(NF-e) é uma legislação tributária que institui a versão digital da nota fiscal modelo 1/1-A, usada principalmente para declarar operações de venda de mercadorias entre empresas em tempo real, substituindo o documento fiscal impresso. Este artigo formaliza e analisa os protocolos de envio e confirmação de processamento. Fizemos uma formalização das mensagens em cada sub-protocolo e então usamos um método consolidado para análise automatizada de protocolos de segurança. Do problema encontrado, avaliamos o impacto e sugerimos modificações aos protocolos da NF-e para torná-los resistentes ao ataque encontrado.*

1. Introdução

Cada vez mais governo e iniciativa privada vêm buscando alternativas para reduzir custos operacionais e aumentar a eficiência na realização de processos e rotinas de trabalho. A modernização do relacionamento tributário entre governo e contribuintes deixou de ser uma tendência e passou à realidade com o advento da Nota Fiscal Eletrônica (NF-e): ”É o primeiro sistema de informação governamental que integra as esferas federal

*Bolsista CAPES - Processo BEX #4226-05-4

e estadual, e através da interoperabilidade entre seus sistemas de informação e o dos contribuintes"[SRF 2007].

É sem duvida uma mudança de paradigma que estabelece um novo modelo de confiança entre fornecedor (emitente do documento fiscal), comprador (destinatário) e Administração Tributária Estadual, anteriormente fundamentado na nota fiscal impressa (papel). Tal mudança se reflete na forma como a autoria e integridade da nota fiscal são garantidas e verificadas pelas partes, além de sua manipulação e armazenamento seguro. Implica naturalmente na adaptação dos processos de trabalho e sua informatização por parte dos contribuintes. Também implica na segurança do ambiente corporativo e de tecnologia de informação relacionada ao novo processo.

Isto significa uma mudança muito maior do que os habituais sites de serviços oferecidos pelo governo, pois os sistemas de informação dos contribuintes interoperam diretamente com os portais estaduais (e seus web services), sem qualquer intervenção humana. Para viabilizar esse processo jurídica e eletronicamente, utiliza-se a assinatura digital como recurso para garantia da autoria e integridade das notas fiscais eletrônicas e demais documentos fiscais eletrônicos. A adoção deste método dá-se pelo esforço governamental em fomentar o uso de certificação digital baseada no modelo de Infra-estrutura de Chaves Públicas X.509 e seu sistema governamental brasileiro, chamado ICP-Brasil[Presidência da República 2001].

Tem-se uma mudança de paradigma em vários sentidos, mas principalmente no modelo de confiança entre as partes envolvidas (emitente, destinatário e Administração Tributária). Este modelo era calcado na nota fiscal impressa, na sua autorização prévia (AIDF), na sua manipulação e conferência física. Este modelo de confiança foi completamente substituído, assim como o papel.

Historicamente o sistema de escrituração fiscal é alvo constante de fraudes visando a sonegação de impostos para aumento de lucros e concorrência desleal. "Com o advento da nota fiscal eletrônica e da implantação de um cenário totalmente digital entre empresas e Administrações Tributárias as possibilidades de fraudes não se limitam ao mundo físico, elas estendem-se ao cenário eletrônico também." [Gorges 2006]

Este trabalho tem como objetivo analisar formalmente os protocolos da NF-e do ponto de vista do emitente na perspectiva do uso do documento fiscal eletrônico assinado digitalmente e sua confiabilidade para as partes, restringindo sua utilização apenas para a operação fiscal de comercialização de mercadorias e serviços, ou seja: fornecedor (emitente) comercializa para comprador (destinatário). Todas as informações foram obtidas na versão 2.02 do Manual de Integração Contribuintes[Projeto NF-e 2007], documento disponível nos sites dos governos estaduais e federal, o qual descreve a comunicação e interoperabilidade dos sistemas governamentais e privados no âmbito da NF-e.

A NF-e brasileira não é pioneira, os precursores na emissão de documentos fiscais eletrônicos em tempo real são Chile [Servicio de Impuestos Internos - Chile 2003] e México [Secretaría de Hacienda y Crédito Público México 2008]. Outras iniciativas, não se assemelham a NF-e brasileira, em virtude de não serem on-line e em tempo real.

Este artigo também tem como objetivo secundário descrever os protocolos do sistema de emissão e controle da nota fiscal eletrônica usando um formato amplamente aceito pela comunidade científica para tal fim, o qual foi inicialmente proposto por

Needham-Schroeder[Needham and Schroeder 1978]. A descrição dos protocolos desta forma tem como objetivo propiciar a análise usando uma notação menos ambígua - diferente da atual em linguagem natural - e que habilite a tradução simplificada para as ferramentas de verificação de protocolos hoje existentes e amplamente utilizadas, tais como validadores de modelos e provadores de teoremas. A profundidade da tradução semântica foi a necessária para provar nossos objetivos.

O modelo formal empregado neste artigo foi proposto por Weidenbach [Weidenbach 1999], consistindo na formalização das mensagens usando um conjunto de modelos indutivos em um sistema de lógica de primeira ordem. O uso desta técnica aliada aos provadores automáticos de teoremas, tais como o SPASS[Weidenbach et al. 2002], nos permite fazer buscas no espaço de execução dos protocolos, buscando assim por conjecturas sobre a validade dos objetivos de segurança dos mesmos.

Outro ponto importante é quanto ao modelo de atacante dos protocolos. O modelo seguido é o sugerido por Dolev-Yao[Dolev and Yao 1983], no qual o atacante, além de poder analisar todo o tráfego em aberto das comunicações dos protocolos, pode desmontar as mensagens em seus componentes atômicos - quando de posse das chaves necessárias também pode reverter os processos criptográficos - remontar mensagens válidas a partir destes componenetes, e repetir mensagens no meio de comunicação. Em extensões ao modelo inicial de Dolev e Yao, o atacante também pode atuar com consentimento de uma parte interna, o que sugere por exemplo a exposição proposital de chaves criptográficas e o deliberado ato para o corrompimento do(s) protocolo(s) pelas partes.

É importante frisar que apesar do uso massivo de tecnologias de tunelamento e autenticação tais como o SSL/TLS, o protocolo da NF-e tem pouca ou nenhuma preocupação quanto a atacantes mais bem posicionados no sistema, inclusive de participantes corruptos e organizações bem fundadas. Este ponto deve ser levado em consideração, pois o atual cenário de perigo ao qual as organizações são submetidas todos os dias na Internet é muito grande. Ameaças como golpes através de correio eletrônico (phishing scams) e cavalos de tróia são uma realidade constante. Mesmo um usuário bem instruído pode ser enganado por tais técnicas, deixando suas chaves criptográficas (privadas) com as respectivas senhas de acesso, serem copiadas por um atacante. Devemos levar em consideração que mesmo o modelo Dolev-Yao estendido não leva em consideração primitivas criptográficas falhas, probabilidades e resultados assintóticos.

Para tratar o problema da análise formal dos protocolos da NF-e brasileira, o presente artigo inicia com esta introdução. Avançando descrevemos os protocolos com a notação Needham-Schroeder e seus objetivos de segurança na seção 2. Na seção 3 apresentamos a modelagem lógica do modelo Needham-Schroeder para a implementação proposta por Weidenbach, assim como a descrição do atacante com as capacidades propostas por Dolev-Yao e um fato que comprova um problema teórico com implicações práticas nos protocolos. Na seção 4 comentamos a análise formal dos protocolos e o impacto dos problemas encontrados. Na seção 5 sugerimos contra-medidas para assegurar que os protocolos não sejam vulneráveis aos problemas encontrados e na seção 6 apresentamos as considerações finais quanto a esta análise inicial dos protocolos da NF-e.

2. Descrição dos Protocolos da NF-e

A NF-e é um conjunto de protocolos e práticas que interopera os sistemas de informação dos contribuinte e das Administrações Tributárias de uma forma digital, para substituir o modelo tradicional em papel. Estes protocolos e práticas são descritos no manual de Integração - Contribuinte[Projeto NF-e 2007], documento disponível nos sites dos órgãos de governo relacionados ao processo fiscal. Deve-se frisar que os protocolos são sempre descritos textualmente, e seu texto é escrito na perspectiva do Governo, e não do contribuinte. Desta forma o Manual de Integração - Contribuinte cita ”recepção”de documentos, enquanto no ponto de vista do contribuinte, o que ocorre é a ”transmissão”.

Encontramos dois tipos de protocolos presentes na descrição do Manual de Integração - Contribuinte, os síncronos e assíncronos. Os protocolos do sistema de NF-e são síncronos, ou seja terminam com respostas afirmativas ou negativas na mesma conexão, com exceção dos web services de Recepção e Retorno de Recepção, escolhidos para escopo deste trabalho. Os protocolos foram projetados para serem assíncronos para otimização de desempenho dos sistemas de informação das Administrações Tributárias.

Na tradução do documento Manual de Integração - Contribuinte para o modelo Needham-Schroeder foram utilizados sempre as opções mais complexas de execução dos sub-protocolos, ou seja, as que contêm mais de uma Administração Tributária e outros órgãos fiscalizadores regionais. Isto foi feito para enriquecer o processo de verificação dos protocolos na seção 3. Ainda na questão da complexidade, foi optado por não se representar a estrutura semântica interna da NF-e, pois ela não nos fornece detalhes necessários para uma análise inicial dos protocolos. A expansão do modelo para incluir estes detalhes semânticos, com certeza enriqueceria o modelo, e será implementado num momento posterior. Para a provas iniciais de segurança dos protocolos, um modelo semântico simplificado se mostrou suficiente.

A descrição Needham-Schroeder dos sub-protocolos usa cifragens assimétricas para garantir o sigilo e a integridade das mensagens durante sua transmissão, simulando assim o SSL/TLS sendo utilizado na NF-e. Esta simplificação visa dar a garantia de sigilo dos protocolos SSL/TLS, os quais já tiveram suas propriedades provadas formalmente usando um método indutivo similar ao utilizado neste trabalho desenvolvido por Paulson e Bella[Paulson 1999b, Paulson 1999a]. A propriedade de autenticidade e não repúdio, por características intrínsecas dos protocolos da NF-e, são garantidas pelas assinaturas digitais em cada uma das NF-e e requisições solicitadas aos web services dos sistemas de TI das Administrações Tributárias utilizando-se uma autenticação SSL no cliente.

Uma outra característica importante da representação dos protocolos da NF-e usando o modelo Needham-Schroeder e posteriormente a modelagem formal neste trabalho é a representação do emitente e do transmissor da NF-e como sendo o mesmo ator nos protocolos. A inclusão deste detalhe não resultaria em mais informações relevantes neste momento para a avaliação dos sub-protocolos. Ainda na representação dos sub-protocolos, chamados pela legislação de web services, optou-se por representar inicialmente o núcleo dos protocolos da NF-e que são suficientes para provar os problemas de interesse deste artigo. A ampliação deste modelo é um trabalho conseqüente desta avaliação inicial, mas que demandará tempo e recursos não disponíveis neste momento. Também por motivos de espaço, optou-se por não incluir a descrição e formalização dos sub-protocolos (web services) de Cancelamento, Inutilização e Consultas, os quais já fo-

ram modelados, formalizados e fizeram parte do modelo testado, mas desnecessários para provar os problemas descritos na seção 4.

A seguir nas sub-seções 2.1 e 2.2 veremos a descrição dos protocolos usando o modelo Needham-Schroeder, ao invés da linguagem natural (textual) utilizada.

2.1. Recepção

O protocolo relativo ao web service de Recepção - transmissão no ponto de vista do contribuinte - é responsável pelo processo de emissão de notas fiscais eletrônicas por parte do contribuinte: o fornecedor, na operação de venda de mercadorias e/ou serviços, envia as NF-e referentes à operação fiscal para a Administração Tributária Estadual de origem na qual está inscrito, ou seja, aquela da Unidade da Federação que emitiu seu CNPJ, ou onde sua Inscrição Estadual está vinculada.

As mensagens são simplificadas, retratando nesta tradução unicamente os modelos semânticos significativos aos protocolos de segurança, ou seja: a inclusão do parâmetro de mensagem "Header"é a representação de todos estes dados que fazem parte das mensagens, mas não tem valor semântico para a segurança do mesmo ou foi optado por não incluí-los nesta modelagem.

Os itens que fazem parte do campo Header e estão presentes na descrição feito no documento base[Projeto NF-e 2007] são:

- versao - Versão do leiaute da NF-e.
- tpAmb - Identificação do Ambiente: Produção ou Homologação.
- verAplic - Versão do Aplicativo que recebeu o Lote.
- cStat - Código do status da resposta.
- xMotivo - Descrição literal do status da resposta.
- cUF - Código da Unidade da Federação que atendeu a solicitação.
- infRec - Dados do Recibo do Lote (Só é gerado se o Lote for aceito).
- tMed - Tempo médio de resposta do serviço (em segundos) dos últimos 5 minutos.

Ainda como parte das mensagens do protocolo de transmissão, tem-se os seguintes componentes:

- NFe - Documento XML representando a NF-e, assinado posteriormente pela chave privada do contribuinte para conferir a sua autenticidade.
- idLote - Identificador único de controle do envio do lote. A responsabilidade de gerar e controlar esse número é exclusiva do contribuinte.
- nRec - Número do Recibo gerado pelo Portal SEFAZ, composto por: Código da UF onde foi entregue e treze posições numéricas seqüenciais.
- dhRecbto - Data e Hora do Recebimento do lote de NF-e no Formato = AAAA-MM-DD-HH:MM:SS com data e hora da gravação no Banco de Dados em caso de confirmação.

O protocolo do web service de recepção de NF-e por parte da Administração Tributária Estadual é descrito abaixo com a seguinte representação:

1. $EMIS \longrightarrow SEFAZ : \{Header, IdLote, \{|NFe_1|\}_{Kr_{EMIS}} \cdots \{|NFe_{50}|\}_{Kr_{EMIS}}\}_{Ku_{SEFAZ}}$
2. $SEFAZ \longrightarrow EMIS : \{Header, IdLote, nRec, dhRecbto\}_{Ku_{EMIS}}$

Na mensagem 1, o emitente ($EMISS$) após gerar o fato fiscal e fazer a sua declaração através da geração em seus sistemas de TI dos respectivos documentos fiscais, assina cada um dos documentos denominados NFe_x. Estes documentos são as declarações fiscais assinadas com a chave privada do detentor do certificado digital emitido para tal fim e especificado no manual de integração do contribuinte. O envio das NF-e é realizado em lotes à Secretaria da Fazenda (SEFAZ) da unidade federativa a qual o emitente possui sua inscrição.

Após ter preparado um lote com tamanho variável de 1 (uma) a 50 (cinqüenta) NF-e, cujo tamanho não pode exceder a 500Kb, o contribuinte gera um lote de NF-e para transmissão, o qual é então enviado através de um túnel SSL, aqui representado por uma cifragem assimétrica usando a chave pública do destinatário, neste caso sendo $SEFAZ$. Nota-se aqui a criação de um identificador chamado $IdLote$, o qual deveria atuar como um Nonce, no controle da sessão sendo executada e posteriormente na recuperação dos dados no protocolo de Retorno de Recepção, mas no Manual de Integração do Contribuinte, este número é estabelecido como auto-incremental e seqüencial. Deve-se atentar que segundo as regras de negócio presentes no Manual, a seqüencialidade e auto incremento não são checados para permitir assim a paralelização do processo.

Uma vez tendo recebido esta mensagem, o sistema de TI da Administração Tributária Estadual responde ao contribuinte emitindo, conforme a mensagem 2, um número de recibo($nRec$) , um carimbo de tempo não assinado ($dhRecbto$), e o cabeçalho informando dados do processamento que virá a ocorrer. O contribuinte emitente do lote de NF-e utilizará o número do recibo para consultar o resultado do processamento do lote e averiguar se as NF-e foram autorizadas pela Administração Tributária Estadual.

2.2. Retorno de Recepção

O protocolo apresentado é a continuação da recepção, ocorrida após o término do processamento em lote feito pela Administração Tributária Estadual do emitente da(s) NF-e(s). O emitente da(s) NF-e(s) previamente enviada(s) transmite nova mensagem, contendo o número do recibo do lote fornecido no passo anterior pela Administração Tributária.

Desta forma o contribuinte emitente verifica se as NF-e possuem status de autorizadas (sucesso), rejeitadas (problemas técnicos) ou denegadas (problemas tributários).

1. $EMIS \longrightarrow SEFAZ : \{Header, nRec\}_{Ku_{SEFAZ}}$
2. $SEFAZ \longrightarrow EMIS : \{Header, nRec, \{Header, chNFe, dhRecbto, nProt, digVal\}_1 ... \{Header, chNFe, dhRecbto, nProt, digVal\}_{50}\}_{Ku_{EMIS}}$

Na mensagem 1, o emitente conecta-se a SEFAZ normalmente após o período estipulado por $tMed$. Desta forma ele aumenta a probabilidade de seu processamento já ter ocorrido, mas o protocolo não sugere necessariamente este encadeamento. Nesta mensagem, além de cabeçalhos com valor semântico desprezível neste momento, ele envia também o número do recibo ($nRec$), relacionando esta execução com o subprotocolo apresentado na seção 2.1. A mensagem é então cifrada com a chave pública da Administração Tributária Estadual, conferindo assim sigilo à mensagem.

Seguindo a execução do protocolos, caso o lote de NF-e tenha sido devidamente processado, a SEFAZ envia ao emitente da NF-e um lote de NF-e processadas, de acordo com a descrição da mensagem 2. Nesta mensagem são incluídos um Header com detalhes

do ambiente de execução, o número do recibo enviado na mensagem 1, e os resultados de processamento individuais de cada NF-e para o emitente. Cada uma das NF-e autorizadas, rejeitadas ou denegadas, possui um Header com informações do tipo de ambiente, uma chave de acesso ($chNFe$) a qual permitirá o destinatário da NF-e ou os entes fiscalizadores consultarem sua validade no sistema da SEFAZ, um carimbo de tempo não assinado ($dhRecbto$), um número de protocolo ($nProt$), e o valor de uma função de resumo criptográfico sobre a mensagem original ($digVal$).

Deve-se atentar que mesmo a mensagem 2 sendo transmitida de forma sigilosa ao emitente através da cifragem com sua chave pública (emulando a propriedade do SSL/TLS), a não obrigatoriedade de assinatura da NF-e por parte da SEFAZ e a não utilização de um carimbo de tempo assinado, mesmo assumindo a fé pública do sistema fazendário, não exime a existência de problemas de confiança entre outras partes presentes em outros sub-protocolos, tais como o destinatário, que é solidário aos problemas fiscais do emitente segundo a legislação vigente.

3. Formalização dos Protocolos da NF-e

O processo de formalização dos sub-protocolos da NF-e segue o modelo proposto por Weidenbach, e utiliza um modelo lógico de primeira ordem com uma descrição de atacante seguindo um modelo Dolev-Yao extendido. A avaliação dos objetivos dos protocolos e seus possíveis problemas, aqui representados por conjecturas lógicas, é automatizado utilizando um provador automático de teoremas, neste caso: SPASS[Weidenbach et al. 2002].

A representação lógica dos protocolos consiste em descrever e formalizar o conjunto de mensagens M que são enviadas durante uma execução dos protocolos potencialmente infinita e paralela. O uso de um modelo lógico indutivo nos capacita a tal. Aliado ao uso de uma lógica Horn monádica de primeira ordem, que graças a sua redutividade e decidibilidade, nos permite o uso de um provador automático de teoremas para provar conjecturas quanto à segurança dos protocolos nela descritos.

A formalização consiste no uso de predicados, funções e constantes em conjunto com os símbolos normalmente usados em notações de lógica de primeira ordem, tais como os operadores de negação ($\neg$), conjunção ($\wedge$), disjunção ($\vee$), implicação ($\supset$) e os quantificadores universal ($\forall$) e existencial ($\exists$).

3.1. Modelo Lógico

A formalização dos protocolos da NF-e, já representados nas seções 2.1 e 2.2, é implementada usando uma tradução do modelo descrito e posteriormente é testado no SPASS. Optou-se por modelar os dois sub-protocolos de forma conjunta para melhorar a expressividade das conjecturas que gostaríamos de provar, e também pelo fato que os dois sub-protocolos nada mais são que as duas partes de um mesmo protocolo assíncrono.

No decorrer da descrição da implementação faremos a introdução dos símbolos necessários (predicados, funções e constantes) onde eles primeiramente aparecerem:

1. $P(e)$
2. $Knows(kp(krkey(kre, e), kukey(cere, e)), e)$
3. $Knows(kukey(cerf, f), e)$

4. $P(f)$
5. $Knows(kp(krkey(krf, f), kukey(cerf, f)), f)$
6. $Knows(kukey(cere, e), f)$

Inicialmente estabelecemos os atores e e f - neste exemplo Emissor e Fazenda respectivamente - aqui representados por constantes, usando o predicado $P()$ (fórmulas 1 e 4). Após, damos o conhecimento inicial aos atores, adicionando ao predicado $Knows()$ os seus respectivos pares de chave assimétricas e a chave pública da outra parte do protocolo (fórmulas 2, 3, 5 e 6).

Na fórmula 2, introduzimos as funções $kp()$, $kukey()$ e $krkey()$, as quais denotam respectivamente um par de chaves, e suas componentes públicas e privadas. Também temos a inclusão das constantes kre, a chave privada do ator e, $cere$, o certificado da chave pública do ator e, krf, a chave privada do ator f, e $cerf$, o certificado da chave pública do ator f.

7. $\forall U, V[$
   $Knows(kukey(cerf, f), U) \wedge Knows(kp(krkey(kre, e), kukey(cere, e)), U)) \supset$
   $M(sent(U, f, encr(triple(header, idLote, sign(V, kre)), cerf))) \wedge$
   $Stores(triple(header, idLote, sign(V, kre)), U) \wedge Ff(idLote)]$

A partir da fórmula 7, começamos de fato a modelagem dos protocolos. Nesta fórmula, definimos como precondições para o envio da primeira mensagem, que o ator representado pela variável U conheça o certificado de f, e que possua um par de chaves de um emissor de NF-e. Ao cumprirmos estas condições temos a implicação, que é o envio da mensagem 1 da seção 2.1. Também adicionamos o conteúdo desta mensagem ao banco de conhecimento do ator que a enviou. Por fim afirmamos que este lote de NF-e é um lote não enviado anteriormente.

Os novos símbolos introduzidos na fórmula 7 são: os predicados $M()$, para todas as mensagens enviadas pelo protocolo, $Stores()$, para todas a informações enviadas por um ator especifico e $Ff()$, para todos os componentes ainda não vistos por f. As funções: $sent()$, que nos dá a direção na qual uma determinada mensagem foi enviada (por ex. de $A \longrightarrow B$); $encr()$, que determinado termo foi cifrado; $sign()$, que determinado termo foi assinado com uma chave privada, e $triple()$, que é uma função para termos compostos de 3 elementos. As constantes $header$ e $idLote$, que são ambas partes semânticas resumidas do protocolos. Por fim temos as variáveis U e V, que representam todos os atores ($\forall$) e todas as NF-e respectivamente.

8. $\forall U, V, W, X, Y[$
   $Knows(kukey(cere, e), f) \wedge Knows(kp(krkey(krf, f), kukey(cerf, f)), f) \wedge$
   $Ff(V) \wedge M(sent(U, f, encr(triple(header, V, sign(Y, kre)), cerf)))) \supset$
   $M(sent(f, U, encr(triple(header, W, X), cere))) \wedge$
   $Stores(triple(header, W, X), f) \wedge Knows(nfe(W, Y), U) \wedge Knows(nfe(W, X), U)]$

A fórmula 8, tem como pré-condições que o ator f possua seu par de chaves, assim como conheça a chave pública do emitente, além de reconhecer o lote de NF-e como sido emitido anteriormente e que a fórmula 7 tenha efetivamente ocorrido. Ao satisfazermos as condições temos a geração da mensagem 2 da seção 2.1 e o seu armazenamento no banco de conhecimento do ator f. Nesta fórmula temos as variáveis U, que é o ator que iniciou a comunicação; V, que é o identificador do lote; W, que é o número do recibo emitido por f; X, que é o carimbo de tempo e Y que representa as NF-e emitidas.

9. $\forall U, V[$
$Knows(nfe(U, dhRcbt), V) \supset$
$M(sent(V, f, encr(pair(header, U), cerf))) \wedge Stores(pair(header, U), V)]$

Prosseguindo, a fórmula 9, que representa a mensagem 1 da seção 2.2. Nela temos como precondições que o ator representado pela variável V possua o número de recibo da NF-e emitido na fórmula 8 , aqui representado pela variável U. De posse destes dados, ele envia a mensagem, e armazena os dados enviados em sua base de conhecimento.

10. $\forall U, V, W, X, Z, X1, X2, X3[$
$Stores(triple(U, V, W), f) \wedge Knows(kukey(cere, X), f)) \supset$
$M(sent(f, X, encr(triple(header, V, pair(pair(Z, X1), triple(W, X2, X3))), cere)))$
$\wedge Stores(triple(header, V, pair(pair(Z, X1), triple(W, X2, X3))), f) \wedge$
$Knows(nfe(V, X1), X) \wedge Knows(nfe(V, X2), X) \wedge Knows(nfe(V, X3), X)]$]

Finalizando temos a fórmula 10, que possui como precondições que o ator f tenha em seu armazenamento local os dados da mensagem 2 da seção 2.1 e conheça a chave pública do ator e. Com as precondições satisfeitas, adicionamos ao predicado $M()$ a mensagem 2 da seção 2.2, guardamos seus dados na base de conhecimento do ator f e damos as informações sobre a emissão da NF-e ao ator que estamos nos comunicando.

As variáveis U,V,W,X,Z,$X1$,$X2$ e $X3$ são respectivamente, todos os possíveis cabeçalhos recebidos, todos os possíveis recibos, todos os possíveis carimbos de tempo, todos os possíveis atores, todos os possíveis cabeçalhos gerados, todas as possíveis chaves de acesso, todos os possíveis números de protocolo e todos os possíveis resumos criptográficos das NF-e.

3.2. Testes sobre o Modelo

O primeiro passo no modelo previamente descrito é testá-lo quanto a sua redutividade e a manutenção das características propostas pela Logica Horn Monádica de Primeira Ordem[1]. Temos o Fato 1:

Fato 1 Saturação do Modelo

Ao executarmos as fórmulas de 1 a 10 sem conjecturas temos a saturação do modelo, o que indica a manutenção das características desejadas no modelo.

Após garantirmos as características que nos darão a decidibilidade dos problemas, partimos para um teste semântico do protocolo formalizado. Um emitente deve ser capaz de emitir uma determinada NF-e usando o protocolo. Isto é provado pelo fato 2.

Fato 2 $\exists U[Knows(nfe(U, NFe1), e) \wedge Knows(nfe(U, chnfe), e)]$

Este fato nos mostra um traço que é a execução do protocolo com as garantias formalizadas. É importante atentar que se o modelo não é capaz de provar a realização de seus objetivos, tais como o dos protocolos reais, normalmente aconteceram problemas na tradução do modelo AD-HOC para a especificação formal, pois o mesmo não finaliza uma execução com sucesso.

[1]O artigo não mostra resultados da execução do provador de teoremas SPASS, em virtude de seu tamanho (aproximadamente 50 linhas por prova)

3.3. Modelo do Atacante

O atacante é modelado tendo como base o sugerido por Weidenbach[Weidenbach 1999], pois o atacante por ele descrito tem as capacidades para representar um ataque real, em um ambiente tão hostil quanto a Internet, salvo as limitações do modelo Dolev-Yao, perante os protocolos da NF-e. As fórmulas são:

11. $Knows(kukey(cerf, f), i)$
12. $Knows(kukey(cere, e), i)$
13. $\forall U, V, W[M(sent(U, V, W)) \supset Im(W)]$
14. $\forall U, V[Im(pair(U, V)) \supset Im(U) \wedge Im(V)]$
15. $\forall U, V, W[Im(triple(U, V, W)) \supset Im(U) \wedge Im(V) \wedge Im(W)]$

Primeiramente são dadas as informações de conhecimento público ao atacante (11 e 12). Atribui-se então ao atacante a capacidade de coleta de quaisquer mensagens que forem enviadas por atores participantes nos protocolos (fórmula 13). Após fazemos a decomposição atômica de quaisquer mensagens compostas recebidas e adicionamos ao predicado Im (Fórmulas 14 e 15) o qual representa o conhecimento adquirido pelo atacante I pela coleta de mensagens.

16. $\forall U, V[Im(U) \wedge Im(V)) \supset Im(pair(U, V))]$
17. $\forall U, V, W[Im(U) \wedge Im(V) \wedge Im(W) \supset Im(triple(U, V, W))]$
18. $\forall U, V, W[Im(U) \wedge P(V) \wedge P(W) \supset M(sent(V, W, U))]$

A partir do conhecimento adquirido pela coleta e decomposição de mensagens anteriores, nas fórmulas 16 e 17, atribui-se ao atacante a capacidade de composição arbitrária de seu conhecimento para a geração de mensagens e o conseqüente envio (adição a M), o que é possível através da fórmula 18. Esta apresenta que para todas as mensagens passíveis de serem produzidas por I pelo seu conhecimento prévio, adquirido ou processado, ele possa enviá-las na execução dos protocolos.

19. $\forall U, V, W[Im(V) \wedge P(W) \supset Knows(krkey(V, W), i)]$
20. $\forall U, V, W[Im(U) \wedge Knows(kukey(V, W), i) \wedge P(W) \supset Im(encr(U, V))]$
21. $\forall U, V, W[Im(U) \wedge Knows(krkey(V, W), i) \wedge P(W) \supset Im(sign(U, V))]$

Por fim, na fórmula 19 atribui-se ao atacante I as capacidades de análise criptográfica, onde ele pode aprender qualquer chave transmitida nos protocolos e associá-la a um ator que executa o mesmo, além de poder também compor todas as possíveis mensagens cifradas e assinadas com as chaves em seu conhecimento (fórmulas 20 e 21).

22. $\forall U, V, W[Im(encr(U, V)) \wedge Knows(krkey(V, W), i) \wedge P(W) \supset Im(U)]$

Uma extensão proposta ao modelo de Weidenbach é a adição de uma fórmula que permita ao atacante aprender o conteúdo de mensagens as quais ele tem conhecimento da chave que decifra os componentes cifrados. Isso é representando na fórmula 22

A execução do modelo formal sem conjecturas novamente leva a sua saturação, garantindo assim as caraterísticas da Logica Horn de Primeira Ordem. Devemos no entanto atentar que mesmo o modelo sendo saturado e assim considerado finito, temos casos de execução potencialmente infinitos sendo analisados, conforme as fórmulas 16 e 17 demonstram.

Ao testarmos a seguinte conjectura, obtemos um novo fato por saturação:

Conjectura 3 $\exists U[Knows(nfe(U, NFe1), i) \wedge Knows(nfe(U, chnfe), i)]$

A conjectura 3 não se transforma em fato, sua inclusão unicamente nos leva à saturação do modelo. É esperado, pois o atacante não deve ser capaz de emitir NF-e sem acesso a uma chave privada de um emissor autorizado. O fato do modelo estar saturado e a conjectura não ser provada, indica a sua refutação, a qual é a conclusão esperada.

3.4. Objetivos e Conjecturas Formais

Os objetivos iniciais dos protocolos, como o término das execuções do modelo e o não aprendizado por parte do atacante de chaves durante a execução foram testados através da saturação do modelo sem conjecturas, e através de conjecturas simples, onde se provou o não aprendizado por parte do atacante de chaves somente pela execução.

Ao introduzirmos conjecturas mais elaboradas, explorando o comprometimento de atores dos protocolos, temos que, se não utilizarmos o método de consulta exaustivamente buscando todo o intervalo possível de NF-e não emitidas e com numeração consistente a cada execução do sub-protocolo de recepção, consegue-se provar os seguintes fatos:

Fato 4 $\exists U[Knows(kp(krkey(kre, e), kukey(cere, e)), i) \supset$
$Knows(nfe(U, NFe1), i) \wedge Knows(nfe(U, chnfe), i)]$

O Fato 4, mesmo trivial, demonstra que caso um atacante tenha acesso à chave privada de um emitente de NF-e, é capaz de fazer a emissão de uma nota fiscal em nome do emitente. Este fato é esperado uma vez que a segurança do protocolo se baseia na segurança das chaves privadas relacionadas aos certificados dos emitentes de NF-e. O seu comprometimento mostra exatamente um cenário possível em termos práticos.

Fato 5 $\forall U[Knows(kp(krkey(kre, e), kukey(cere, e)), i) \supset$
$Knows(nfe(U, NFe1), i) \wedge Knows(nfe(U, chnfe), i)) \wedge$
$\neg(Knows(nfe(U, NFe1), e) \wedge Knows(nfe(U, chnfe), e))]$

O Fato 5 representa que, se um atacante tem acesso à chave privada de um emitente de NF-e, o emitente não é capaz de detectar o uso desta chave por outra pessoa. Isto é um falha conceitual dos protocolos.

O modelo de atacante utilizado pelos desenvolvedores não leva em conta um atacante com as capacidades necessárias - Dolev-Yao extendido - o que é essencial para um sistema de informação em execução num ambiente tão inseguro quanto a Internet[Projeto NF-e 2007]. Mesmo sendo inevitável a confiança nas chaves privadas, e estas estarem suscetíveis ao comprometimento, o protocolo deveria informar ao emitente que o mesmo pode estar sendo vítima de uma fraude.

A prova de tal fato demonstra a necessidade de uma validação formal estendida deste protocolo, assim como a definição de modelos de atacantes abrangentes, reais e inseridos no contexto de execução do protocolo. Devemos também especificar de forma mais abrangente a semântica fiscal envolvida no protocolo.

A especificação de um modelo de risco também é importante para o protocolo, pois as partes envolvidas podem a partir deste elaborar suas necessidades de segurança para operar em tal ambiente, sabendo desta forma dos riscos aos quais estão submetidas.

4. Análise Formal e Impacto dos Ataques Encontrados

A avaliação formal foi feita sobre um modelo simplificado, e o número de conjecturas testado foi relativamente pequeno. Mesmo assim foi possível identificar claramente a falta de um controle encadeado no protocolo de retorno de recepção. A expansão do modelo dos protocolos é necessário para se provar conjecturas mais elaboradas quanto às

propriedades de cada mensagem e do processo de execução dos protocolos. A inclusão de mais semântica é necessária para representar possíveis problemas mais complexos.

O impacto deste problema é facilmente visível para o cenário de certas empresas. Empresas usando NF-e poderiam sofrer ações lesivas, principalmente partindo de entes internos corrompidos - proposital e acidentalmente - , que somente seriam percebidas, quando ela tentasse solicitar uma NF-e cuja numeração já constaria no sistema da SEFAZ como utilizado, ou quando fosse autuada pela Administração Tributária Estadual pelo não pagamento do imposto devido e declarado nas NF-e emitidas pelo atacante.

Um cenário de fácil análise pode ser percebido em empresas exportadoras, as quais tem regimes tributários diferenciados para exportação e mercado interno. As mesmas poderiam ser alvos de contrabandistas, que trazem seus produtos exportados de volta ao mercado nacional, e poderiam, através dos problemas apresentados, colocar no mercado produtos contrabandeados, com notas fiscais válidas, e com imposto devido pela empresa produtora. Problema similar aplica-se ao roubo de cargas, adulteração, falsificação, pirataria de produtos, espionagem industrial, concorrência desleal, entre outros problemas comuns no Brasil, especialmente em determinadas categorias de produtos, como combustíveis líquidos (gasolina, álcool), cigarros, bebidas e medicamentos.

5. Contra-Medidas aos Ataques

O conceito da autorização prévia de utilização de numeração para emissão de novas NF-e, é uma das alternativas válidas a considerar-se para evitar e/ou detectar emissões fraudelentas, sem impacto na eficiência e agilidade do processo eletrônico. Adotado de forma serializada e sistemática, previamente à emissão de novas NF-e, a solicitação de numeração eletrônica seria assinada digitalmente pelo contribuinte emissor, e autorizada pela Administração Tributária competente, a qual responderia à solicitação autorizando-a e gerando um hash da mesma, o qual seria informado na próxima solicitação do mesmo contribuinte emitente. Tal serviço seria provido nos moldes atuais dos demais web services, informando porém o hash da solicitação de numeração anterior. Desta forma haveria uma serialização obrigatória sobre as autorizações de emissão, permitindo que o emitente detectasse fraudes no seu processo de emissão de NF-e, minimizando seus riscos.

A opção pela não modificação dos protocolos obriga as empresas a adquirir meios de proteção de suas chaves privadas muito mais severos, sendo um meio eficaz o uso de Módulos de Segurança Criptográficos (Hardware Security Modules)[NIST 2002], como já recomendado pelo Manual de Integração [Projeto NF-e 2007]. Estes equipamentos são especificamente projetados para proteger as chaves privadas relacionadas com certificados digitais, quanto a cópia e uso não autorizado. Normalmente uma outra funcionalidade importante destes equipamentos é a construção de trilhas de auditoria confiáveis, as quais as Administrações Tributárias Estaduais poderiam recorrer no caso sobre dúvidas na emissão de NF-e ou de contestações por partes dos contribuintes. Esta área de pesquisa vem sendo ativamente desenvolvida no Brasil, visto sua aplicabilidade a sistemas bancários e de Infra Estrutura de Chaves Públicas [Martina et al. 2007, de Souza et al. 2008], mas não limitando-se a estes. As aplicabilidades de sistemas de gerenciamento seguro de chaves são necessidades de quaisquer sistemas que fazem uso de chaves criptográficas que demandem sigilo e controle de uso.

Do ponto de vista da utilização de certificados digitais, a adoção de certitica-

dos padrão A3[Presidência da República 2001] seria a mais recomendada em termos de segurança das chaves privadas, entretanto tal opção torna-se inviável pelos moldes atuais na perspectiva da eficiência, sobre o processo de emissão de NF-e. O padrão A1, embora menos seguro, é a opção viável para as empresas emissoras de NF-e, mesmo com os riscos apontados e demonstrados neste artigo.

6. Considerações Finais

O sistema de emissão de notas fiscais eletrônicas é um fato hoje no Brasil. A aderência a seus padrões é de incontestável importância para as empresas. Assim sendo as garantias dadas às empresas que utilizam o sistema devem se equiparar às garantias dadas às Administrações Tributárias em termos de segurança do processo. A geração de protocolos para a transmissão de dados é um importante fator para a agilidade dos processos empresariais e fiscais. A geração destes protocolos deve levar sempre em consideração cenários reais de (in)segurança presentes nos sistemas utilizados. O processo de validação formal para tais protocolos é essencial para a obtenção das garantias mínimas necessárias.

Neste artigo apresentamos a tradução do modelo em linguagem natural desenvolvido pelo governo brasileiro para um sistema mais formal e rígido envolvendo sistemas lógicos e métodos automatizados de detecção de problemas. Como resultado obtivemos uma avaliação estrita e confiável dos protocolos. Também ficou evidente que o método utilizado pelo Governo não é fundamentado de premissas amplas e a sua informalidade de expressão pode conduzir a problemas que afetem os participantes, causando prejuízos financeiros, tributários e institucionais - em muitos casos, irrecuperáveis.

Os protocolos apresentam todas as características importantes para garantir a execução do processo de comunicação desejado, mas falham na modelagem das ameaças, neste caso, presentes na Internet. A correção proposta aos protocolos é simples e pode ser sanada de uma forma prevista nos documentos e legislação da NF-e: a incorporação de um novo web service para a autorização prévia de utilização de numeração, para emissão de novas NF-e, serializada e assinada digitalmente pela empresa emitente e autorizada pela Administração Tributária responsável. Esta nova alternativa garantiria segurança ao processo de emissão de nf-es, com baixo impacto para as Administrações Tributárias e seus contribuintes, sem comprometer aspectos técnicos e operacionais. A serialização é um componente importante, e presente em propostas similares, por minimizar os fatos demonstrados neste artigo. A descrição formal completa dos protocolos por parte dos autores também auxiliaria no processo de verificação formal e estabelecimento dos objetivos e ameaças à segurança da informação e dos processos em si.

Como trabalhos futuros, além da complementação semântica do modelo apresentado, sugere-se o aumento do modelo formal do protocolos para propiciar a avaliação da não obrigatoriedade da assinatura por parte das Administrações Tributárias nos recibos das NF-e. Assumir a fé pública do Estado não exime problemas de confiança entre Emitente e Destinatário, os quais não necessariamente têm confiança entre si, mas são solidários aos problemas fiscais que por ventura possam ser introduzidos nestes documentos digitais. Outros pontos importantes e passíveis de análise são a utilização de âncoras temporais fortes nos sistemas de NF-e e do processo de armazenamento dos dados fiscais por partes das Administrações Tributárias Estaduais.

Referências

[de Souza et al. 2008] de Souza, T. C. S., Martina, J. E., and Custódio, R. F. (2008). Audit and backup procedures for hardware security modules. In *IDtrust '08*, New York, NY, USA. ACM.

[Dolev and Yao 1983] Dolev, D. and Yao, A. (1983). On the security of public key protocols. *Information Theory, IEEE Transactions on*, 29(2):198–208.

[Gorges 2006] Gorges, A. J. (2006). *O Seu Plantão Fiscal - Dicionário de ICMS de A a Z*. CENOFISCO, 8 edition.

[Martina et al. 2007] Martina, J. E., de Souza, T. C. S., and Custódio, R. F. (2007). Openhsm: An open key life cycle protocol for public key infrastructure's hardware security modules. In *EuroPKI'07*, LNCS. Springer-Verlag Berlin Heidelberg.

[Needham and Schroeder 1978] Needham, R. M. and Schroeder, M. D. (1978). Using encryption for authentication in large networks of computers. *Commun. ACM*, 21(12):993–999.

[NIST 2002] NIST, N. I. o. S. (2002). Fips pub 140-2 - security requirements for cryptographic modules.

[Paulson 1999a] Paulson, L. C. (1999a). Inductive analysis of the internet protocol tls. *ACM Trans. Inf. Syst. Secur.*, 2(3):332–351.

[Paulson 1999b] Paulson, L. C. (1999b). Proving security protocols correct. In *LICS '99: Proceedings of the 14th Annual IEEE Symposium on Logicin Computer Science*, page 370, Washington, DC, USA. IEEE Computer Society.

[Presidência da República 2001] Presidência da República (2001). Medida provisória número 2.200-2.

[Projeto NF-e 2007] Projeto NF-e (2007). Manual de integra cão do contribuinte - padrões técnicos de comunica cão. Technical Report 2.0.2, ENCAT.

[Secretaría de Hacienda y Crédito Público México 2008] Secretaría de Hacienda y Crédito Público México (2008). Factura eletrónica - faq. http://www.sat.gob.mx/sitio_internet/e_sat/comprobantes_fiscales/15_6606.html.

[Servicio de Impuestos Internos - Chile 2003] Servicio de Impuestos Internos - Chile (2003). Resolucion exenta sii no.45. http://www.sii.cl/documentos/resoluciones/2003/res_ind2003.htm/.

[SRF 2007] SRF, S. d. R. F. (2007). Portal nacional da nota fiscal eletrônica. http://www.nfe.fazenda.gov.br/.

[Weidenbach 1999] Weidenbach, C. (1999). Towards an automatic analysis of security protocols in first-order logic. In *CADE-16: Proceedings of the 16th International Conference on Automated Deduction*, pages 314–328, London, UK. Springer-Verlag.

[Weidenbach et al. 2002] Weidenbach, C., Brahm, U., Hillenbrand, T., Keen, E., Theobalt, C., and Topić, D. (2002). SPASS version 2.0. In *18th International Conference on Automated Deduction*, Lecture Notes in Artificial Intelligence. Springer.