Segurança Cibernética em Smart Metering

Charles Bezerra do Prado[1], Davidson Rodrigo Boccardo[1], Raphael Carlos Santos Machado[1], Tiago Monteiro do Nascimento[1],Luiz Fernando Rust da Costa Carmo[1], Renato Almeida Oliveira[2]

[1] Instituto Nacional de Metrologia, Qualidade e Tecnologia, Rio de Janeiro, Brasil
cbprado@inmetro.gov.br , drboccardo@inmetro.gov.br, rcmachado@inmetro.gov.br, tmnascimento@inmetro.gov.br, lfrust@inmetro.gov.br
[2] Eletrobrás Distribuidora Rondônia, Porto Velho-RO, Brasil
renato.oliveira@ceron.com.br

Abstract* — *Medidores inteligentes são medidores dotados de software embarcado e que possuem capacidade de complexo processamento digital de dados. Medidores inteligentes já são uma realidade na maioria das áreas de Metrologia. Ao mesmo tempo em que trazem a possibilidade de uma série de novas aplicações, tais medidores inteligentes representam um novo desafio no que diz respeito à sua validação, em especial, no âmbito da Metrologia Legal. No presente trabalho, descrevemos as iniciativas do Inmetro em parceria com a Eletrobrás (Ceron) no sentido de produzir conhecimento e desenvolver ferramentas que sirvam de apoio às atividades de validação de medidores inteligentes de energia elétrica.

Keywords — *Segurança Cibernética*, Smart Grid, Medidores Inteligentes.

I. Introdução

Através da evolução tecnológica, o surgimento dos Smart Grid (Redes Inteligentes) aponta para melhoramentos desde o processo de geração de energia elétrica até o ponto final desta cadeia que é o usuário fim desta energia gerada. Por meio de monitoração, análise, controle e comunicação de todas as partes que integram uma rede elétrica, as Redes Inteligentes buscam alcançar: melhorias no desempenho, otimização do uso dos recursos energéticos, aumento na eficiência energética, alternativas de armazenamento e etc. E, assim garantir um sistema com maior qualidade e eficiência para o consumidor final.

No Brasil, o desenvolvimento e a implementação de Smart Grids permitirão às concessionárias um controle e uma monitoração mais eficaz da distribuição do consumo de energia elétrica. Consequentemente será possível realizar um melhor planejamento da expansão do fornecimento de energia.

Ademais, os Smart Grids possibilitarão um combate mais efetivo da fraude de energia elétrica. Este problema aparece com maior frequência e com alto risco de acidentes em comunidades de baixa renda, aonde os chamados "gatos" são visíveis, e em virtude destas instalações ocorrerem em péssimas condições, os riscos de acidentes causados por curtos-circuitos se mostram elevados. Com a tecnologia do Smart Grid será possível, por exemplo através de sensores de abertura de porta, a detecção da violação de cada componente pertencente a rede o que minimizaria a possibilidade da adulteração dos equipamentos de medição, reduzindo em muito as fraudes de energia elétrica [1-5].

Dentre diverso nós de processamento de um Smart Grid, o medidor inteligente (Smart Meter) caracteriza-se por ser um elemento ativo que envolve comunicação de dados, monitoração e tomada de ação remota e que agrega portas de acesso que conectam usuários finais a todo o sistema Smart Grid. Dentro do escopo de avaliação destes equipamentos pelo Inmetro, uma atribuição do Inmetro é garantir a integridade das informações que trafegam pelo medidor e em específico a que se refere ao consumo de energia elétrica. Atualmente, este cenário tem sido alvo de estudos na área de segurança cibernética aplicada aos Smart Grids [6].

Segurança cibernética, a que nos referimos neste contexto, se refere à aplicação de metodologias que impossibilite (ou torne quase que impossível) que pessoas não autorizadas tenham acesso e poder de manipulação de qualquer serviço ou informação inerente a um Smart Grid e assim utilizá-los para fins inapropriados.

O caráter emergente da tecnologia de Smart Grids no panorama mundial, em que os padrões ainda não se encontram consolidados, requer uma participação mais ativa dos órgãos nacionais inerentes ao processo, de forma a considerar as especificidades nacionais (por exemplo: a redução de perdas por fraudes), desenvolvendo um modelo regulatório apropriado e fornecendo subsídios para competitividade da indústria nacional.

O desenvolvimento de atividades de pesquisa no Brasil em linha com atividades semelhantes em centros avançados permite ao pais acompanhar e compartilhar tecnologias inovadoras. Diante disso, o Inmetro, como órgão responsável pela metrologia no Brasil, e em parceria com a Eletrobrás Distribuidora Rondônia, vem desenvolvendo um projeto de pesquisa intitulado "Segurança Cibernética em Smart Metering". Esta pesquisa se divide em seis frentes:

1) Aprimorar o processo de validação dos softwares embarcados nos sistemas de medição de energia elétrica.
2) Investigar e compreender o processo de mapeamento do código fonte em um código executável a ser executado no medidor.
3) Verificação de integridade dos softwares embarcados nos medidores.
4) Investigar como uma cadeia de confiança poderia ser estabelecida em um Smart Meter.
5) Projeto de um "chip" para controle metrológico.
6) Investigação das técnicas de proteção de software para a infraestrutura avançada de medição.

II. FRENTES DE PESQUISA

A) Aprimorar o processo de validação dos softwares embarcados nos sistemas de medição de energia

Esta frente refere-se à necessidade de aperfeiçoar o processo de avaliação de software de um medidor. Já existem algumas propostas para tentar identificar possíveis focos de vulnerabilidades nas aplicações embarcadas [7]. Propostas essas que podem ser classificadas como abordagens caixa-preta, quando partem do pressuposto do total desconhecimento de como a aplicação foi desenvolvida; ou abordagens caixa-branca, quando requerem o conhecimento do código fonte da aplicação [8]. Apesar da abordagem caixa-preta apresentar um maior espectro de aplicabilidade, normalmente são bem menos eficientes, dado a natural limitação quanto ao número de elementos analisáveis. Apesar de uma abordagem caixa-branca poder ser conduzida através de uma simples inspeção do código fonte, esse procedimento está longe de ser prático ou eficiente.

A ideia é desenvolver uma metodologia para a geração de árvores de ataques derivadas das vulnerabilidades conhecidas e divulgadas pelas comunidades de segurança afins (em função do ambiente de desenvolvimento/plataforma empregada) e, em seguida, validar a eficácia do ferramental de testes derivados destas árvores de ataque pela inserção automática de vulnerabilidades por técnicas de mutação de código. O trabalho de [9] se aproxima em termos funcionais da proposta de mutação pra validação de testes de segurança, porém se baseia apenas na injeção manual de erros (SQL *injection*). O uso de uma abordagem baseada em mutação amplifica muito o escopo de validação dos testes, pois compreende até fatores imprevisíveis.

B) Investigar e compreender o processo de mapeamento do código fonte em um código executável a ser executado no medidor

Esta frente está associada à validação de software, pois ao final do processo de validação, é importante determinar se o software estará em execução no medidor. No entanto, como a validação é feita de forma muito mais eficiente no código fonte (abordagem caixa-branca), é ainda necessário uma tarefa de rastreabilidade do código executável. Esta consiste na identificação do código executável associado ao código fonte analisado ou, mais precisamente, verificar se o código executável apresentado pelo fabricante do medidor corresponde ao código fonte apresentado por este fabricante.

Duas abordagens imediatas são possíveis, mas não práticas. Uma primeira abordagem é auditar o processo de compilação no ambiente de desenvolvimento do fabricante. O risco desta abordagem é a dificuldade de se conduzir uma auditoria perfeita no ambiente de compilação. Uma segunda abordagem é a reprodução da compilação no ambiente do avaliador (no caso, o Inmetro). As desvantagens desta abordagem são o custo de reproduzir o ambiente do fabricante (compra de ferramentas, máquinas, compiladores,...) e a grande possibilidade de produzir um código executável diferente daquele apresentado pelo fabricante devido a detalhes de configuração (por exemplo, uma função de otimização de um compilador ou uma versão ligeiramente diferente de alguma biblioteca).

Resultados preliminares utilizando redes neurais artificiais com características triviais, como o número de arestas e nós, mostram que existe uma correspondência entre os grafos de fluxo de execução do código-fonte e do código executável [10].

C) Verificação de integridade dos softwares embarcados nos medidores

Esta frente refere-se à necessidade de se verificar, de forma eficiente, prática e segura, a integridade do software em execução em um medidor. Uma abordagem simples e direta é permitir que qualquer indivíduo com acesso ao medidor possa "ler" externamente o código do software em execução neste medidor. Esta abordagem, no entanto, encontra forte resistência de fabricantes de medidores, os quais buscam proteger sua propriedade intelectual (software) de acesso indevido. Além disso, em algumas situações, pode ser interessante (por questão de segurança) manter oculto o código em execução [11].

D) Criação/Avaliação de cadeias de confiança para medidores inteligentes

O foco principal, diferentemente dos anteriores apresentados, é de se criar um ambiente no qual diversas técnicas de assinatura digital e certificação digital poderão ser avaliadas visando garantir a segurança da informação a partir do instante que esta sai dos medidores e trafega dentro do Smart Grid. Baseados em criptografia assimétrica, esperamos construir um ambiente que se assemelhe a um Smart Grid genérico. Dentro desse ambiente seremos capazes de simular ataques no sentido de manipular os dados (informações secretas) que trafegam dentro da rede. Ao final, esperamos fornecer uma metodologia de segurança da informação capaz de evitar ou praticamente tornar impossível a manipulação e alteração de dados relevantes que trafegam desde um medidor de consumo até o ponto de destino na cadeia de um Smart Grid.

E) Projeto de um "chip" para controle metrológico

Esta frente refere-se ao desenvolvimento de uma arquitetura computacional que facilite o atendimento a requisitos de segurança da informação em medidores especificados em regulamentos e portarias do Inmetro (rastreadas em normas internacionais). Tal arquitetura terá sua organização baseada na presença de um dispositivo eletrônico "chip" cuja especificação será um dos produtos finais do presente projeto. Este "chip" funcionaria como um controlador metrológico customizado através do qual seja possível: realizar funções criptográficas (incluindo assinatura eletrônica da leitura de instrumentos de medição), garantir a integridade do software durante o controle metrológico legal [12,13] e exercer uma possível função de firewall de comandos maliciosos (intencionais ou não) entre outras possíveis funções.

F) Investigação das técnicas de proteção de software para uma infraestrutura avançada de medição

Este objetivo visa explorar caminhos de proteção de propriedade intelectual para sistemas de software embarcado, visto que a utilização desses em aplicações de propósito nacional (como de *smart grids*), pode tornar-se em uma ameaça potencial caso estes sistemas sejam atacados. Entre as motivações para os atacantes podemos mencionar ganho financeiro, sabotagem e vingança.

Atualmente, desenvolvedores tem realizado um grande esforço para que seus softwares sejam eficientes e livres de vulnerabilidades (o tanto quanto possível), porém tem manifestado pouco interesse quanto a proteção destes sistemas. A proteção de um software pode ser caracterizada como uma forma de conter ou dificultar um usuário mal intencionado de atacar o sistema. Por exemplo, um atacante com acesso ao sistema poderia realizar vários comandos de desligamento, causando assim, prejuízos.

Assim, a investigação do impacto dos melhores métodos de proteção e como estes podem ser subvertidos são fundamentais, assim como a avaliação do impacto no desempenho para diferentes formas de proteção. Adicionalmente, devem ser investigadas novas formas para proteção de software com o objetivo de incrementar o estado da arte.

Dentre as técnicas de proteção de software, temos a ofuscação de código, marca d'água e *tamper-proofing* (incorruptibilidade). Técnicas de ofuscação de código visam dificultar engenharia reversa tornando o software inteligível através de modificações em sua sintaxe, porém mantendo sua funcionalidade (semântica). Tem sido utilizada para prover diversificação por meio da geração de cópias distintas do mesmo artefato; prevenção de conluio, pois a diversificação dificulta ataques de diferença; privacidade de código e dados, pois o código é de difícil discernimento assim é difícil descobrir a localização de dados secretos (chaves); e integridade, pois um código de difícil entendimento é, por conseguinte difícil de ser modificado. Uma defesa contra pirataria de software são as técnicas de marca d'água que tem por objetivo rastrear origem de um artefato, e uma defesa contra a modificação são as técnicas de incorruptibilidade, em que modificações não autorizadas no software resultariam em códigos não funcionais [14, 15].

III. CONCLUSÕES

Com o avanço da computação e da microeletrônica, observa-se, cada vez mais, a presença de dispositivos "inteligentes" nos mais diversos campos de atuação. No campo da Metrologia, observa-se os medidores deixarem de ser dispositivos mecânicos para tornarem-se pequenos computadores dedicados à medição. O advento do uso de medidores inteligentes de energia elétrica trouxe uma série de desafios no que diz respeito à sua avaliação pela Autoridade Metrológica.

No presente trabalho, mostramos que a validação de tais medidores somente poderá ser efetiva se a Autoridade Metrológica investir fortemente na produção de conhecimento científico, no desenvolvimento de ferramentas especializadas, e na formação de recursos humanos. No presente artigo, apresentamos as iniciativas do Inmetro em parceria com a Eletrobrás Distribuidora Rondônia visando ao desenvolvimento dos métodos de avaliação de medidores inteligentes, com foco na Segurança da Informação. Apresentamos as linhas de pesquisa atualmente em andamento no Inmetro, em especial na áreas de Análise e Proteção de Software, e defendemos a atuação conjunta do Inmetro e de fabricantes de medidores e distribuidoras de energia no sentido de desenvolver arquiteturas e equipamentos que incrementem o nível de segurança dos medidores inteligentes de energia.

IV. AGRADECIMENTOS

Os autores gostariam de agradecer a Eletrobrás Distribuidora Rondônia pelo suporte financeiro ao projeto sob o nº DR/069/2012.

REFERÊNCIAS

[1] Mateus, J. C.; Cuervo, P.E.; "Transmission Cost and Loss Allocation Method through Linearized Distribution Factors.", International Conference European Electricity Market (EEM06), Varsóvia, p. 413-420, 2006.

[2] Barreto, G. ; Cuervo, P.E.; Mateus, J. C.; "Estudo de Métodos de Alocação de Perdas de Transmissão Aplicados ao Sistema Interligado Nacional.", X Simpósio de Especialistas em Planejamento da Operação e Expensão Elétrica, Florianópolis, 2006.

[3] Mateus, J. C.; Franco, P. E. C.; "Transmission Loss Allocation through Equivalent Bilateral Exchanges and Economical Analysis.", IEEE/PES Powertech, Saint Petesburg, 2005.

[4] Fernandes Filho, C.; Barreto, G.; Mateus, J. C.; Cuervo, P.E.; Biagio, M. A.; Coelho, M.A.; "Implementação de Metodologias de Alocação de Perdas de Transmissão para a Rede Básica Brasileira.", III Congresso de Inovação Tecnológica em energia elétrica, Florianópolis, 2005.

[5] Franco, P. E. C.; Mateus, J. C.; Fernandes Filho, C.; Egito, M.; Biagio, M. A.; "Metodologia de Avaliação Incremental de Métodos de Alocação de Perdas de Transmissão." IEEE/PES T&D2004 Latin America, São Paulo, 2004.

[6] NIST - Issues Expanded Draft of Smart Grid Cyber Security Strategy For Public Review and Comment, http://www.nist.gov/public_affairs/releases/smartgrid_020310.cfm (Último acesso, março 2013)

[7] NIST, SAMATE - Software Assurance Metrics and Tool Evaluation, http://samate.nist.gov/index.php/Main_Page.html (Último acesso, março 2013)

[8] Huang, Y. W.; Yu, F.; Hang, C.; Tsai, C. H.; Lee, D. T.; Kuo, S.Y.; "Securing web application code by static analysis and runtime protection", 13th International Conference on World Wide Web, 2004.

[9] Huang,Y. W.; Huang, S. K.; Lin,T. P.; Lin, T. P.; Tsai,C. H.; "Web application security assessment by fault injection and behavior monitoring", 12th International Conference on World Wide Web, Budapest, Hungary, pp. 148 – 159, 2003.

[10] T. M. Nascimento; D. R. Boccardo; C. B. Prado; R. C. S. Machado; L. F. R. C Carmo, "Program Matching Through Code Analysis and Artificial Neural Networks." *International Journal of Software Engineering and Knowledge Engineering*, v. 22, pp. 225-241, 2012.

[11] Sá, V. G. P. de; Boccardo D. R.; Rust L. F.; Machado R. C. S.; "A tight bound for exhaustive key search attacks against Message Authentication Codes," RAIRO - Theoretical Informatics and Applications.

[12] Carmo, L. F. R. C.; Machado, R. C.; Madruga, E. L.; "Metrologia temporal na verificação de integridade de software em instrumentos de medição", V Congresso Brasileiro de Metrologia, Salvador, 2009.

[13] Carmo, L. F. R. C.; Machado, R. C.; "Verificação de integridade de software embarcado através da análise de comportamento temporal", SBSeg, IX Simpósio Brasileiro de Segurança da Informação, Campinas, 2009.

[14] Collberg, C., Nagra, J.; *Surreptitious Software: Obfuscation, Watermarking, and Tamperproofing for Software Protection*, Addison Wesley, Reading, 2010.

[15] Lakhotia, A.; Boccardo, D. R.; Singh, A.; Manacero Jr, A.; "Context-sensitive analysis of obfuscated x86 executables.", Proceedings of the 2010 ACM SIGPLAN workshop on Partial evaluation and program manipulation, Madrid, Spain, pp. 131-140, 2010.