Segurança no Sensoriamento e Aquisição de Dados de Testes de Impacto Veiculares

Wilson S. Melo Jr[1,2], Luiz F. R. C. Carmo[1,2], Charles Prado[1], Paulo R. Nascimento[1], Luci Pirmez[2]

[1]Instituto de Metrologia, Qualidade e Tecnologia (Inmetro), RJ – Brasil

[2]PPGI iNCE/IM, Universidade Federal do Rio de Janeiro (UFRJ), RJ – Brasil

{wsjunior,lfrust,cbprado,prnascimento}@inmetro.gov.br,
luci.pirmez@ufrj.br

Abstract. *This paper deals with the cyber security of vehicular impact tests (crash tests). A model attack describes main attacks that can be launched against the sensing and data acquisition system. For each attack, it is described countermeasures based on methodologies already consolidated in the literature. However, one of the described attacks is related with the difficult on identify that the expected sensors were indeed inside the vehicle during the test. For this attack is presented an original idea which is the emission of a unique identifier for each sensor using a light device. The identifier is recovered using a camera already present in the test context. The idea feasibility is demonstrated on a practical experiment.*

Resumo. *Este trabalho trata da segurança cibernética em um teste de impacto de veículos (crash tests). Um modelo de ataque descreve os principais ataques que podem ser lançados contra os sistemas de sensoriamento e aquisição de dados. Para cada ataque, são apresentadas contramedidas baseadas em metodologias já consolidadas na literatura. Todavia, um desses ataques está relacionado com a dificuldade de se confirmar que os sensores foram de fato embarcados no veiculo durante o teste. Para este ataque é apresentada uma ideia original de emissão de um identificador único para cada sensor usando um dispositivo luminoso e a recuperação deste por uma câmera já utilizada no teste. A factibilidade da ideia é demonstrada por meio de um experimento.*

1. Introdução

Estima-se que no Brasil, a cada 11 minutos, uma pessoa morre em acidente de trânsito. Anualmente este número ultrapassa o total de 43 mil mortos e 150 mil feridos, um número de vítimas maior do que em muitos conflitos armados. Se forem calculadas as perdas sociais e econômicas, o valor estimado ultrapassa R$ 30 bilhões [Bacchieri e Barros 2011]. Dada a seriedade do problema, diversas medidas são continuamente propostas tanto na tentativa de reduzir o número de acidentes quanto de minimizar seus impactos. Neste segundo grupo, alternativas tecnológicas que vão desde o uso de materiais mais eficientes na absorção do impacto até os modernos sistemas de evasão de colisão estão disponíveis como arsenal para a indústria automotiva [Caveney 2010]. Em alguns casos, essas tecnologias tornam-se elementos de segurança obrigatórios, como é o caso recente dos *airbags* e freios ABS no Brasil. Entretanto, tais inovações resultam

no aumento do custo do veículo, de modo a gerar conflitos de interesses de mercado por parte da indústria, dos consumidores e das autoridades interessadas. Em muitos casos, a eficiência destas soluções não corresponde àquela divulgada pelo fabricante, o que torna necessária a verificação das mesmas em testes realizados por uma terceira parte.

Nesse contexto, os testes de impacto ou colisão, popularmente chamados de *crash tests*, possuem uma função consolidada em diversos países desenvolvidos e começam a ganhar destaque também nos países em desenvolvimento [Paine and Haley 2008]. No Brasil, só recentemente alguns veículos passaram a ser submetidos a testes de impacto. Os resultados dos primeiros testes são preocupantes, pois apontam os carros brasileiros como pouco seguros quando comparados ao mercado global. Em resposta, o governo brasileiro determinou que o Inmetro passe a realizar testes de impacto a partir de 2015 em seu futuro Centro de Tecnologia Automotivo, atualmente em construção.

Um teste de impacto se propõe a avaliar o comportamento dinâmico dos elementos voltados a prover a segurança passiva de um veículo. Conceitualmente simples, o teste consiste em se colidir um veículo contra um obstáculo dentro de condições pré-determinadas e observáveis, avaliando-se em seguida a gravidade do impacto sobre a estrutura do veículo e principalmente sobre seus ocupantes. Um aspecto importante é instrumentação do teste por meio de sensores como acelerômetros e células de impacto. Em poucos segundos, uma massa significativa de dados é coletada e armazenada por dispositivos de aquisição de dados. Esses dados são posteriormente analisados e assim se determinam os resultados do teste [Hobbs and McDonough 1998].

Todavia, uma questão que pode ser levantada diz respeito à confiabilidade dos dados coletados. Embora existam padrões que definam a sensibilidade dos sensores, frequências de operação, taxas de amostragem, protocolos de comunicação e capacidade dos dispositivos de armazenamento, não existem quaisquer requisitos relacionados à segurança cibernética dessas informações. É fato que os resultados de testes de impacto realizados sistematicamente podem afetar as relações de mercado, seja pela definição quanto à homologação de um determinado modelo de veículo ou ainda pela decisão do consumidor quanto a optar por um veículo indicado mais seguro. Sendo assim, é necessário se garantir que esses resultados derivam de informações confiáveis.

Neste trabalho, os autores apresentam uma discussão voltada à segurança cibernética dos processos de instrumentação e aquisição de dados em um teste de impacto. O termo sensoriamento seguro é utilizado como ponto de partida para se avaliar trabalhos relacionados a essa problemática. Em seguida, um modelo de ataque é descrito para se evidenciar os principais ataques que podem ser lançados contra os sistemas de sensoriamento e aquisição de dados durante a realização de um teste de impacto. Desses ataques, a maioria pode ser tratada de forma satisfatória por meio de metodologias de segurança da informação já consolidadas na literatura. Todavia, um ataque específico está relacionado com dificuldade de se identificar os sensores embarcados no veiculo durante o teste. Para tanto, os autores apresentam uma proposta original de propagação de um identificador único para cada sensor por meio de um dispositivo luminoso. A recuperação e verificação deste identificador são feitas por meio das câmeras de alta velocidade já utilizadas no teste. Com isso, pode-se além de se autenticar cada sensor utilizado, garantir que o mesmo encontra-se de fato embarcado no veículo, sem a necessidade de se acrescentar novos equipamentos ao contexto de testes.

2. Trabalhos relacionados

O conceito de sensoriamento seguro é encontrado em diversos trabalhos recentes na literatura [Sorber et al. 2012, Colak et al. 2012, Han et al. 2013]. Em muitos sistemas de controle ou de coleta de informações, o uso de sensores é cada vez mais comum. Em geral, sensores são usados para prover informação de forma automática a um sistema de tomada de decisão. A resposta do sistema como um todo depende da precisão e integridade dos dados obtidos. Entretanto, no processo de aquisição de dados, muitas vezes a informação é transmitida por diferentes canais e protocolos ou processada por elementos computacionais que podem não prover mecanismos de segurança da informação. Ao mesmo tempo, estes elementos intermediários estão sujeitos tanto a falhas quanto a ataques maliciosos, externos ou internos ao sistema. Assim, é necessário que o sistema de tomada de decisão disponha de mecanismos para avaliar as informações providas e confirmar se as mesmas são confiáveis.

Um caso interessante de sensoriamento seguro é dado por Sorber et al. (2012). Os autores consideram o sistema mHealth, que é um caso particular de PHMS (*Pervasive Health Monitoring System*). Neste sistema, sensores corporais coletam dados sobre as condições de saúde de pacientes e as transmitem a um centro médico de monitoramento. No mHealth, os sensores e os servidores que recebem os dados são considerados seguros; entretanto, o meio de transmissão, que consiste de um telefone celular, não o é, implicando que os dados dos sensores podem ser interceptados, usados indevidamente ou mesmo adulterados, resultando na emissão de diagnósticos equivocados. Os autores apresentam então uma estratégia para proteger as informações coletadas durante todo o trajeto não seguro, usando um *smart card* para autenticação dos sensores e armazenamento das informações, até que seja possível transmitir os dados pelo telefone celular. Durante a transmissão, o *smart card* é usado novamente para criptografar os dados e protegê-los durante todo o trajeto até o servidor seguro.

Um exemplo simples do uso de sensoriamento seguro na área veicular pode ser encontrado no cronotacógrafo digital europeu [Colak et al. 2012]. Tal como no Brasil, o cronotacógrafo é utilizado na Europa para controlar a jornada de trabalho de motoristas. Neste dispositivo existe um sensor de movimento não intrusivo capaz de contar o número de giros do eixo do veículo e assim determinar a distância percorrida. O sensor é ligado por meio de um cabo ao cronotacógrafo. Na primeira geração destes dispositivos, eram comuns fraudes envolvendo a substituição do sensor de movimento por um sensor malicioso. Na segunda geração de cronotacógrafos, foi introduzido o uso de sensores inteligentes, onde o sinal analógico obtido é digitalizado pela própria eletrônica embarcada. Cada sensor possui um identificador único, que é gravado apenas uma vez, em tempo de fabricação. O sensor é protegido contra adulteração (*tamper proofing*) de modo que qualquer tentativa de leitura ou modificação de seu identificador seja facilmente detectada. A transmissão dos dados para o cronotacógrafo é feita por meio de um canal autenticado e criptografado, estabelecido a partir do identificador.

Outro trabalho com ideias relacionadas é apresentado em Han et al. (2013). Neste trabalho, os autores consideram o uso do sistema Ford OpenXC, que permite ao usuário obter informações de sensores e subsistemas de seu veículo. Um telefone inteligente é utilizado para coletar informações da rede de controle veicular, processá-las e exibi-las ao usuário. O problema é que a rede de controle não faz distinção entre

um nó conectado apenas para obter informações e outro que possa também transmitir informações. Um software malicioso pode fazer uso desse canal de comunicação para envio de mensagens espúrias, comprometendo o desempenho do veículo e pondo em risco a vida de seus ocupantes. Neste trabalho os autores definem um modelo de integração segura, apresentando os cenários de ataque e definindo requisitos de segurança. Por fim, é proposto um mecanismo de verificação em três etapas, baseado em um *gateway* de segurança e processos de autenticação mútua entre dispositivos do usuário e as unidades de controle veicular.

Até onde é de conhecimento dos autores, não existem até o momento trabalhos abordando questões relacionadas ao sensoriamento seguro em testes de impacto. Ideias abstraídas dos trabalhos descritos nessa seção podem auxiliar tanto na identificação de vulnerabilidades no sensoriamento desses testes como na concepção de soluções para aumentar a segurança cibernética dos mesmos. Estas considerações serão desenvolvidas nas seções subsequentes deste trabalho.

3. Dinâmica e Sensoriamento de Testes de Impacto

3.1. Aspectos gerais de um teste de impacto

Existem tipos variados de testes de impacto, cada qual em função de finalidades, que vão desde a homologação de um veículo por fins de legislação até a pesquisa ou desenvolvimento de novos materiais e dispositivos de segurança. Para cada tipo diferente de teste, existe um protocolo que descreve a configuração física durante o impacto, as condições ambientais que devem ser observadas e também os elementos de instrumentação utilizados para coleta das informações [Hobbs and MacDonough 1998].

Durante um teste de impacto, o veículo é acelerado lentamente por meio de um mecanismo auxiliar baseado em cabos para evitar que uma aceleração brusca modifique o ajuste físico dos sensores. Além disso, é necessário que no momento da colisão a aceleração do veículo seja praticamente zero e sua velocidade constante. Próximo à área de impacto, o mecanismo de aceleração libera o veículo para que o mesmo continue sua trajetória de forma livre. A colisão do veículo ocorre sob condições de controle bem definidas, em conformidade com o protocolo de testes adotado. Durante a colisão, as dinâmicas de desaceleração, absorção de impacto e deformação dos elementos envolvidos proveem os dados necessários para a análise e resultados do teste. Essas informações serão coletadas pelo sistema de instrumentação, que é descrito a seguir.

3.2. Instrumentação de um teste de impacto

O primeiro trabalho sobre sensoriamento e instrumentação de testes de impacto é de Snider (1964). Embora as tecnologias envolvidas tenham evoluído significativamente, a metodologia usada atualmente difere muito pouco dessa proposta inicial. Nos testes de impacto modernos, a instrumentação também é definida nos protocolos de teste. Usualmente um protocolo de testes estabelece sua configuração de instrumentação levando em conta três elementos de teste principais:

1) O ATD (*Anthropomorphic Test Dummy*), um boneco humanoide usado para avaliar as consequências do impacto sobre pessoas dentro do veículo;

2) O próprio veículo, cuja instrumentação coleta informações sobre a dinâmica da colisão e os efeitos do impacto sobre a estrutura mecânica do mesmo;

3) A barreira de colisão, que também é instrumentada para se avaliar principalmente as forças de impacto envolvidas na colisão.

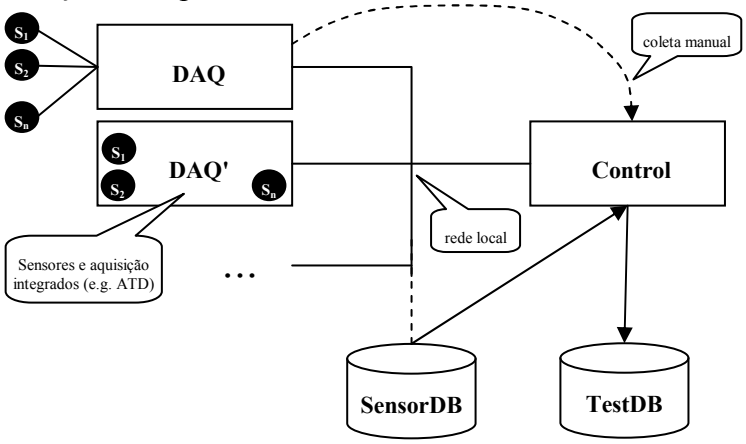

Figura 1: Visão geral do sensoriamento de um teste de impacto

A Figura 1 ilustra uma arquitetura de instrumentação geralmente adotada em testes de impacto. Ela relaciona os sensores, os dispositivos de aquisição de dados (DAQ), um banco de dados de informações de sensores (SensorDB), uma central de controle (Control) e um banco de dados de resultados dos testes (TestDB).

Os sensores são a parte crucial da instrumentação. Cada sensor possui um cadastro no banco de dados de sensores (SensorDB) que armazena informações sobre a identificação do sensor, propriedades físicas e parâmetros de calibração. O banco de dados é alimentado e revisado durante o processo de calibração do sensor, que ocorre sempre antes da realização de um teste de impacto.

Duas configurações são comuns na comunicação entre os sensores e o DAQ. Na primeira os sensores são acoplados ao DAQ durante a preparação do teste. Usualmente os sensores são analógicos e o DAQ funciona como conversor analógico/digital e armazenador temporário das informações. Em alguns casos podem-se utilizar sensores inteligentes, os quais executam uma parte do processamento do sinal em sua própria eletrônica. Outra configuração possível é quando sensores e DAQ são integrados pelo fabricante, de maneira que a unidade de instrumentação possa ser vista como um único bloco funcional. O ATD é um exemplo deste caso de instrumentação, onde sensores e DAQ formam um único conjunto. Nas duas configurações, os sistemas DAQ são elementos para controle, armazenamento temporário e disponibilização dos dados. No aspecto de controle, o DAQ é muitas vezes capaz de identificar e testar cada sensor a ele conectado e verificar se este corresponde a uma configuração esperada. O DAQ também contém memórias internas para armazenamento das informações coletadas. Alguns modelos permitem a transferência dos dados por meio de remoção da memória do dispositivo, conforme ilustrado.

O centro de controle (Control) tem a função de controlar as atividades de verificação da instrumentação e aquisição dos dados de teste. O *software* em Control pode inclusive fazer verificação de consistência dos dados, analisando a resposta de um

sensor em relação aos demais. Concluído o teste, a análise dos dados também será feita por Control, para posterior disponibilização dos resultados em TestDB.

Um elemento que não é parte direta da instrumentação, mas que é absolutamente relevante neste estudo é o sistema de câmeras de alta velocidade. O uso do vídeo para inferir informações sobre os resultados de um teste de impacto é algo bem consolidado. Sistemas comerciais de aquisição e processamento de imagens usualmente permitem a identificação de elementos físicos no vídeo. O vídeo pode inclusive fornecer informações de sensoriamento, como determinar a aceleração do veículo ou de um ATD interno a ele em função da triangulação de três pontos conhecidos na imagem.

4. Modelo de Ataque

Nesta seção é proposto um modelo de ataque visando identificar as principais ameaças e vulnerabilidades associadas ao sensoriamento e aquisição de dados de um teste de impacto. Um ataque pode ser motivado por diversas razões, conforme descrito na introdução deste trabalho. Os resultados dos testes podem afetar significativamente as decisões de mercado quanto à aquisição de um veículo ou não. Atores internos e externos ao teste, incluindo pessoal técnico, podem sofrer pressão ou mesmo suborno para interferirem nos resultados dos testes de modo a favorecer interesses específicos.

Como ponto de partida, são propostas três condições iniciais a serem satisfeitas para se garantir que o sensoriamento de um teste de impacto ocorre de forma confiável:

1) Todos os sensores utilizados no teste foram previamente calibrados.
2) Os sensores foram autenticados e suas medições estão integras.
3) Os sensores foram de fato utilizados no teste de impacto respectivo.

Cada uma das condições citadas é discutida em pormenores nas seções subsequentes, bem como os ataques que podem ocorrer em violação a essas condições.

4.1. Calibração dos sensores

Conforme descrito na seção 3, existe um processo prévio à realização dos testes que é a calibração dos sensores. A calibração é feita em laboratório. Os dados para correção das medições obtidas de cada sensor são inseridos em SensorDB e a partir dele disponibilizados para Control, e eventualmente ao próprio DAQ.

Com relação a esta condição, os seguintes ataques são identificados:

A1 - Modificação deliberada ou acidental dos dados de calibração dos sensores. Este ataque é lançado contra SensorDB e pode ocorrer antes do teste, no momento da calibração de um sensor ou ainda em posteriormente, por ação deliberada do atacante.

A2 - Negação de Serviço (DoS) em SensorDB. Este ataque consiste em tornar SensorDB indisponível para acesso, seja pelo envio excessivo de pacotes de requisição ao banco de dados ou ainda por quebra do canal de comunicação.

Em uma breve análise, ambos os ataques exploram vulnerabilidades cujas alternativas de solução são bem conhecidas. Entende-se que a segurança de um sistema de banco de dados é um assunto extensamente abordado na literatura, e diversas abordagens são passíveis de aplicação aqui.

4.2. Autenticação dos sensores e integridade das medições

Esta condição está associada especificamente aos sensores, ao DAQ e às interações entre eles que ocorrem durante o teste de impacto. Qualquer erro ou falha pode implicar na perda de dados e consequentemente na invalidação do teste.

Com relação a esta condição, os seguintes ataques são identificados:

A3 - Substituição de sensor calibrado por um não calibrado. Um atacante que tenha acesso ao arranjo físico dos sensores pode substituir o sensor esperado por um devidamente modificado para gerar medições espúrias.

A4 - Perturbação dos parâmetros físicos do sensor. Tal como em *A3*, um atacante pode inserir qualquer elemento que perturbe aspectos físicos do sensoriamento.

A5 - Envio de comandos espúrios para o DAQ. Quando o DAQ suporta comandos remotos, um atacante pode explorar a segurança destas interfaces.

A6 - Modificação deliberada ou acidental dos dados coletados. Este ataque pode incidir de diferentes formas, em quaisquer dos canais de comunicação disponibilizados pelos sensores e pelo DAQ, ou ainda nos dados armazenados pelo DAQ.

Dos ataques mencionados, *A3* e *A4* são ataques de natureza física. A substituição de um sensor calibrado por outro malicioso pode ser prevenida por autenticação do sensor. A possibilidade de se ter mecanismos para tal depende da tecnologia utilizada. Sensores analógicos, por exemplo, não possuem eletrônica suficiente para implementar uma autenticação tradicional. Neste caso, o mais adequado é que o sensor e o componente de digitalização do DAQ sejam vistos como um único elemento no escopo da autenticação. Já para os sensores inteligentes podem ser propostos mecanismos de autenticação mais sofisticados. De fato, algumas soluções comerciais de sensoriamento de testes de impacto baseadas em sensores inteligentes alegam possuir mecanismos de autenticação. Por serem soluções fechadas não é possível avaliar sua eficácia. Entretanto, existem soluções para esse problema na literatura, com é o caso do cronotacógrafo digital citado na seção 2. Por sua vez, a perturbação de parâmetros físicos do sensor pode ser detectada por algoritmos que avaliem sua resposta. Uma perturbação não será capaz de produzir respostas coerentes, e muito provavelmente afetará outros sensores, podendo ser identificada por sistemas de detecção de anomalias.

O ataque *A5* constitui também um problema de autenticação. Uma vez que o DAQ passe a exigir credenciais para qualquer execução de comandos em suas interfaces, esse ataque é mitigado e mesmo eliminado se o sistema de autenticação for suficientemente seguro. Estas solução já existem para muitos dispositivos e o poder computacional disponível no DAQ é suficiente para implementar uma delas.

O ataque *A6*, por sua vez, diz respeito especificamente à garantia de integridade das informações. Este ataque pode ocorrer em diferentes partes no fluxo de informações do processo de teste, uma vez que a informação pode ser corrompida já no momento de sua digitalização pelo DAQ, ou ainda no envio da mesma para Control. Independente do momento quando ocorre o ataque, diferentes técnicas para prover integridade podem ser utilizadas. É possível, por exemplo, se prevenir ataques de falsificação da informação protegendo-se os canais de troca de dados, por meio do uso de tecnologias vastamente exploradas. É possível ainda o uso de mecanismos para verificação da integridade da

informação em cada etapa, rastreando sua origem ao ponto mais primário possível. No caso dos sensores inteligentes, é possível estabelecer uma política de chave pública, sendo que cada sensor tem uma chave privada e suas medições são assinadas digitalmente. Embora abordagens similares possam apresentar complexidade em termos de custo computacional e implementação, existem propostas eficientes para tal.

4.3. Verificação da utilização dos sensores no teste de impacto

Embora em um primeiro momento esta condição pareça trivial, sua verificação é importante em face de dois ataques relativamente simples, todavia plausíveis. Estes ataques são descritos a seguir:

A7 - Uso de sensores diferentes daqueles que foram previamente calibrados. Essa é uma variação do ataque descrito em *A3*, todavia se considera aqui que um arranjo completo de sensores foi modificado, como a substituição de um ATD completo.

A8 – Uso dos sensores calibrados em um ambiente que diferente do teste de impacto. Este ataque constitui uma tentativa deliberada de fraude, pois envolve a preparação de um ambiente específico para se produzir dados de teste falsos.

No ataque *A7*, a substituição dos sensores pode ocorrer por razões não intencionais ou mesmo intencionais. Em uma situação não intencional, por exemplo, pode haver por parte dos responsáveis a intenção de omitir o ocorrido, em virtude dos custos envolvidos em uma eventual repetição dos testes. Entretanto, a solução para o problema é a mesma descrita em *A3*.

O ataque *A8*, por sua vez, difere dos demais ataques pelo fato de que a autenticação dos sensores e aquisição de dados pode ocorrer normalmente, dentro do ambiente forjado para os testes. Considere-se como ilustração uma situação onde um veículo será submetido a um teste de impacto de homologação. Em paralelo, um ambiente a parte é preparado para simular uma colisão cujo comportamento dinâmico estará em conformidade com parâmetros avaliados. Ao mesmo tempo em que o veículo é submetido ao teste, o conjunto de instrumentação que deveria estar embarcado no veículo é "testado" no ambiente de simulação. A coleta de dados ocorre normalmente, estes são transmitidos e disponibilizados para a análise em Control. Os sensores foram autenticados, os dados estão íntegros, mas os sensores não estavam dentro de veículo.

Conforme discutido nesta seção, todos os ataques identificados, com exceção de *A8*, possuem contramedidas conhecidas na literatura, algumas delas muito bem consolidadas, tais como os mecanismos baseados em assinatura digital para prover integridade das informações. No entanto, no caso do ataque *A8*, não é do conhecimento dos autores abordagens que se proponham a solucionar o problema. Na próxima seção deste trabalho, é apresentada uma ideia original para o mesmo, que se baseia no uso dos sistemas de visão computacional para identificação física dos sensores utilizados.

5. Proposta para autenticação dos sensores a partir de imagens

Na seção anterior, foi apresentado que o ataque *A8* explora condições específicas de fraude na qual um teste de impacto ocorre sem que sua instrumentação esteja de fato embarcada no veículo. Para se evitar este ataque é necessário o uso de algum mecanismo que permita identificar os sensores embarcados dentro do veículo e

confirmar que os mesmos correspondem àqueles previstos para tal na etapa de calibração. Intuitivamente, é natural que se considere o uso de tecnologias comuns para transmissão de um identificador único, como RFID ou redes sem fio. Entretanto, conforme discutido na seção anterior, tecnologias que se baseiam unicamente na transmissão de dados podem ser utilizadas no conjunto correto de sensores em um teste simulado, que ocorre em paralelo com o teste real. Outras tecnologias, por sua vez, podem requerer a instalação de antenas e equipamentos adicionais, poluindo fisicamente o espaço destinado à colisão do veículo e mesmo interferindo nos resultados dos testes.

Como alternativa nossa proposta se baseia no uso das câmeras de alta velocidade, já presentes no cenário de teste, para identificar os sensores utilizados. A identificação é feita por meio de um sinal luminoso processado no próprio vídeo, que permite identificar de forma única um determinado sensor dentro do campo visual da câmera.

Para viabilizar a proposta, assumem-se as seguintes pré-condições:

a) Cada sensor a ser identificado possui associado a ele um dispositivo luminoso visível (por exemplo, um LED), seja sobre a superfície do veículo ou interno a este. O dispositivo luminoso é acionado pelo próprio sensor ou então pelo DAQ respectivo, caso se trate de um sensor analógico;

b) Cada sensor a ser identificado está dentro do campo visual de alguma das câmeras usadas no teste de impacto, dentro do período de intervalo definido para que o sensor emita seu identificador visual.

O período de intervalo em questão corresponde ao tempo disponível durante o teste de impacto no qual cada sensor deve emitir sua identificação, por meio de seu dispositivo luminoso. Essa identificação corresponde a um código de autenticação exclusivo do sensor, que pode ser verificado por meio de uma política de chaves. O identificador é emitido usando-se uma representação binária no dispositivo luminoso (zero quando apagado, um quando aceso) e esta informação pode ser recuperada por meio de processamento do vídeo associado à câmera respectiva. Cada um desses aspectos será tratado em detalhes nas subseções que se seguem.

5.1. Tempo disponível para propagação do identificador de um sensor

Um aspecto prático que precisa ser considerado é a questão do tempo disponível para propagação do identificador de cada sensor por meio do dispositivo luminoso. Para tanto, é necessário considerar não apenas o tempo real disponível, como também a disponibilidade de recursos para processamento desta informação.

Durante o teste de impacto, após o veículo ser liberado pelo mecanismo auxiliar de aceleração, o tempo que envolve a colisão é muito curto. Segundo Snider (1967), todos os eventos relevantes (desaceleração, a absorção do impacto por elementos de segurança e deformação do veículo) ocorrem em um tempo aproximado de 200 milissegundos. Todavia, se for considerado o tempo no qual o veículo está próximo à área de impacto, ou seja, desde sua liberação até a parada após a colisão, pode-se estabelecer um período de tempo entre 1 a 2 segundos. Por questões práticas, estamos considerando o tempo de um segundo como o disponível para que os sensores emitam seus respectivos identificadores. A proximidade do veículo com a área de impacto é

essencial porque nesta condição existem mais câmeras disponíveis para monitoramento de diferentes grupos de sensores.

5.2. Processamento do identificador exibido por dispositivo luminoso

Como já apresentado em linhas gerais, este trabalho propõe que o identificador exibido pelo sensor por meio do dispositivo luminoso seja recuperado a partir do processamento de vídeo de uma câmera de alta velocidade utilizada no teste de impacto. Tal como descrito na seção 3, o processamento de vídeo para se inferir resultados de um teste de impacto é algo usual nas ferramentas comerciais atualmente disponíveis. Assim, o que se propõe aqui é que os mesmos recursos sejam utilizados para se processar um sinal que é propagado em vídeo por meio do dispositivo luminoso do sensor.

Para tanto, considere-se o vídeo gerado por uma câmera durante o teste de impacto, e que o mesmo possui em sua área de imagem um determinado sensor para os qual se deseja recuperar o identificador emitido. Espera-se que a cada quadro seja possível identificar o sinal luminoso por meio de processamento de imagem, determinando-se se o mesmo encontra-se apagado ou aceso, o que em codificação binária equivale à representação de zero ou um respectivamente. Os principais protocolos de definição de testes de impacto estabelecem que a taxa mínima de quadros gerados por uma câmera deve ser de mil quadros por segundo, que para fins de praticidade consideramos com 1024 quadros. Em circunstâncias ideais, seria possível recuperar neste intervalo de tempo 1024 bits, fazendo com que os dispositivos luminosos sejam sincronizados com o sinal de vídeo da câmera. No entanto, a instalação de uma estrutura para sincronismo de sinal no ambiente de testes pode ser complexa. Seria necessário prever o uso de diversos cabos de sincronismo ligados à câmera ou ainda um sistema de sincronismo sem fio, o que pode não ser factível. Será analisada assim a possibilidade de propagação e captura do identificador de forma assíncrona.

Considere-se inicialmente que os sensores são programados para propagar seu identificador na mesma frequência de captura de quadros da câmera. No entanto, pelo fato de não haver um sincronismo de sinal, algumas condições especificas podem ocorrer, as quais são descritas a seguir.

Primeiramente, em virtude do erro acumulado na diferença de frequência, em algum momento pode ocorrer uma das seguintes situações: a perda de um bit quando a frequência de propagação do identificador é levemente maior do que a frequência interna da câmera ou a leitura duplicada de um bit quando o oposto. Esse problema é um caso comum na transmissão de dados digitais sobre um canal não confiável, e pode ser tratada pelo uso de um algoritmo de FEC (*Forward Error Correction*), levando-se em consideração apenas o *overhead* de bits de correção de dados.

A segunda condição é que, em função da defasagem do sinal, existe a possibilidade remota do dispositivo luminoso ter sua transição de sinal sobreposta ao instante de abertura do obturador da câmera. Em consequência, este sinal assumiria no frame de vídeo um estado indeterminado, sem que o algoritmo de processamento de imagens consiga determinar com exatidão se seu valor é zero ou um. Este problema pode ser eliminado se a frequência de propagação do identificador for definida como a metade da frequência de captura de quadros da câmera, de modo que é esperado que

cada bit do identificador seja propagado em dois frames. Em consequência, a disponibilidade de bits para composição do identificador é reduzida pela metade.

Em face destas condições, nossa proposta define que o identificador deve ser propagado com a metade da frequência disponível para captura de vídeo, o que equivale a 500 Hz, o que arredondamos para fins de praticidade para 512 Hz. Esta alternativa tem ainda como vantagem o fato de tornar desnecessário o uso de um algoritmo de FEC, uma vez que a perda ou duplicação de bits pode ser apropriadamente tratada com a duplicação dos mesmos. Deste modo, nossa proposta passa a considerar que se dispõe de um pacote de até 512 bits para encapsulamento do identificador de um sensor.

5.3. Composição do identificador de um sensor

Para a composição do identificador do sensor, alguns aspectos precisam ser levados em consideração. Primeiramente, esse identificador deve ser único e sua verificação deve estar fortemente associada ao sensor, de modo a garantir que somente este seja capaz de gerar o identificador. Um aspecto secundário diz respeito à propagação deste sinal. Por se tratar de um processamento assíncrono, não é possível transmitir apenas o identificador; é necessário se acrescentar um preâmbulo ao pacote, que sirva como sinal de sincronismo, viabilizando assim o processamento do mesmo pelo sistema de visão computacional. Por fim, preâmbulo de sincronismo e identificador devem ser acomodados dentro de um pacote limite de 512 bits, conforme visto na seção 5.2.

Para garantir que o identificador seja único, nossa proposta se baseia no uso de uma política de chave pública. Para tanto consideramos que cada sensor possui um par de chaves. A chave privada é embarcada no sensor, e não pode ser extraída deste. A chave pública é informada pelo sensor no momento da calibração e faz parte dos dados disponíveis em SensorDB. No caso dos sensores analógicos, é possível propor que a atribuição das chaves estaria associada ao canal do DAQ respectivo, observando-se as mesmas premissas já definidas quanto à política de chaves.

Uma vez definido o uso de um par de chaves, um identificador único pode ser obtido por meio da assinatura digital de uma informação conhecida tanto pelo sensor quanto pelo processo responsável pela verificação deste identificador. Por praticidade, definiremos esta informação como R. O valor de R pode ser definido de diferentes formas. Um exemplo é a concatenação dos últimos n valores aferidos pelo sensor imediatamente antes do início da propagação do identificador pelo dispositivo luminoso, ou ainda simplesmente um valor aleatório qualquer. Deste modo, para se obter o identificador I de um sensor qualquer, define-se a seguinte expressão:

$$I = R \oplus sign(K, hash(R))$$

Onde *hash()* e *sign()* são respectivamente funções para geração de um resumo criptográfico e para criptografar um *string* usando a chave privada K do sensor, e $\oplus$ o operador de concatenação.

Resta agora definir quais algoritmos criptográficos devem ser adotados para as funções *hash()* e *sign()* em função do tamanho L definido como o número máximo de bits disponíveis para propagação do identificador. Seja P o preambulo de dados usado como sinal de sincronismo na propagação do identificador, tem-se que:

$$L \geq length(P \oplus I)$$

Onde *length()* é a função que informa o comprimento de um *string* de texto.

Pelas conjecturas definidas na seção 5.2., temos que o valor de L deve ser inferior a 512 bits. Portanto, o mesmo se aplica ao comprimento do preambulo de sincronismo concatenado com o identificador. O identificador, por sua vez, tem como prefixo o valor de R. A princípio, ambos P e R podem ter seus tamanhos arbitrados. Considerando-se que 16 bits sejam suficientes para cada um deles, temos um restante de 480 bits disponível para a assinatura digital de R, que é efetivamente a parte mais importante do identificador. Este tamanho impede o uso do algoritmo RSA para tal aplicação, uma vez que o tamanho mínimo para uma chave RSA, conforme recomendado pelo NIST, é de 1024 bits. A alternativa é, portanto, o uso de um algoritmo de curvas elípticas, que propicia o mesmo nível de segurança com chaves bem menores. Além disso, os algoritmos de curvas elípticas são mais adequados para implementação em dispositivos com recursos computacionais limitados, como é o caso de um sensor.

Em face disso, optamos por adotar os mesmos algoritmos usados em Camara et al. (2012), que são a função SHA-224 como *hash()* e algoritmo ECDSA 224 bits como *sign()*, equivalente em segurança ao RSA com chaves de 2048 bits. As funções escolhidas resultam em uma assinatura digital de 448 bits, suficiente para o tamanho limite de 480 bits já determinado em função de P e R. Ao mesmo tempo em que satisfazem as condições estabelecidas para propagação do identificador, estes algoritmos permitem a geração de um identificador único, com um elevado grau de confiabilidade.

6. Experimentos e discussões

6.1. Experimento prático com uma câmera de alta velocidade

Com o objetivo de demonstrar a factibilidade da proposta apresentada, foi realizado um experimento com uma câmera de alta velocidade para se demonstrar que é possível recuperar um identificador propagado por um sinal luminoso a partir do processamento de vídeo.

O experimento foi realizado utilizando um LED conectado à saída de um gerador de sinais, modelo 33220A do fabricante Agilent, para simular o envio de dados do sensor na frequência de 500 Hz. O sinal gerado constitui em uma onda quadrada com *duty cycle* de 50 % e amplitude variando de 0 a 5 Volts. Uma câmera de alta velocidade, modelo M310 do fabricante Vision Research, foi configurada com de resolução de 1200x800 e taxa de aquisição de 1000 quadros por segundo para realizar um teste de validação dos dados simulados pelo LED. A Figura 2 mostra o experimento monitorado a partir de um osciloscópio. A linha amarela indica o sinal de captura de vídeo, enquanto o sinal verde mostra a onda quadrada usada para ativação do LED. Como é possível observar, o momento de captura do quadro, que ocorre na borda de descida do sinal, coincide com posições nas quais o sinal do LED representa estados diferentes, que para a onda quadrada em questão correspondem aos valores zero e um. No exemplo demonstrado, cada quadro captura um bit diferente de informação, evidenciando que possível se recuperar um identificador propagado no sinal de vídeo.

Figura 2: Experimento prático demonstrando recuperação do identificador

6.2. Discussões e próximos passos

O resultado do experimento realizado teve por objetivo demonstrar a viabilidade da ideia proposta para recuperação do identificador de determinado sensor usando o próprio sistema de câmeras já presente em um teste de impacto. Entretanto, diversos aspectos práticos da implementação dessa proposta podem ser citados e endereçados como os próximos passos em nossa investigação.

O primeiro aspecto diz respeito à própria implementação do firmware responsável pelo cálculo e propagação do identificador. Embora os sensores inteligentes modernos tenham avançado significativamente em termos de recursos computacionais, é necessário se estimar quais os requisitos mínimos necessários para que este dispositivo suporte as funcionalidades requeridas pelo firmware em questão. Uma alternativa já cogitada é que o identificador seja gerado pelo próprio DAQ, o qual pode ser facilmente dimensionado para suprir esses recursos computacionais.

Outro aspecto está relacionado ao processamento de vídeo para recuperação do identificador. A literatura apresenta diversos algoritmos de visão computacional voltados para a identificação e acompanhamento (*tracking*) de elementos de interesse [Yilmaz et al. 2006]. Entretanto, em um teste impacto, os sensores sofrerão movimentos bruscos em função da propagação da onda de choque do veículo com a barreira. Em função deste movimento indeterminado, algumas dificuldades podem se apresentar, como a obstrução do sensor no campo visual da câmera por um determinado instante, por exemplo. Consequentemente, este aspecto do problema requer uma investigação mais profunda, para se identificar quais algoritmos melhor se adequam às condições descritas. Uma alternativa que pode ser investigada é o uso de mais de uma câmera por sensor, de modo que informações que venham a ser perdidas por uma câmera possam ser recuperadas a partir do vídeo de câmeras secundárias.

7. Conclusão

Neste artigo foi apresentado um estudo amplo sobre a segurança cibernética no sensoriamento e instrumentação dos testes de impacto de veículos. Como apresentado, estes testes são cruciais para se garantir que um determinado veículo atende a requisitos

específicos de segurança. A confiabilidade das informações de teste é, por sua vez, requisito para se legitimar os resultados do mesmo.

São duas as principais contribuições deste trabalho. A primeira é a apresentação do modelo de ataque descrevendo em detalhes ameaças e vulnerabilidades às quais um teste de impacto está sujeito, e que podem ser exploradas de diferentes formas por um atacante mal intencionado. A segunda é a ideia original de atribuir a cada sensor um identificador único que é propagado por um dispositivo luminoso durante o teste de impacto e pode ser recuperado usando-se o sistema de câmeras de alta velocidade já utilizado nos testes. Essa ideia pode ser explorada de diversas formas, e por si só abre espaço para investigações ainda mais detalhadas no campo de visão computacional e tratamento de sinais digitais.

Referências

Bacchieri, G. and Barros, A. J. D. (2011) "Acidentes de trânsito no Brasil de 1998 a 2010: muitas mudanças e poucos resultados", Saúde Pública, 45(5), p. 949–963.

Camara, S., Machado, R., Pirmez, L. and Carmo, L. F. R. C. (2012), "Uma arquitetura de segurança para medidores inteligentes – verificação prática de dados de energia multitarifada", Anais do XII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais (SBSeg), p. 221-234.

Caveney, D. (2010). "Cooperative Vehicular Safety Applications. IEEE Control Systems", 30(4), p. 38–53.

Colak, M., Bishop, J., Nordvik, P. J., Mahieu, V. and Loeschner, J. (2012), "Cryptographic security mechanisms of the next generation digital tachograph system and future considerations". In: Joint Research Centre Scientific and Policy Report, European Commission, Ispra, Italy.

Han, K., Potluri, S. D. and Shin, K. (2013), "On authentication in a connected vehicle: secure integration of mobile devices with vehicular networks", In: ACM/IEEE International Conference on Cyber-Physical Systems (ICCPS), 2013, p. 160–169.

Hobbs, C. A. and McDonough, P. J. (1998). "Development of the European new car assessment programme (Euro NCAP)", Regulation, 44, p. 3.

Paine, M. and Haley, J. (2008). "Crash testing for safety - possible enhancements to ANCAP test and rating methods", In: Australasian Road Safety Research Policing Education Conference, p. 33–42.

Snider, H. P. (1964), "Vehicle Instrumentation for Crash Testing", In: *IEEE Transactions on Industrial Electronics and Control Instrumentation*, 11(1), p. 44–49.

Sorber, J., Shin, M., Peterson, R. and Kotz, D. (2012), "Plug-n-Trust: Practical Trusted Sensing for mHealth", In: Proceedings of the 10th International Conference on Mobile Systems, Applications, and Services, p. 309–322.

Yilmaz, A., Javed, O. and Shah, M. (2006), "Object Tracking: A Survey", In: ACM Journal of Computing Surveys, 38(4), p. 1-45.

