Ciber(in)segurança da Infraestrutura de Transportes Públicos

Nelson Nobre Escravana

Engenheiro informático pelo IST com especialização em Gestão pelo ISEG. Tem efetuado no INOV INESC Inovação (Instituto de Novas Tecnologias) atividades associadas à criação e desenvolvimento de software para sistemas embebidos, de aplicações para operadores de telecomunicações móveis, consultadoria em segurança informática, análise de risco e auditorias de segurança com ênfase em testes de penetração. Atualmente coordena a área de Comunicações do INOV onde se inclui a área de investigação e desenvolvimento em cibersegurança.

João Lima

Aluno finalista de Engenharia Informática e Computadores do IST e investigador de segurança informática no INOV INESC Inovação.

Carlos Ribeiro

Licenciado em Engenharia Electrotécnica, mestre e doutor em Engenharia Informática e docente neste departamento do Instituto Superior Técnico. Tem duas obras publicadas sobre arquitetura de computadores e sistemas operativos. De 1995 a 1998 foi consultor de segurança do Gabinete Nacional de Segurança. Entre 2008 e 2011 foi vice-presidente do conselho diretivo do centro de informática do Instituto Superior Técnico. É, desde Janeiro de 2012, pró-reitor da universidade técnica de Lisboa para a área das tecnologias de informação.

Resumo

A insegurança informática tem estado principalmente associada a ataques a computadores pessoais, ao furto de cartões de crédito ou aos ataques de negação de serviço aos sítios de internet de organizações de alta visibilidade. No entanto com a recente proliferação de ataques informáticos de elevada complexidade e eficácia, tem crescido entre os operadores de transportes públicos a necessidade de aumentar a resiliência da sua infraestrutura informática contra este tipo de ataques.
Não obstante já existir um conjunto considerável de ferramentas construídas com o objetivo de prevenir e detetar ataques informáticos, estas não estão devidamente adaptadas às necessidades específicas de proteção de infraestruturas críticas. A nossa proposta consiste numa ferramenta de deteção de intrusões especialmente construída para ambientes com um elevado nível de automação e cujos processos podem ser facilmente descritos. O sistema desenvolvido pode ser uma forma especialmente eficaz de detetar ataques nas infraestruturas de transportes públicos e, por extensão, ser utilizada na proteção de infraestruturas críticas em geral.

Abstract
Cyber-(in)security in Public Transportation Infrastructure

Cyber-(in)security has been mainly associated with attacks to personal computers, credit card theft or denial-of-service attacks to high-visibility organization's websites. However, with the recent proliferation of cyber-attacks aimed at critical infrastructures, have been growing among public transport operators the need to increase the resilience of their technological infrastructure against this type of attacks.
Despite the significant amount of tools developed in order to prevent and detect cyber-attacks, these tools were not adequately adapted to the specific needs of critical infrastructure protection. Our proposal consists of an intrusion detection tool specifically developed to be used in environments with a considerable level of automation, whose processes may be easily described. These processes may be an especially effective way to detect attacks not only in public transport infrastructures but also in critical infrastructures in general, thus increasing their protection.

Introdução

Ao longo do tempo as organizações têm vindo a adotar um número significativo de sistemas e tecnologias de informação e comunicação (TIC) como forma de automatizar e melhorar os seus processos, ao mesmo tempo que reduzem a dependência do trabalho manual. O uso desses sistemas teve origem em pequenas aplicações cujos objetivos diferem entre melhorar e acelerar a comunicação entre colaboradores, clientes e fornecedores, substituir processos manuais e mecânicos por processos automatizados praticamente sem intervenção humana e melhorar a segurança face a acidentes (*safety*), tendo crescido para aplicações críticas que controlam quase todos os processos e operações de uma organização.

Esta automatização, resultante da introdução das TIC, é comum a praticamente todos os setores da sociedade, incluindo aqueles que são atualmente considerados pela Comissão Europeia (The Council of the European Union, 2008; The Council of the European Union, 2007) como infraestruturas críticas nacionais (ICN) abrangendo setores como a energia (eletricidade, petróleo e gás), águas e transportes (terrestres, marítimos e aéreos) e muitos outros, desde o setor financeiro até à generalidade do tecido empresarial.

Os centros urbanos cresceram significativamente, quer em tamanho, quer em população, nas últimas décadas e consequentemente as infraestruturas de transportes sofreram alterações como forma de suportar as necessidades de mobilidade de pessoas e bens. Com o crescimento das redes de transportes, a tarefa de manualmente gerir e operar cada linha dos vários sistemas de transportes tornou-se complexa. Como forma de lidar com este problema, os Operadores de Transportes Públicos (OTP) criaram um conjunto de sistemas de informação de forma a automatizar as suas operações, tornando-as ao mesmo tempo mais seguras, reduzindo a dependência do controlo humano, muitas vezes sujeito a falhas.

Ataques terroristas à infraestrutura de transportes públicos como aqueles observados em 20 de março de 1995 em Tóquio, 11 de março de 2004 em Madrid, e posteriormente em 7 de julho de 2005 em Londres mostraram a criticidade do papel que estas têm na sociedade, e ao mesmo tempo quão vulneráveis são.

O advento das Tecnologias de Informação, aliado a más práticas de codificação, instalação e administração de sistemas, trouxe também um conjunto de problemas de segurança. Aliado à questão tecnológica, encontra-se o facto do desenho dos processos de negócio dos operadores de transportes públicos, tal como de várias outras

ICN, não ser na sua maioria pensado de raiz com as preocupações de segurança face a ataques maliciosos (*security*), nomeadamente de ciber-segurança, mas antes com preocupações de segurança face a acidentes e ações não intencionais (*safety*). Tal resulta fundamentalmente destes sistemas terem sido desenhados para ambientes controlados onde escasseavam "predadores", mas também da ausência de soluções de segurança específicas para sistemas tão especializados como os sistemas dos OTP.

Genericamente, os sistemas informáticos são diariamente sujeitos a um grande número de ataques com o objetivo de interromper o seu funcionamento, ganhar acesso a estes, ou retirar-lhes informação valiosa. Os sistemas de informação e gestão da rede dos OTP não são exceção.

Que seja do nosso conhecimento, nenhum ciberataque de larga escala às redes de transportes públicos foi reportado, no entanto a sua criticidade aliada às vulnerabilidades usualmente existentes em sistemas informáticos levantam preocupações quanto à sua proteção.

Tome-se como exemplo um ataque conduzido por um estudante polaco de 14 anos que, usando apenas um comando de TV modificado, foi capaz de tomar o controlo de uma rede de elétricos, mudando as agulhas da linha à sua vontade. As únicas consequências deste ataque foram alguns comboios descarrilados, e algumas pessoas com ferimentos ligeiros. No entanto, a facilidade e reduzido esforço necessário para o conduzir, mostra quão vulneráveis estes tipos de infraestruturas estão.

Apesar das ameaças de segurança das TIC serem tão antigas como as mesmas (devemos recordar episódios como a interferência em transmissões morse no início do século XX, ou a guerra de grupos de *hackers* na década de 80) foi recentemente após episódios como o ataque ao Pentágono em 2008, o ataque à rede Sony, o ataque à Lockheed Martin, e culminando no *Stuxnet* (Falliere *et al*, 2011), dirigido aos sistemas de supervisão, controlo, automação e aquisição de dados (SCADA) de uma central nuclear iraniana em 2010, que emergiu o facto de que os tradicionais *script kiddies* e *hackers* individuais ou em pequenos grupos estão a ser substituídos por grupos altamente organizados e com capacidade para desferir poderosos ataques. Sendo as infraestruturas críticas um alvo apetecível para ciberataques de larga escala que apenas começaram a ser explorados, urge identificar mecanismos para a sua proteção.

Os sistemas de deteção de intrusões (IDS) apresentam-se como uma das soluções para aumentar o nível de proteção de qualquer infraestrutura informática, e por consequência as infraestruturas informáticas de suporte de infraestruturas críticas. No entanto, historicamente estes sistemas sofrem de um conjunto de problemas de eficácia, dado o número elevado de falsos alarmes gerados (Axelsson, 2000) que fazem com que os responsáveis de segurança das organizações estejam muitas vezes demasiado ocupados a distinguir os verdadeiros alarmes de entre os alarmes gerados, limitando assim a sua capacidade de resposta. Este número elevado de falsos alarmes não resulta tanto da ineficiência dos sistemas de deteção

de intrusos, que apresentam taxas de eficácia da ordem dos 99%, mas sim da elevada quantidade de informação a tratar o que é usualmente designada por *base-rate fallacy* (Axelsson, 2000).

Como solução para alguns dos problemas identificados acima, o INOV desenvolveu um sistema de deteção de intrusões híbrido (patente pendente), que combina técnicas de deteção de assinaturas (*misuse detection*), com técnicas de deteção baseadas em especificações (*specification-based*) de processos de negócio. As primeiras com o objetivo de detetar eficientemente ciberataques já conhecidos e as segundas como forma de detetar desvios da execução dos sistemas face ao especificado.

A grande vantagem desta solução é, não só, a capacidade de detetar ataques que explorem vulnerabilidades não conhecidas mas também ataques que resultem de comportamento malicioso, sem, no entanto, sofrer dos problemas do elevado número de falsos positivos que os sistemas de deteção de intrusos baseados na deteção de anomalias têm (Debar *et al*., 1999).

Tecnologias de Informação nas Redes de Transportes Públicos

O uso de tecnologias de informação tem crescido ao longo do tempo como forma de apoiar os operadores de transportes públicos a prestar um serviço melhor e mais seguro aos seus clientes.

Apesar da sua relevância não são conhecidas descrições detalhadas ou mesmo superficiais das tecnologias de informação utilizadas nas redes de transportes públicos o que dificulta a avaliação das vulnerabilidades do sistema e o desenho de tecnologias de proteção contra ciberataques. É pois particularmente pertinente a realização de uma avaliação, ainda que breve, sobre os sistemas em causa. Dado que a par da aviação, a rede metropolitana de comboio (de agora em diante Metro) é o tipo de redes de transporte em massa cuja infraestrutura tecnológica é mais complexa, foi esta a escolhida para uma breve análise. Desta resultaram cinco grupos de sistemas que serão descritos de seguida.

Sistemas de Bordo

Os sistemas de bordo são os utilizados para gerir tudo aquilo que acontece dentro dos veículos, ou está relacionado com o seu movimento. O conjunto de funcionalidades que estes sistemas oferecem é diverso, passando pelo controlo físico do veículo, até à disponibilização de informação aos passageiros:

- O Sistema de Informação aos Passageiros (SIP) é não só responsável por informar os passageiros acerca do tempo estimado até à chegada à próxima

paragem, mas também acerca das condições atuais de circulação, conexões com outros meios de transporte, e até, em alguns casos, oferecer acesso a internet sem fios;
- Por outro lado, o Sistema de Bilhética é usado para receber dos passageiros o pagamento pelas viagens que estão a realizar, bem como validar os seus títulos de transporte;
- Finalmente, e talvez mais importante, o Sistema de Controlo e Seguimento do Veículo é usado para controlar, monitorizar e operar todos os componentes eletromecânicos do veículo. De entre estes componentes estão incluídos os subsistemas de propulsão, travagem, e deteção de obstáculos, sendo estes componentes vitais para o correto funcionamento do veículo.

Em alguns casos, a operação dos veículos é inteiramente assegurada por este sistema. Nesses casos, este grupo de sistemas assume um caráter ainda mais crítico, dado que este é responsável pela operação do veículo, quer seja em condições normais ou numa emergência. É também responsabilidade deste sistema o cálculo da posição atual do veículo, para que os sistemas auxiliares possam determinar a zona até onde este pode avançar em segurança.

Sistemas de Linha

Neste grupo de sistemas constam todos os sistemas instalados ao longo das linhas, e que gerem a interação dos veículos com os sistemas de controlo centrais. Uma linha é usualmente dividida em várias zonas, sendo que cada zona contém uma instância dos sistemas abaixo:

O Sistema Automático de Gestão de Velocidade é o sistema de terra responsável por interagir com o Sistema de Controlo do Veículo. A sua principal função é calcular o ponto que pode ser atingido com segurança por cada um dos veículos sem que se corra o risco destes colidirem ou se aproximarem demasiado;

Por sua vez, o Sistema de Controlo de Zona interliga os diversos sensores e controladores existentes numa zona da linha tais como as agulhas, passagens de nível, energia e equipamento de sinalização, e gere o seu estado de acordo com os veículos em circulação nessa zona.

Sistemas de Estação

As estações, como agregadores de pessoas por excelência, estão equipadas com um conjunto de sistemas desenhados com o objetivo de assistir os passageiros a alcançar os transportes desejados de forma rápida, fácil e confortável:

- Nas estações, o Sistema de Informação a Passageiros (SIP) tem um papel central. A sua principal função é ajudar os passageiros a movimentar-se dentro das estações, dado que tem o conhecimento das plataformas a que os veículos esperados pelos passageiros irão chegar. Da mesma maneira, em caso de emergência, este sistema é usado para encaminhar os passageiros para uma localização segura;
- O Sistema de Controlo de Estação gere, controla e monitoriza os diversos componentes eletrónicos e eletromecânicos existentes numa estação, tal como as portas das plataformas, elevadores, escadas rolantes, sistemas de deteção e supressão de incêndios, etc.;
- O Sistema de Bilhética é utilizado não só para vender títulos de transporte aos passageiros, mas também para os validar, e consequentemente permitir o acesso dos passageiros às diversas plataformas existentes na estação.

Sistemas de Centro de Controlo de Operações

Como forma de centralizar a gestão e operação das diversas linhas à responsabilidade de cada operador, estes criaram centros de controlo de operações que assumem esta função que, por consequência, contam com um conjunto significativo de sistemas de apoio:

- A gestão e operação de uma linha em que circulam um número considerável de veículos ao mesmo tempo seria muito difícil sem a existência de um Sistema de Controlo de Tráfego. O objetivo deste sistema é capturar, em alto nível, o estado da rede de forma a manter os operadores informados, e ao mesmo tempo permitir comparar este estado com o estado esperado dos veículos;
- O objetivo do Sistema de Controlo de Energia é monitorizar e controlar o estado da rede elétrica usada para mover os veículos. Este trabalha em colaboração com o Sistema de Controlo de Tráfego, de forma a saber os troços de linha que devem ter a energia ativada a cada momento;
- O Sistema de Videovigilância é usado para guardar e monitorizar as imagens de videovigilância das várias entidades na rede (veículos, estações, postos de transformação elétricos, etc.). Em algumas situações, estes sistemas usam capacidade inteligentes de processamento de vídeo, de forma a detetarem imagens às quais deve ser dada especial atenção pelos operadores;
- O Sistema de Gestão da Informação de Passageiros é responsável pela preparação, configuração e distribuição da informação a ser apresentada nos vários pontos, nomeadamente naqueles em que existem Sistemas de Informação de Passageiros em uso.

Tecnologias de Comunicação

A comunicação entre as várias entidades envolvidas numa rede de transportes é de extrema importância. Para além disto, os próprios sistemas usados nestas redes necessitam de comunicar de forma expedita e contínua, de forma a coordenarem a sua operação. Três tipos principais de redes de comunicação são tipicamente utilizados:

- Redes móveis profissionais, como o TETRA e o GSM-R são usadas não só para comunicação de voz entre os operadores e o pessoal de terra, mas também para executar pequenas aplicações de assistência à operação dos veículos. No futuro, é esperado que a rede GSM-R seja utilizada para possibilitar a interoperabilidade entre as redes de transportes de cada país;
- Redes sem fios, como o Wi-Fi, são usadas com dois propósitos: por um lado, são usadas por aplicações utilizadas nos veículos com necessidades de grande largura de banda, como seja a transferência de imagens de bordo para o centro de controlo de operações, e por outro lado para suportar a comunicação de aplicações críticas como a localização de veículos e cálculo de posição máxima permitida. No segundo caso é utilizada normalmente uma frequência especial;
- Finalmente, as redes cabladas são utilizadas para interligar as várias subredes existentes numa rede de transportes.

Iniciativas Europeias

Com os ataques terroristas de Tóquio, Madrid e Londres, a União Europeia aumentou a preocupação na procura de soluções de forma a aumentar a proteção das infraestruturas de transportes públicos.

Neste contexto, foram criados vários projetos de investigação e desenvolvimento, suportados pelos Programas Quadro da Comissão Europeia. Dois desses projetos, cuja relevância é maior relativamente a este trabalho são o COUNTERACT e o DEMASST.

COUNTERACT

O projeto COUNTERACT (*Cluster of User Networks in Transport and Energy Relating to Antiterrorist Activities*) é composto por um alargado consórcio industrial, e teve como principal objetivo aumentar a segurança contra ataques terroristas dirigidos a redes de transporte de passageiros e mercadorias, bem como infraestruturas de produção e distribuição de energia.

Este projeto foi conduzido a um alto-nível de abstração, apesar do seu foco na ameaça terrorista, de forma a identificar genericamente as vulnerabilidades nos domínios estudados.

No contexto deste projeto, foi realizada uma análise das ameaças a que estão sujeitos os domínios em estudo, tendo sido apontados os ataques por bombistas suicidas, a detonação remota de dispositivos explosivos improvisados (IED), os ataques incendiários, a vandalização da infraestrutura e as armas químicas, biológicas, radiológicas e nucleares (CBRN) como as principais ameaças (COUNTERACT Consortium, 2010).

A ciberameaça é apenas superficialmente endereçada, sendo no entanto referido que esta é considerada relevante, dadas as consequências que poderia ter quer no funcionamento da rede, quer em termos de vidas humanas.

DEMASST

O projeto DEMASST (*Demo for Mass Transportation Security: Roadmapping Study*), ao contrário do projeto COUNTERACT, teve como objetivo estabelecer o estado da arte da segurança nas redes de transportes, identificando pontos de melhoria e apontando uma estratégia para implementar as soluções propostas.

No estudo realizado acerca do estado da arte da segurança nas redes de transportes (DEMASST consortium 2009), e naquilo que à ciberproteção diz respeito, é referido que o esforço empregue pela maioria dos operadores para melhorar a sua proteção é baixo, limitando-se ao uso de mecanismos de proteção já oferecidos pelas tecnologias utilizadas.

Cibersegurança nas Redes de Transportes Públicos

Não obstante já terem sido realizados diversos projetos com foco na segurança em redes de transportes, a cibersegurança tem sido subvalorizada, e por vezes totalmente ignorada. Nos projetos descritos anteriormente, o fraco desenvolvimento desta área é associado ao facto de os operadores de transportes não possuírem o conhecimento suficiente para abordar o problema.

No entanto, a ciberameaça é unanimemente considerada como de elevado risco, cujas consequências caso fosse explorada seriam significativas. Michael *et al.* (2003) apresenta uma comparação entre um ataque cinético e um ciberataque usando uma análise quantificada de Schmitt, provando que os ciberataques têm consequências similares, se não superiores, aos ataques cinéticos.

Baseado no nosso estudo da infraestrutura TI das redes de transportes públi-

cos, foram identificados três cenários de ataque de alto nível, cuja realização teria consequências relevantes no normal funcionamento destas:

- Sequestro de veículo – um atacante que consiga ganhar acesso aos sistemas de controlo automático dos veículos pode dirigi-los para onde quiser, podendo fazer dois veículos colidirem em hora de ponta por exemplo;
- Disrupção da circulação numa linha – se um atacante for capaz de ganhar acesso a qualquer um dos sistemas de controlo de linha, ele consegue parar essa linha, e assim gerar o pânico e a confusão entre os passageiros;
- Manipulação da informação aos passageiros – os passageiros apoiam-se consideravelmente nos SIP para se movimentarem nas estações. Se um atacante for capaz de manipular a informação apresentada por esses sistemas, por exemplo gerando um false alarme de incêndio, este conseguiria gerar o pânico numa estação e assim pôr em causa a integridade física dos passageiros. Se esta ação for complementada com outras como por exemplo colocar as escadas rolantes e torniquetes em posição de entrada, as consequências podem ser dramáticas.

Sistemas de Deteção de Intrusão

Os Sistemas de Deteção de Intrusão (IDS) têm sido utilizados ao longo do tempo como forma de aumentar a proteção dos sistemas e infraestruturas de TI contra ataques. Um IDS pode ser definido como um sistema que monitoriza a atividade de um sistema, grupos de sistemas ou rede, de forma a detetar qualquer atividade ilícita executada neste, reportando as ilicitudes detetadas de forma estruturada e facilmente percetível pelos responsáveis de segurança.

Os IDS são usualmente classificados em três grandes eixos (Axelsson, 1999): (1) método de captura de dados, (2) arquitetura de sistema e (3) estratégia de processamento.

O primeiro diz respeito ao local onde são capturados os dados que servem de base à deteção, se na memória (persistente ou volátil) das máquinas que suportam as TI, se na rede que interliga as TI. O segundo está intimamente ligado à dimensão do sistema de deteção de intrusos e ao facto dele poder ser: uma instância única que colige e analisa os dados; um sistema centralizado com vários sensores que capturam dados e os enviam para uma unidade central de processamento; ou um sistema distribuído que captura e analisa os dados de forma distribuída. É, no entanto, o terceiro eixo de classificação que se afigura o mais importante para o problema a resolver.

Estratégia de Processamento

De forma a ser capaz de detetar intrusões, o IDS tem de ser capaz de processar os dados capturados, de forma a descobrir algo relacionado com alguma tentativa de intrusão, quer esta já tenha sido bem-sucedida ou não. Quanto à estratégia de processamento, consideramos a existência de três alternativas:

- Deteção de Assinaturas – de molde a detetar intrusões, estes sistemas utilizam assinaturas de ataques, que são criadas cada vez que um novo tipo de ataque é descoberto. Posto isto, estes sistemas têm como limitação o facto de apenas conseguirem detetar ataques para os quais uma assinatura já tenha sido produzida. O Snort (Roesch, 1999) é um exemplo de um sistema que utiliza assinaturas de ataques;
- Deteção de Anomalias – alguns sistemas baseiam a sua deteção em modelos de comportamento dos sistemas monitorizados, gerando alarmes quando são observados desvios a estes modelos. Estes sistemas têm uma fase inicial, chamada de aprendizagem, em que os modelos de comportamento dos sistemas a serem monitorizados são criados. No entanto, esta fase é considerada um dos pontos fracos deste tipo de sistemas (Gates e Taylor, 2006). O sistema IDES (Denning, 1987), e posteriormente o sistema PAYL (Wang e Stolfo, 2004) foram propostos usando técnicas de deteção de anomalias;
- Deteção Baseada em Especificações – este tipo de sistemas foi criado como forma de resolver alguns dos problemas identificados nas duas estratégias de processamento anteriormente descritas. O seu processamento é baseado na comparação entre o comportamento dos sistemas monitorizados, e uma especificação do comportamento esperado. Estas especificações são normalmente modelos definidos por humanos, quer sejam os responsáveis pela segurança da organização ou qualquer outra entidade externa, e que devem refletir, da forma mais aproximada possível da realidade, o comportamento dos sistemas. Por aproximarem a deteção de intrusões ao comportamento esperado pelos sistemas monitorizados, estes sistemas são conhecidos por produzirem um baixo número de falsos alarmes;
- Um dos primeiros sistemas propostos a utilizar esta estratégia de processamento foi apresentado por Ko *et al.* (1997), e o seu funcionamento baseava-se na monitorização da execução de aplicações com privilégios elevados em sistemas UNIX.

Problemas

Apesar do reconhecido valor dos IDS na proteção de redes e sistemas contra ataques, é também apontado um conjunto de problemas que impedem o seu uso de forma mais abrangente. O aspeto à volta do qual tem existido mais discussão, e também sobre o qual os resultados práticos têm sido mais contraditórios, é a estratégia de processamento.

Os sistemas de deteção de assinaturas são conhecidos por produzirem um elevado número de falsos negativos, que se caracteriza por não gerarem um alarme quando um ataque realmente aconteceu. Estes erros acontecem neste tipo de sistemas dado a sua deteção ser baseada em assinaturas especificadas previamente, não sendo portanto capazes de detetar ataques para os quais ainda não tenham uma assinatura especificada.

Por outro lado, os sistemas de deteção de anomalias, são conhecidos por produzirem um elevado número de falsos positivos, que se caracterizam por gerar um alarme quando nenhuma intrusão aconteceu. Neste caso, estes erros acontecem dado que algumas vezes um desvio do padrão "aprendido" não se traduz efetivamente num ataque. Para além disto, é também possível que estes sistemas gerem falsos negativos, uma vez que é muito difícil de garantir que os dados de treino não tivessem qualquer ataque.

Por fim, os sistemas baseados em especificações são conhecidos como sendo mais balanceados do que as outras propostas. No entanto a sua utilização tem sido limitada, e quando usados, esta utilização é restrita aos níveis mais baixos do sistema, como sejam as chamadas de sistema e os protocolos de rede de baixo nível. A sua adaptação e utilização em camadas semânticas mais elevadas é ainda um desafio em aberto.

Uma das grandes vantagens dos sistemas baseados em especificações face aos sistemas clássicos de deteção de anomalias é a possibilidade de existir um aperfeiçoamento constante da especificação ao longo da vida do sistema. Nestes sistemas quando um falso positivo é detetado é possível analisar a especificação e perceber o que estava errado e que levou ao falso positivo. Já nos sistemas clássicos de deteção de anomalias é necessário voltar a treinar o sistema com novos dados, sendo que não há garantia que esses novos dados não tenham eles próprios ataques não detetados.

Por outro lado, os sistemas de deteção baseados em especificações são bem mais difíceis de colocar em produção que os sistemas clássicos de deteção de anomalias, isto porque é necessário efetuar uma especificação completa e detalhada do sistema, razão pela qual só podem ser aplicados a sistemas com processos algo repetitivos e de dimensão limitada, como são muitos dos sistemas que controlam as redes de transportes públicos.

Sistema Desenvolvido

Tal como já foi referido na introdução, o sistema desenvolvido consiste num sistema de deteção de intrusões híbrido, que combina técnicas de deteção de assinaturas com técnicas de deteção baseadas em especificações. A componente baseada em assinaturas tem como objetivo a deteção de ataques já conhecidos que podem ser utilizados para um atacante se estabelecer no interior de uma dada rede/sistema e a partir daí lançar ataques mais complexos, enquanto a componente baseada em especificações é utilizada para detetar ataques relacionados com a lógica de negócio dos sistemas monitorizados.

Este sistema oferece também a hipótese de utilizar sensores baseados na máquina e/ou sensores baseados na rede, como forma de adaptar a deteção ao tipo e especificidades dos sistemas monitorizados.

Modelo de Deteção Baseado em Especificações

Os sistemas de deteção de intrusão baseados em especificações têm sido apenas pontualmente utilizados, de fato, até em iniciativas puramente académicas as propostas na área são raras.

No sistema desenvolvido, a componente de deteção baseada em especificações é utilizada a um nível semântico mais elevado, a camada de negócio. Na camada de negócio, a deteção de atividades ilícitas é baseada quer na verificação da correta execução de processos de negócio, quer na verificação de conformidade das regras de negócio.

Um processo de negócio pode ser definido como sendo a forma como um conjunto de atividades numa determinada organização está estruturado e relacionado, de maneira a produzir um determinado resultado ou atingir um determinado objetivo, e assim criar valor. Estas atividades tanto podem ser executadas automaticamente pelos sistemas monitorizados, bem como podem requerer intervenção humana. A verificação dos processos de negócio é baseada na captura de padrões previamente estabelecidos, sejam estes observados em eventos de rede ou em registos aplicacionais ou de sistema operativo, que são utilizados como indícios da ocorrência de uma determinada atividade. Estes padrões capturados são posteriormente analisados, de forma a verificar que a execução real da atividades ocorreu de acordo com aquilo que foi especificado no processo de negócio.

Por outro lado, as regras de negócio definem ou delimitam uma certa propriedade do negócio, de forma a validar se determinada atividade está a ser conduzida de acordo com as políticas e orientações da organização. A verificação das regras de negócio está centrada na informação de negócio da organização, comummen-

te denominada de entidades informacionais, manipulada e/ou modificada pelos processos de negócio. Quando é verificada alguma alteração numa entidade informacional ligada a uma determinada regra de negócio, esta regra de negócio é reavaliada de forma a determinar a sua conformidade.

Quando existe uma violação da especificação de um processo/regra de negócio (como sejam um conjunto de ações executadas fora da ordem pela qual o deveriam ser, ou uma regra de negócio que é avaliada como não conforme), esta violação é analisada de acordo com um conjunto de critérios previamente estabelecidos, de modo a determinar o nível de alarme de intrusão a ser emitido.

Arquitetura de Sistema

O sistema desenvolvido está organizado segundo uma arquitetura centralizada. Utiliza, para detetar as atividades que ocorrem nos diversos sistemas e redes monitorizados, diversos sensores remotos, quer sejam estes sistemas de deteção de intrusão, sistemas de deteção de incidentes ou sistemas de monitorização e geração de alarmes. De maneira a interagir com estas soluções, que podem ser instaladas para serem usadas com este sistema ou já existirem nos sistemas a monitorizar, é disponibilizada uma camada fina de integração para que seja possível suportar qualquer tipo de sensor remoto.

Não obstante a deteção dos eventos ser realizada de forma distribuída, a gestão dos sensores e verificação dos eventos detetados é efetuada centralmente, num sistema propositadamente desenvolvido para esse efeito. Por um lado, este sistema central interage com os sensores de deteção para configurar as atividades que estes devem detetar. Por outro lado, recebe dos diversos sensores instalados os indícios da execução das atividades.

Este sistema central aplica um algoritmo especificamente desenvolvido para esse efeito de modo a verificar a correção das atividades detetadas. Este algoritmo é responsável por, após ter recebido um indício da execução de uma determinada atividade, selecionar de entre os processos de negócio em verificação aquele a que a atividade recebida pertence, e verificar a sua correção e ordem no respetivo processo. Caso alguma anomalia se verifique, este sistema reporta o processo (ou regra) onde esta anomalia aconteceu, bem como o fluxo de ações, quer no geral, quer no que diz respeito ao processo em análise, que antecederam a anomalia.

Avaliação

De forma a validar o sistema desenvolvido, foram conduzidos um conjunto de testes baseados em capturas de um conjunto de simuladores de uma rede de metro. A utilização deste simulador permitiu testar a ocorrência de situações anormais na circulação de uma rede de transportes sem que para tal fosse necessário recorrer a uma infraestrutura real, que em muito limitaria o âmbito dos testes[1].

O simulador em questão estava configurado para simular a circulação de 14 veículos numa linha, existindo 10 estações ao longo dessa linha. Em cada estação, existiam duas plataformas, às quais se dirigiam os veículos em função da direção em que se deslocavam na linha.

Deste ambiente de simulação foram sintetizados três processos de negócio que correspondem respetivamente à gestão de emergências numa plataforma, à gestão da informação de passageiros numa plataforma, e por fim à gestão da movimentação dos veículos na linha. Para além disto foi estabelecida uma regra de negócio que especificava a distância mínima que deveria ser mantida entre veículos.

Baseado neste ambiente de simulação e nos processos de negócio extraídos, foram realizados dois tipos de teste:

Teste de funcionamento normal – nestes testes foi simulado o funcionamento normal da rede de metro, de forma a avaliar a capacidade do sistema desenvolvido em verificar a execução dos processos e regras de negócio especificados sem que falsos alarmes fossem produzidos;

Teste com injeção de atividades anormais – por outro lado, neste conjunto de testes era pretendido avaliar se o sistema desenvolvido era capaz de detetar violações à especificação dos processos/regras discriminados.

Tendo em conta os veículos a circular na linha, o número de plataformas, e os processos de negócio sintetizados, é possível determinar que em cada teste existiam simultaneamente em verificação no mínimo 34 instâncias de entre os três processos de negócio.

Resultados Práticos

No primeiro conjunto de testes, verificou-se o sistema num contexto de normal funcionamento do ambiente simulado. Neste caso, e na primeira iteração, foi produzido apenas um alarme. Após uma análise detalhada do alarme produzido, foi possível verificar que se tratava de um falso alarme, que se devia a uma falha

1 O acesso ao simulador foi disponibilizado pela Thales Portugal, à qual agradecemos.

de perceção do funcionamento global do sistema que conduziu a uma falha na especificação de um dos processos de negócio. Esta falha foi corrigida, tendo sido seguida de uma nova iteração de testes, sendo que neste caso já não foi produzido qualquer alarme durante a totalidade do período de simulação.

De seguida procedeu-se ao teste num ambiente em que foram injetadas atividades externas. As atividades externas que correspondiam a atividades não especificadas foram assinaladas pelo sistema como atividades anormais; note-se porém que as atividades injetadas permitidas pelo sistema foram consideradas normais. Cada alarme gerado foi manualmente verificado, de forma a garantir não corresponder a um falso positivo, facto de nunca se verificou. De igual modo, foi verificada a relação entre o número de atividades anormais injetadas e, considerando os instantes de tempo em específico em que as mesmas chegaram ao sistema, verificou-se que nenhuma anomalia escapou à verificação da conformidade do processo.

Discussão

Analisando os resultados dos testes realizados na simulação da rede de metro, é possível discutir o potencial da solução desenvolvida.

Em primeiro lugar, demonstra-se que este tipo de abordagem é capaz de detetar intrusões com um reduzido número de falsos alarmes. Na primeira iteração de testes de funcionamento normal, foi verificada a existência de um falso alarme, devido a uma falha na especificação do processo de negócio. Resolvida que foi esta situação, este falso positivo não se verificou mais durante a totalidade dos testes.

Por outro lado, demonstra-se também que o sistema desenvolvido, naquilo a que ao ambiente de simulação diz respeito, não produziu qualquer falso negativo, tendo sido capaz de detetar todas as atividades que constituíam um desvio à correta execução do processo.

Por fim, todos os alarmes emitidos, possuíam um atraso que, caso se tratasse de uma rede real, poderia ter permitido ao responsável de segurança tomar medidas de contingência de forma a contornar a anomalia, possivelmente evitando que danos significativos fossem infligidos na infraestrutura e nos passageiros.

As principais limitações identificadas na aplicabilidade da solução desenvolvida consistem:

Na obrigatoriedade de proceder à completa definição dos processos de negócio a monitorizar. Tal facto limita o âmbito de aplicação da solução a cenários onde os processos de negócio conseguem ser definidos com elevada precisão;

A utilização de sensores (de rede ou de sistema) com o objetivo de obter indícios suficientes para inferir a execução dos processos de negócio, requer um

profundo conhecimento dos sistemas e protocolos envolvidos. No entanto após o desenvolvimento de regras para um dado sistema ou protocolo de comunicação, as mesmas regras podem ser facilmente reutilizáveis em outras instalações dos mesmos equipamentos.

Conclusão

As redes de transportes públicos, como infraestrutura crítica que são, têm-se tornado um alvo cada vez mais apetecível, incluindo através de um ciberataque aos seus sistemas informáticos. Algum trabalho foi já desenvolvido no sentido de aumentar a proteção destas infraestruturas contra este tipo de ataques, no entanto estas iniciativas são consideradas insuficientes.

Os sistemas de deteção de intrusão, sendo uma solução viável para aumentar a proteção destas infraestruturas, são ainda de utilidade limitada, dado o conjunto de problemas normalmente associados às suas técnicas de deteção e às elevadas necessidades de configuração. No entanto, com o sistema desenvolvido, demonstrámos que é possível resolver alguns dos problemas identificados.

A deteção de intrusões através da identificação de discrepâncias entre os indícios revelados pelos sistemas de informação e comunicação e a especificação dos processos de negócio vai bastante além da segurança dos sistemas envolvidos, pois contempla o negócio como um todo. Desta forma é possível não só detetar ataques aos sistemas, mas também tipos de ataque aos processos de negócio que tem historicamente sido consideravelmente difíceis de detetar e prevenir, tal como é o caso de ataques recorrendo à engenheira social.

Para além disto, a correlação dos alarmes da componente baseada em deteção de especificações com a componente de deteção baseada em assinaturas, que está prevista para uma futura versão deste sistema, permitirá obter a sequência de atividades maliciosas executadas por um atacante, e assim permitir aos responsáveis de segurança reconfigurar os seus sistemas de modo a colmatar essas vulnerabilidades.

Com esta nova tecnologia desenvolvida em Portugal no INOV, enquadrada no projeto SECUR-ED (cofinanciado pelo FP7[2] da Comissão Europeia) e que será demonstrada em redes de transportes terrestres europeias, é possível alargar a sua aplicação, para outros domínios onde seja relativamente fácil definir, com considerável precisão, os processos de negócio envolvidos. É possível prever a sua aplicabilidade em setores tais como o da energia, na distribuição de água potável e em muitos ramos da indústria.

2 Sétimo Programa Quadro de Investigação e Desenvolvimento.

Bibliografia

Axelsson, S. (1999). *Research in Intrusion Detection Systems: a Survey*. Disponível em ftp://ftp.cis.upenn.edu/pub/htdocs/verinet/references/Axelsson99.pdf.

Axelsson, S. (2000). "The base-rate fallacy and the difficulty of intrusion detection". *ACM Transactions on Information and System Security* n.º 3, pp.186–205. Disponível em http://portal.acm.org/citation.cfm?doid=357830.357849.

COUNTERACT Consortium (2010). *Deliverable 2 – Security in Transport and Energy: Overview of the Current Situation*. Disponível em http://www.transport-research.info/Upload/Documents/201207/20120719_144510_49401_Report%20_Deliverable%202.pdf.

DEMASST Consortium (2009). *Deliverable D3.1 - Current Status of Security in Mass Transport*. Disponível em http://www.bmbf.de/pubRD/WS_MT_Eriksson.pdf.

Debar, H., Dacier, M. e Wespi, A. (1999). "Towards a Taxonomy of Intrusion-Detection Systems". *Computer Networks* n.º 8, pp. 805–822.

Denning, D.E. (1987). "An intrusion detection model". *IEEE Transactions on Software Engineering*, n.º 2, pp. 222–232. Disponível em http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=1702202.

Falliere, N., Murchu, L.O. e Chien, E. (2011). *Symantec W32.Stuxnet dossier*. Disponível em http://www.cse.psu.edu/~smclaugh/cse598e-f11/papers/falliere.pdf.

Gates, C. e Taylor, C. (2006). "Challenging the anomaly detection paradigm: a provocative discussion" in *New Security Paradigms Workshop (NSPW) '06*. Schloss Dagstuhl: ACM Press, pp. 21–29. Disponível em http://dl.acm.org/citation.cfm?id=1278940.1278945 .

Ko, C., Ruschitzka, M. e Levitt, K. (1997). "Execution monitoring of security-critical programs in distributed systems: a specification-based approach" in *Proceedings. 1997 IEEE Symposium on Security and Privacy (Cat. No.97CB36097)*. IEEE Comput. Soc. Press, pp. 175–187. Disponível em http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=601332.

Michael, J.B., Wingfield, T.C. e Wijesekera, D. (2003). "Measured responses to cyber-attacks using Schmitt analysis: a case study of attack scenarios for a software-intensive system" in *Proceedings 27th Annual International Computer Software and Applications Conference, COMPAC 2003*, pp. 622–626. Disponível em http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=1245406.

Roesch, M. (1999). "Snort – Lightweight intrusion detection for networks" in *Proceedings of LISA '99: 13th Systems Administration Conference*. Seattle: USENIX, pp. 1-11. Disponível em http://citeseer.ist.psu.edu/viewdoc/summary?doi=10.1.1.105.6212.

The Council of the European Union (2007). "Communication from the Commission to the European Parliament and the Council on Stepping up the fight against terrorism". pp. 1–9. Disponível em http://eur-lex.europa.eu/Notice.do?mode=dbl&lang=en&ihmlang=en&lng1=en,pt&lng2=bg,cs,da,de,el,en,es,et,fi,fr,hu,it,lt,lv,mt,nl,pl,pt,ro,sk,sl,sv,&val=459135:cs&page=

The Council of the European Union (2008). "*Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection*". Disponível em http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32008L0114:EN:NOT

Wang, K. e Stolfo, S. J. (2004). "Anomalous payload-based network intrusion detection" in *Recent Advances in Intrusion Detection* (RAID), pp. 203-22.