Dinâmica Hospitalar na Era do Cibercrime

Claudio Augusto Silveira Lelis[1], Cesar A. C. Marcondes[1] e Johnny Marques[1]
[1]Instituto Tecnológico de Aeronáutica, São José dos Campos/SP - Brasil

***Resumo*— Na era do ciberterrorismo, os cibercriminosos agem, frequentemente, para obter vantagem financeira, e também para servir à espionagem. O interesse pelos ambientes hospitalares vem aumentando por trafegarem dados sensíveis de milhares de pessoas. A ação de cibercriminosos em um ambiente hospitalar pode induzir a erro no tratamento e até mesmo ao óbito do paciente. Assim, torna-se fundamental monitorar desde os dispositivos médicos com comunicação sem fio até a central de dados com informações sensíveis dos pacientes em tratamento. Um modelo dinâmico permitiria obter uma visão sistêmica dos componentes da infraestrutura hospitalar e a influência entre eles. Este artigo apresenta um modelo de Dinâmica de Sistemas para o ambiente de saúde. O modelo foi aplicado a um cenário de operação e executado em uma ferramenta de simulação de modelos de Dinâmica de Sistemas. Os resultados mostraram a viabilidade e aderência do modelo proposto.**

***Palavras-Chave*— Ciberterrorismo, Body Area Network, Ambiente Hospitalar.**

I. Introdução

Em um mundo interconectado, o ciberterrorismo traz efeitos devastadores. Na conferência RSA de 2012 em São Francisco, Robert Mueller (FBI), declarou que existem apenas dois tipos de empresas: aquelas já hackeadas e as que serão, confirmando a tendência de fusão em uma categoria[1]. Entre as mais com maior potencial de dano estão as que lidam com informações médicas.

A *Ponemon Institute* [2] realizou um estudo com 507 organizações de 17 setores da indústria em 16 países e regiões, sobre os custos associados a violações de dados ocorridas entre 2018 e 2019. Foi constatado que o custo médio global de uma violação de dados de 2019 é de US$ 3,92 milhões, um aumento de 1,5% em relação ao estudo de 2018. Desde 2014 o crescimento foi de 12%. Os EUA é o país com o custo total médio mais elevado para uma violação de dados, sendo US$ 8,19 milhões, mais que o dobro da média global.

O estudo mostra ainda como é difícil para as organizações se recuperarem de violações. No caso de ataques maliciosos e criminosos, estes levam em média 314 dias para identificar e conter. Comparativamente, a indústria de saúde é a mais cara em custos de violação de dados, apresentando um valor médio de US$6,45 milhões em 2019.

O crescente investimento em dispositivos médicos conduziu à modernização dos tratamentos, tornando a segurança cibernética um componente crítico da TI em saúde. Os cibercriminosos encontram usos variados para dados clínicos, desde reclamações de fraude até roubo de identidade [3].

O Relatório de Investigações de Violações de Dados da Verizon (DBIR) [4] aponta que dentre as motivações para a violação de dados, quando um motivo é conhecido ou aplicável, o ganho financeiro mostra-se como o fator mais comum de violação de dados, representando 71% dos casos e a espionagem é o motivo em 25% das violações. Segundo o relatório, a área de saúde se destaca devido à maioria das violações estarem associadas a atores internos. Relatos da ação de cibercriminosos que visam hospitais tornam-se frequentes, envolvendo chefes de estado.

Em julho de 2014, a empresa Community Health Systems, que administra 200+ hospitais [5] confirmou um ataque cibernético criminoso que teria ocorrido entre abril e junho de 2014. A empresa acredita que o atacante era originário da China, o qual utilizava *malware* altamente sofisticado nas ações. Neste caso, os dados transferidos afetaram aproximadamente 4,5 milhões de indivíduos que, nos cinco anos anteriores, foram encaminhados ou receberam serviços de médicos afiliados à Empresa. Os dados roubados continham nomes de pacientes, endereços, datas de nascimento, números de telefone e números de seguridade social.

De acordo com o *The Wall Street Journal*, um laboratório de cateterização do *United States Department of Veterans Affair* (VA), em Nova Jersey, ficou temporariamente fechado em janeiro de 2010 [6]. Um *malware* infectou os sistemas de computador e causou indisponibilidade de atendimento. Segundo os relatos, o VA passou por centenas de infecções por malware em dispositivos médicos, como máquinas de raios X e equipamentos de laboratório. Por exemplo, o malware Conficker foi detectado em 104 dispositivos no Hospital James A. Haley Veterans, em Tampa, Flórida.

Em 2018, investigações da Agência de Segurança Cibernética de Singapura (CSA) e do Sistema Integrado de Informação de Saúde (IHiS) confirmaram um ataque cibernético direcionado ao sistema de saúde [7]. Os impactos atingiram dados de cerca de 1,5 milhões de pacientes. Os atacantes especularam especificamente dados pessoais do primeiro-ministro Lee Hsien Loong e seu tratamento. Outras preocupações, especialmente a possibilidade de ser assassinado por meio de ataque mal-intencionado, levaram o ex-vice-presidente dos EUA, Dick Cheney, a desativar os recursos sem fio de seu marcapasso [8].

O Brasil também aparece na lista de alvos recentes de ação de cibercriminosos. Em 2017, o Hospital de Câncer em Barretos foi invadido pelo *Ransomware Petya* [9]. O ataque cibernético paralisou o hospital, os cibercriminosos exigiam resgate, a ser pago em criptomoedas. O custo ao hospital seria equivalente a R$ 1,08 milhão. Além do custo financeiro, que o hospital conseguiu evitar, houve o impacto social, já que cerca de 3 mil consultas e exames foram cancelados e 350 pacientes ficaram sem radioterapia por conta da invasão. Outras unidades do hospital, localizadas em Jales (SP) e Porto Velho (RO), também foram afetadas.

Em 2018, após o atentado contra o então candidato a presidência Jair Bolsonaro, houve o vazamento de uma foto dos primeiros atendimentos prestados ao candidato, enquanto era atendido no centro cirúrgico [10].

As operações diárias do hospital moderno são suportadas por uma ampla variedade de dispositivos, sistemas e aplicativos interconectados, todos trocando dados. Os *Health Information Systems* (HIS, em português Sistema de Informação em Saúde) comportam-se como a espinha dorsal

Claudio Augusto Silveira Lelis, lelis@ita.br; César Marcondes, cmarcondes@ita.br; Johnny Marques, johnny@ita.br.

dessa transferência de dados, gerenciando os aspectos da operação de um hospital, incluindo questões médicas, administrativas, financeiras, jurídicas e o correspondente processamento de serviços. É importante entender que todo e qualquer aplicativo e dispositivo executado na rede do hospital é um potencial ponto de entrada para cibercriminosos que visam o hospital [11]. Por isso torna-se fundamental monitorar toda a infraestrutura hospitalar desde os dispositivos médicos conectados até a central de dados que armazenam as informações sensíveis dos pacientes em tratamento.

Este artigo aborda o problema da segurança cibernética, em um Ambiente Hospitalar (AH), através de um modelo de Dinâmica de Sistemas. A seção II apresenta a fundamentação teórica que serve de base para a proposta de modelo, passando pela caracterização das redes de sensores (WSN) e redes próximas ao corpo (BAN), no caso do paciente, que podem ser encontradas em hospitais. A seção III apresenta o arcabouço conceitual que foi utilizado para construir o modelo. A seção IV apresenta a aplicação do modelo em um cenário de operação. A seção V apresenta as lições aprendidas e, por fim, a seção V apresenta as considerações finais.

II. Fundamentação Teórica

Na área de dispositivos médicos, os Sistemas Embarcados (ES, em inglês *Embedded Systems*) atuam nas funções de controle e comunicação intra-sistemas, ou com os pacientes. Os dispositivos médicos, frequentemente, aparecem como tema de estudos abordando técnicas para burlar suas seguranças internas, identificando os riscos para os pacientes e a exploração de suas vulnerabilidades. Por exemplo, um desfibrilador cardíaco implantável [12], ou ainda um neuroestimulador comercial [13]. Esta seção sintetiza os conceitos envolvidos neste trabalho.

A. Body Area Networks (BANs)

A evolução dos dispositivos médicos propiciou incluir nos dispositivos médicos interfaces com e sem fio, permitindo a comunicação em rede e a transferência de dados dos pacientes. No entanto, podem ocorrer resultados não intencionais durante a agregação de dados em dispositivos projetados para operar separadamente por meio da rede *ad-hoc*.

Nos *Health Information Systems*, a comunicação distribuída tem papel dominante ao transferir a informação médica de maneira eficiente através da rede em diferentes sistemas, incluindo a telemedicina, os serviços de assistência domiciliar e a análise clínica online.

Os sistemas de dispositivos médicos em rede exigem design e fabricação complexos, envolvendo implantes de diferentes modalidades, dispositivos nanobiológicos e dispositivos cirúrgicos invasivos com software de alta confiabilidade [14].

Uma BAN (do inglês, *Body Area Network*) também é chamada de BSN (do inglês, *Body Sensor Network*) ou WBAN (do inglês, *Wireless Body Area Network*), é uma rede sem fio de dispositivos portáteis capazes de realizar alguma computação. Na área de saúde e monitoramento de pacientes, estas siglas remetem aos sistemas de redes de sensores sem fio formados por dispositivos médicos localizados no corpo do paciente [15].

Para monitoramento de saúde, os sistemas e redes de sensores sem fio compõem-se de vários tipos de sensores implantáveis, em miniatura ou vestíveis, denominados biossensores, que são capazes de medir os importantes parâmetros fisiológicos, como a pressão arterial, a frequência respiratória e cardíaca, a temperatura corporal e cutânea e o eletrocardiograma.

As informações médicas adquiridas são interligadas por meio de um link com ou sem fio a um nó central, que em sequência exibe as informações na interface do usuário ou transmite os sinais vitais acumulados a um centro médico. Este processo pode ser explorado. Algumas abordagens para a segurança das BANs e formas de ataque já foram tema de estudos anteriores, por exemplo, a abordagem de sistema criptográfico biométrico para proteger comunicações sem fio de dispositivos de saúde [16].

B. Infraestrutura Hospitalar

A arquitetura de sistemas médicos mais recentes, possuem interfaces com ou sem fio, permitindo a comunicação de dispositivos em rede e o registro dos dados dos pacientes, que podem ser conectados simultaneamente a diferentes dispositivos médicos. Tais dispositivos podem ser capazes, por exemplo, de regular a respiração, administrar medicamentos ou relatar um estado fisiológico. As informações de saúde disponíveis nos diversos dispositivos médicos precisam ser analisadas e coordenadas por um sistema central. Neste cenário, indivíduos podem estar sujeitos a falhas de comunicação, sobrecarga de informações e fadiga do sistema, provocando resultado adverso para o paciente [17].

C. Dinâmica de Sistemas

Dinâmica de Sistemas é uma disciplina de modelagem que surgiu na década de 60 para problemas de gestão [18] cujos modelos utilizam conceitos de controle com retroalimentação (ciclos de *feedback*) para organizar as informações disponíveis de um sistema, criando modelos que podem ser simulados em um computador [19].

Os modelos podem ser representados através de diagramas de causa e efeito e diagramas de estoque e fluxo. Estes últimos são mais precisos na representação do modelo e apresentam um nível de detalhe maior que os diagramas de causa e efeito, forçando o responsável pela modelagem a refinar sua definição da estrutura do sistema [20].

Uma das motivações na produção de modelos com técnicas da Dinâmica de Sistemas é a capacidade de descrever características que não são facilmente expressas em outros modelos, como comportamento endógeno [19], integração, ciclo de realimentação de sistema fechado, bem como causas e consequências distantes no tempo. O Mapeamento de Modelos Mentais também é uma destas características, já que os modelos da Dinâmica de Sistemas não se baseiam apenas em informações numéricas. Embora a principal ferramenta de diagramação e as técnicas de simulação exijam a formulação de equações, estas podem ser geradas a partir do conhecimento contido nos modelos mentais dos indivíduos, permitindo a representação de comportamentos genéricos.

Além disso, as análises quantitativas e qualitativas , individualmente, não capturam todos os aspectos importantes de um sistema. Assim, a construção de modelos de uma maneira semi-quantitativa pode ser baseada em uma visão de pensamento sistêmico, demandando a compreensão do

comportamento de um sistema baseada nos relacionamentos causais entre as variáveis que o descrevem. Isto significa que o sentido de uma mudança em uma parte de um sistema é conhecido, mas não o tamanho do efeito desta mudança em outras partes [21].

D. Trabalhos Relacionados

Desde seu surgimento, a Dinâmica de Sistemas já foi aplicada ao entendimento das interações de entidades, em diferentes contextos. Por exemplo, em modelos de negócio para sustentabilidade [22] e a análise dos componentes da produção agrícola [23]. Na área de Engenharia de *Software*, foi aplicado um modelo dinâmico de reputação para auxiliar na alocação de desenvolvedores a tarefas de manutenção de *software* [24].

Algumas abordagens já foram apresentadas para a segurança cibernética, no entanto, em um aspecto ou sub-partes de uma infraestrutura hospitalar. Por exemplo, através de um sistema de autenticação para transmissão segura de informação médica [25], ou ainda, pelo uso de *blockchain* no armazenamento dos dados sensíveis de pacientes, médicos e os tratamentos em andamento [26].

Em um estudo focado na cibersegurança em hospitais [27], os autores analisaram, através de entrevistas, como as dinâmicas organizacionais internas interagem para formar um sistema de segurança cibernética hospitalar nos Estados Unidos.

Diferentemente, neste trabalho a infraestrutura hospitalar é observada como um conjunto de BANs, por possuírem caráter dinâmico, e a capacidade de influenciar outras BANs. Assim, um modelo dinâmico permitiria obter uma visão sistêmica dos componentes da infraestrutura hospitalar e a influência entre eles.

III. Arcabouço Conceitual para Aplicação de Dinâmica de Sistemas

Essa seção sintetiza o arcabouço conceitual, desenvolvido pelos autores deste trabalho, propiciando a construção do modelo de Dinâmica de Sistemas para um Ambiente Hospitalar (AH).

O **Passo 1 - Definir entidade (quem?)** constitui a identificação da entidade quem está associada a característica que se deseja modelar.

O **Passo 2 - Definir aspecto/característica (o que?)** objetiva responder sobre o que se trata o modelo, propiciando a formalização do objeto de estudo.

O **Passo 3 - Definir componentes do aspecto/característica** busca compreender quais os componentes da entidade, ou seja, quais características definem a entidade, ou a descrevem.

O **Passo 4 - Definir meios de cálculo para os componentes** concentra-se em responder do que é composto o componente. Uma vez apresentados os componentes que afetam a entidade, determinam-se as formas disponíveis de cálculo para cada um dos componentes.

Para os Passos 3 e 4, existe a possibilidade de utilização de entrevistas, *surveys*, mapeamentos, ou ainda Revisões Sistemáticas da Literatura (RSL) para conduzir suas definições.

O **Passo 5 - Conduzir *Goal-Question Metric* (GQM) [28] e/ou Entrevistas** identifica os algoritmos e fórmulas para o cálculo de cada componente. Pode ser necessária uma nova iteração da etapa anterior com entrevistas junto a especialistas ou novas buscas na literatura técnica. Aprofundando o modelo, podem surgir sub-componentes e anti-componentes.

O **Passo 6 - Criar estrutura Ontológica para o Domínio em Análise** surge como um passo opcional que depende da necessidade de uma estrutura para descrever os componentes, a existência ou não de sub-componentes, suas fórmulas ou algoritmos para o cálculo, e como se relacionam.

No **Passo 7 - Definir o conjunto de métricas aplicáveis ao cálculo do valor de cada componente**, como cada componente está associado a possibilidades variadas de fórmulas e algoritmos, a escolha sobre qual algoritmo ou fórmula utilizar é feita através da natureza dos dados disponíveis. Assim, cada fórmula e cada algoritmo estão associados a um conjunto de métricas e parâmetros. Por outro lado, estas métricas são agregadas através de uma das fórmulas ou algoritmos identificados e, como consequência, obtêm-se o valor do componente.

O **Passo 8 - Verificar as Influências existentes entre os componentes** contém três partes:

- No **Passo 8.1 - Identificar Influências Teóricas** faz-se um levantamento objetivando identificar frases, teorias e definições que ofereçam indícios da existência de relações entre os componentes apresentados pelos trabalhos levantados da literatura, ou através das entrevistas;
- O **Passo 8.2 - Identificar Influências Práticas** concentra-se na avaliação e verificação de Influências Teóricas implementadas através das fórmulas e algoritmos analisados, chamadas de Influências Práticas; e
- No **Passo 8.3 - Identificar influência entre cada par de componentes** cria-se uma questão de pesquisa a ser respondida para cada par de componentes que podem se influenciar entre si. Identificando, assim, o sentido da influência e as referências da literatura, ou baseado em entrevistas, que oferecem suporte à existência da influência.

No **Passo 9 - Diagrama de Causas e Efeitos** cria-se um modelo inicial, em que utiliza-se a notação de causas e efeitos onde uma ligação entre dois componentes indica uma relação de influência entre eles. As setas existentes nestas ligações identificam a direção da influência e indicam a tendência de aumento ou diminuição do valor de um componente.

No **Passo 10 - Refinamento** define-se o escopo de atuação da influência entre componentes foram criadas duas classificações:

- Influências intra-entidade: relativo às influências internas entre componentes da própria entidade, ou seja, associadas apenas à entidade em análise; e
- Influências inter-entidade: relativo às influências dos componentes entre entidades, ou seja, estes se relacionam e afetam componentes de outras entidades.

O Passo 10 pode ser repetido quantas vezes necessário, para rever características, influências e valores.

No **Passo 11 - Diagrama de Estoques e Fluxos** realiza-se a construção do modelo a ser executado em uma ferramenta de simulação para Modelos Dinâmicos. Também é possível passar por novas etapas de Refinamento representando as influências inter-entidades.

Um fluxograma com os 11 Passos descritos anteriormente

é apresentado na Figura 1. Já o modelo construído para Ambiente Hospitalar (AH) seguiu os passos anteriores e é apresentado esquematicamente na Figura 2.

IV. Cenário de operação

Na dinâmica de funcionamento de um hospital moderno com possibilidade de acesso, a áreas comuns, de visitantes e acompanhantes dos pacientes em atendimento, podem emergir vulnerabilidades a serem exploradas por potenciais cibercriminosos. Nestes casos, um mau funcionamento induzido em um dispositivo do tipo Cardioversor Desfibrilador Implantável (CDI) ou em uma bomba de insulina, podem representar um risco significativo para o paciente, permitindo uma falha na detecção de quando a terapia é necessária. Em um CDI que não detecta um ritmo cardíaco irregular ou, em pior caso, falha em proporcionar um choque que mantenha o coração do paciente em um ritmo que afete o risco de vida. Tais situações podem resultar em ferimentos graves ou até mesmo morte em determinadas circunstâncias [29].

A. Descrição do Ambiente Hospitalar

O Ambiente Hospitalar (AH) deste trabalho encontra-se inspirado na planta do Hospital Geral de São José dos Campos, com as devidas reduções para descrição do cenário de operação. A descrição do AH é apresentada na Figura 3.

Este AH representa um hospital composto de:

- Uma sala de espera (Destaque 1 na 3);
- Uma sala de servidores do Sistema de Informações Hospitalares (Destaque 2);
- Quatro Unidades de Tratamento Intensivo (UTI) (Destaque 3 e 7);
- Uma enfermaria masculina com 6 leitos (Destaque 4);
- Banheiros (Destaque 5);
- Uma sala de enfermagem (Destaque 1); e
- Uma enfermaria feminina com 6 leitos (Destaque 8).

Em um regime normal de atividades, o ambiente hospitalar é um ecossistema de dispositivos, procedimentos e gerencia de recursos médicos para o melhor atendimento de pacientes. O cenário normal tem um fluxo de informação de mão-dupla, em geral, entre os quiosques de enfermaria, que é o comando e controle do hospital, onde médicos e enfermeiros trocam procedimentos por meio de sistemas de registro médico eletrônico (EHR, em inglês *Electronic Health Record*).

Em seguida, tal informação é passada pela infra-estrutura de redes sem-fio até chegar em dezenas ou até centenas de dispositivos médicos heterogêneos. Essa via dupla de dados, permite capturar informações em um sentido, como informações de alarmes, medições de pacientes, como eletrocardiogramas (ECG), temperatura na Unidade de Tratamento Intensivo (UTI), entre outros. No sentido oposto, atuadores podem ser utilizados para configurar automaticamente cadencia de fluido de terapia intravenosa, configuração de aparelhos de medição, e reinicialização de alarmes, entre outras atividades rotineiras.

O cenário normal onde a dinâmica de sistemas pode auxiliar é demonstrar como os sub-sistemas eletrônicos e de comunicação dentro do hospital formam um grande ecossistema complexo, interconectado e com várias superfícies de ataque. Em estudos prévios [12] [13], pesquisadores, em geral, apontam certas vulnerabilidades selecionadas em cada um dos dispositivos, por exemplo, captura do protocolo, sem criptografia, em nível de aplicação de uma bomba de insulina em rede sem fio, ou fazendo a engenharia reversa do sistema de magnetização de estimulador de nervo vago. Neste trabalho, a novidade é o olhar holístico do sistema como um todo, promovendo a detecção de vulnerabilidades devido a interdependência entre componentes, possibilitando ataques graves.

Por exemplo, a exploração dos dispositivos médicos com uso intensivo de Internet das Coisas (IoT) possuem sistema operacional embarcado com baixo poder computacional e criptográfico. Assim, são facilmente alvos de *malware* injetáveis tornando-os dispositivos de uma *botnet* hospitalar, que poderia atacar usando técnica de negação de serviço (DDoS, em inglês *Distributed Denial of Service*), o fluxo de informação de monitoração de vários pacientes em estado grave.

Sem a devida monitoração em tempo real, existe uma ameaça iminente à vida dos pacientes, devido a saturação de tráfego dos *bots* para o sistema de comando e controle do EHR. Ao mesmo tempo, outros ataques mais assertivos, cujo alvo pode ser um paciente específico, pode usar técnicas de assalto MiM (*Man-in-the-Middle*), onde informações de atuadores podem ser manipulados pelo atacante. Este tipo de ataque pode acontecer pela clonagem de endereços físicos de *Media Access Control* (MAC) em nível da rede sem fio institucional, fazendo com que dispositivos médicos e EHR troquem mensagens, através do agente malicioso, que pode enviar um comando adulterando a cadência de soro em um sistema de entrega intravenosa.

Para mostrar essa visão unificada, os autores realizaram a modelagem dos 3 cenários, descritos anteriormente, na mesma planta hospitalar 3 utilizando-se de modelagem dinâmica através da ferramenta InsightMaker [30]. A modelagem dinâmica é bastante usada em problemas de tomada de decisão, e no escopo deste trabalho, combinando causas e efeitos de troca de informações entre os personagens do dia-a-dia hospitalar.

Na modelagem proposta neste trabalho, os autores preferiram essa aplicação para trabalhar com o AH como um sistema de fluxos de informação em circulação de mão dupla. Portanto, foram modelados os reservatórios de informação em EHR e nos dispositivos. Essa modelagem encontra-se apresentada na Figura 2, que captura todos os elementos que compõe a troca de informações do ecossistema, e traçando os fluxos de envio de dados, baseado em processos semi-automáticos de tomada de decisão.

Para dar coerência ao fluxo de dados e tomadas de decisão, os autores usaram modelos de tráfego baseado em cauda longa, auto-similar, que mimetiza os humanos em sua natureza em rajada e com pausas longas, tanto para tomada de decisão, quanto na natureza do acesso a informações via web. Portanto, os componentes dos dispositivos médicos, que se conectam com as BANs, foram modeladas como fontes de distribuição usando escala de log-normal.

Os acessos do banco de dados e o sistema de comando e controle do EHR, que coleta informações das BANs via rede sem fio, também são feitos em jornadas de trabalho de enfermeiros e médicos cujas paradas não são determinísticas, portanto, tem comportamento assintótico de cauda longa.

Com base no modelo unificador (Figura 2), também foi necessário modelar o atacante, cujo modelo de ameaças

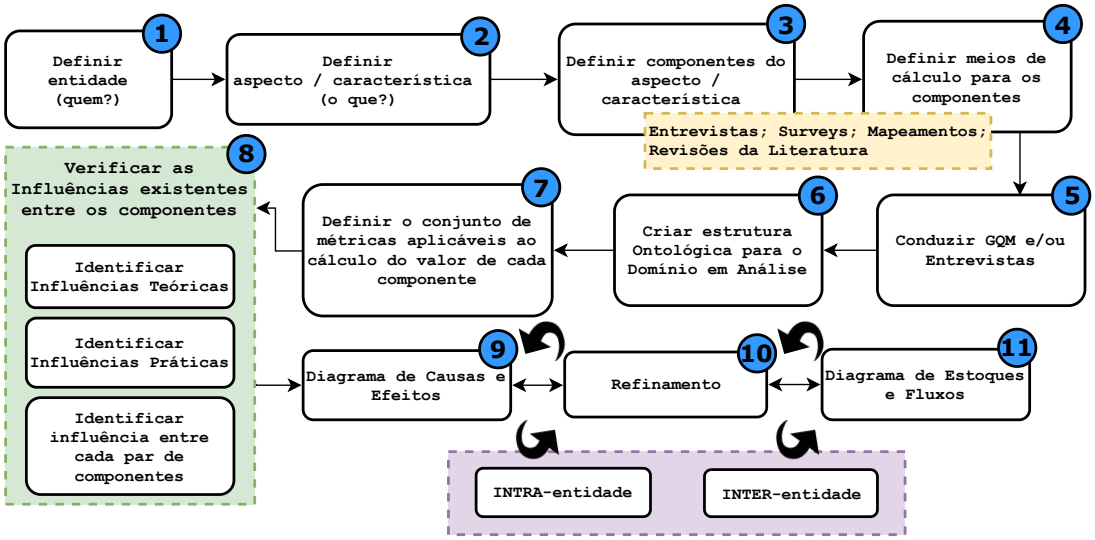

Fig. 1. Arcabouço conceitual e seus passos

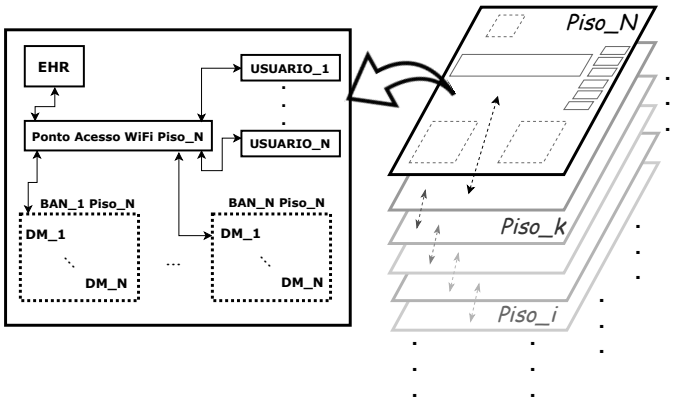

Fig. 2. Modelo Dinâmico para Ambiente Hospitalar

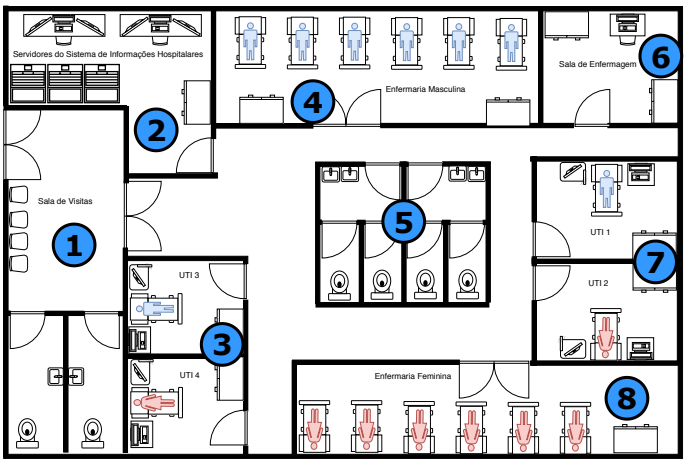

Fig. 3. Planta do Ambiente Hospitalar

considera como um usuário ou malware que conseguiram comprometer a infraestrutura do AH, mas sem grande poder computacional. Para modelar as ameaças no modelo de análise dinâmica e tomada de decisão, foi criado uma parametrização especial no componente Atacante que permite, ora acionar uma rede de bots baseada em invasão prévia de dispositivos médicos, ora através de forjamento de endereços e redirecionamento de parte do tráfego para manipulação.

Com esse controle de certos fluxos pelo Atacante, ele passa a ser um centro de comando e controle do AH, ultrapassando o papel do sistema de EHR. A modelagem de ataques pode ser modelada pela parametrização de ativadores determinísticos, como multiplicação por zero, em casos para controlar a ausência de tráfego.

Para validar a modelagem, simulações foram realizadas com o InsightMaker. Os resultados são apresentados na Figura 4 para verificar tanto saturação de canais de tomada de decisão até o EHR. A Figura 4.a apresenta ataque DDoS: 1-Inicio do Ataque; 2-Requisições para EHR saturam e EHR nega serviços; 3- Ponto de Acesso Wifi passa a ser alvo do Atacante; 4-Saturação geral e Ponto de Acesso nega serviços). Outro ponto foi exercitar a completa ausência de retroalimentação nos cenários onde se ataca o atuador do dispositivo médico. A Figura 4.b apresenta o ataque *Man in the middle-MinM*: 1-Inicio do Ataque e Atacante obtêm controle gradativo do tráfego entre as BANs e o Ponto WiFi; 2-Atacante não suporta o Tráfego completo mas continua coletando dados das BANs restantes; 3-Atacante finaliza o ataque e o fluxo normal é restabelecido.

Portanto, apresentando que o modelo consegue capturar com eficiência em uma única forma, os vários cenários heterogêneos e várias superfícies de ataques que o AH dispõe.

V. Lições Aprendidas

A simulação do modelo proposto permitiu verificar a viabilidade do modelo em mimetizar o ambiente hospitalar em diferentes cenários de operação.

A possibilidade de modelar as BANs como conjuntos de dispositivos médicos que se comunicam e se influenciam é uma segunda lição aprendida. Similarmente, o ambiente hospitalar mimetizado como um conjunto de BANs em interação com os usuários e pontos de acesso de redes sem fio, bem como, a unidade central de dados sensíveis dos pacientes.

Outro ponto importante é que não apenas o aumento de fluxo (exemplo do ataque DDoS) que deve ser monitorado, a redução de fluxo pode significar desvio de tráfego, caso do ataque de MiM, capturada com sucesso pela simulação.

Adicionalmente, foi possível modelar medidas restritivas de acesso e limites de tráfego, representada pela limitação do

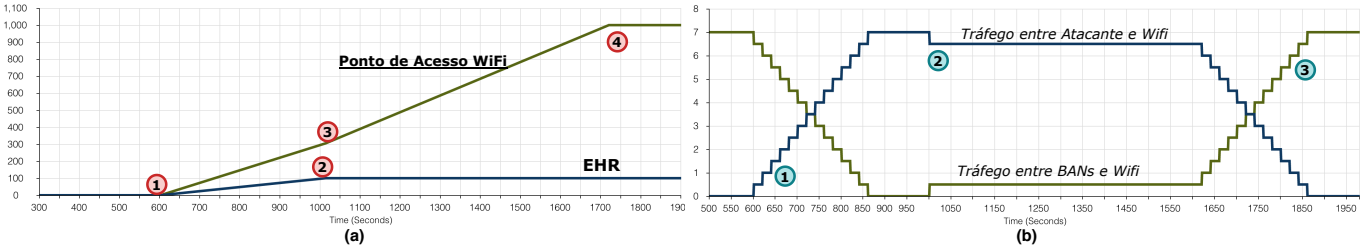

Fig. 4. Resultados de Simulação de Casos de Ataque

Atacante ao tentar interceptar as comunicações de todas as BANs. Finalmente, o uso do modelo dinâmico propiciou a análise de fenômenos adversos à normalidade de operação do ambiente hospitalar apresentado. O conhecimento dos ataques, e respectivos processos, permitem planejar o monitoramento e as contramedidas de defesa.

VI. Considerações Finais

Este artigo apresentou modelo dinâmico para um Ambiente Hospitalar (AH), construído através de um arcabouço conceitual desenvolvido pelos autores deste trabalho e adaptado com sucesso ao contexto. O modelo foi aplicado em um cenário de operação que mostra a viabilidade do modelo para mimetizar a operação normal do ambiente hospitalar, bem como, situações de ataque e seus desdobramentos sob uma visão sistêmica. Vale lembrar que os cenários de operação foram inspirados em relatos recentes, das ações de cibercriminosos que colocam em risco membros chave de nações. Como trabalho futuro, pretende-se analisar o modelo junto aos processos do hospital, expandindo assim, o modelo inserindo componentes de risco.

Referências

[1] S. Cowley, "Fbi director: Cybercrime will eclipse terrorism," 2012, http://money.cnn.com/2012/03/02/technology/fbi_cybersecurity/, acessado 10 de Junho 2019.

[2] L. Ponemon, "What's new in the 2019 cost of a data breach report," 2019, https://securityintelligence.com/posts/whats-new-in-the-2019-cost-of-a-data-breach-report/, acessado 10 de Agosto 2019.

[3] N. Lee, *Counterterrorism and cybersecurity, Second Edition*, 2nd ed. Springer, 2015.

[4] Verizon, "2019 data breach investigations report executive summary," 2019, https://enterprise.verizon.com/resources/executivebriefs/2019-dbir-executive-brief.pdf, acessado 10 de Junho 2019.

[5] U. S. S. E. Commission, "Current report on form 8-k," 2014, https://www.sec.gov/Archives/edgar/data/1108109/000119312514312504/d776541d8k.htm, acessado 10 de Junho 2019.

[6] C. Weaver, "Patients put at risk by computer viruses," 2013, https://www.wsj.com/articles/SB10001424127887324188604578543162744943762, acessado 10 de Junho 2019.

[7] M. of Health Singapure Government, "Singhealth's it system target of cyberattack," 2018, https://www.moh.gov.sg/news-highlights/details/singhealth's-it-system-target-of-cyberattack, acessado 10 de Junho 2019.

[8] A. Peterson, "Yes, terrorists could have hacked dick cheney's heart," 2013, https://www.washingtonpost.com/news/the-switch/wp/2013/10/21/yes-terrorists-could-have-hacked-dick-cheneys-heart/ , acessado 10 de Junho 2019.

[9] K. Guimarães, "Os crimes dos hackers que interrompem até quimioterapia em sequestros virtuais de hospitais," 2017, https://www.bbc.com/portuguese/brasil-40870377, acessado 10 de Junho 2019.

[10] B. Abbud and M. Grillo, "Policiais vasculharam celulares de equipe após foto de bolsonaro em hospital vazar," 2018, https://oglobo.globo.com/brasil/policiais-vasculharam-celulares-de-equipe-apos-foto-de-bolsonaro-em-hospital-vazar-23049220, acessado 10 de Junho 2019.

[11] M. R. Fuentes and N. Huq, "Securing connected hospitals," 2018, https://documents.trendmicro.com/assets/rpt/rpt-securing-connected-hospitals.pdf, acessado 10 de Junho 2019.

[12] E. Marin, D. Singelée, F. Garcia, T. Chothia, R. Willems, and B. Preneel, "On the (in)security of the latest generation implantable cardiac defibrillators and how to secure them," *ACM International Conference Proceeding Series*, vol. 5-9-December-2016, pp. 226–236, 2016.

[13] E. Marin, D. Singelée, B. Yang, V. Volski, G. Vandenbosch, B. Nuttin, and B. Preneel, "Securing wireless neurostimulators," *CODASPY 2018 - Proceedings of the 8th ACM Conference on Data and Application Security and Privacy*, vol. 2018-January, pp. 287–298, 2018.

[14] N. Huebsch and D. J. Mooney, "Inspiration and application in the evolution of biomaterials," *Nature*, vol. 462, no. 7272, p. 426, 2009.

[15] K. Daniluk and E. Niewiadomska-Szynkiewicz, "Energy-efficient security in implantable medical devices," *2012 Federated Conference on Computer Science and Information Systems, FedCSIS 2012*, pp. 773–778, 2012.

[16] Y. Sun and B. Lo, "An artificial neural network framework for gait based biometrics," *IEEE Journal of Biomedical and Health Informatics*, 2018.

[17] C. Pattichis, E. Kyriacou, S. Voskarides, M. Pattichis, R. Istepanian, and C. N. Schizas, "Wireless telemedicine systems: an overview," *IEEE Antennas and Propagation Magazine*, vol. 44, no. 2, pp. 143–153, 2002.

[18] J. W. Forrester, *Industrial Dynamics*. M.I.T. Press, Cambridge, Mass., 1961.

[19] ——, "System dynamics and the lessons of 35 years," in *A systems-based approach to policymaking*. Springer, 1993, pp. 199–240.

[20] S. Albin, J. W. Forrester, and L. Breierova, *Building a system dynamics model: Part 1: conceptualization*. M.I.T. Press, Cambridge, Mass., 2001.

[21] G. G. Camiletti and L. Ferracioli, "The use of semiquantitative computational modelling in the study of predator-pray system," *X International Organization for Science and Technology Education, 2002, Foz do Iguaçu*, 2002.

[22] N. Abdelkafi and K. Täuscher, "Business models for sustainability from a system dynamics perspective," *Organization & Environment*, vol. 29, no. 1, pp. 74–96, 2016.

[23] J. P. Walters, D. W. Archer, G. F. Sassenrath, J. R. Hendrickson, J. D. Hanson, J. M. Halloran, P. Vadas, and V. J. Alarcon, "Exploring agricultural production systems and their fundamental components with system dynamics modelling," *Ecological modelling*, vol. 333, pp. 51–65, 2016.

[24] C. A. S. Lélis *et al.*, "Um modelo dinâmico de reputação para apoiar a manutenção colaborativa de software," Master's thesis, Universidade Federal de Juiz de Fora (UFJF), Juiz de Fora - MG, 2017.

[25] W.-S. Bae and K.-H. Han, "An authentication system for safe transmission of medical information in u-health environment," *International Journal of Applied Engineering Research*, vol. 9, no. 20, pp. 7909–7918, 2014.

[26] H. Pham, T. Tran, and Y. Nakashima, "A secure remote healthcare system for hospital using blockchain smart contract," *2018 IEEE Globecom Workshops, GC Wkshps 2018 - Proceedings*, 2019.

[27] M. S. Jalali and J. P. Kaiser, "Cybersecurity in hospitals: a systematic, organizational perspective," *Journal of medical Internet research*, vol. 20, no. 5, p. e10059, 2018.

[28] V. R. Basili and D. M. Weiss, "A methodology for collecting valid software engineering data," *IEEE Transactions on software engineering*, no. 6, pp. 728–738, 1984.

[29] K. Fu, "Inside risks reducing risks of implantable medical devices," *Communications of the ACM*, vol. 52, no. 6, pp. 25–27, 2009.

[30] S. Fortmann-Roe, "Insight maker: A general-purpose tool for web-based modeling & simulation," *Simulation Modelling Practice and Theory*, vol. 47, pp. 28–45, 2014.