Um Modelo Declarativo para Gestão de Riscos em IoT

Luiz Otávio B. Lento[1], **Pedro Patinho**[1], **Salvador Abreu**[1]

[1]Instituto de Informática – Uiversidade de Évora (UEVORA) - Uevora - Portugal

{luiz.lento,pp,spa}@uevora.pt

Abstract. *A key issue with IoT environments is ensuring security across all services and devices. The diversity of threats, together with the lack of concern of most of its administrators and device designers, made the IoT network environment vulnerable. This article introduces RTRMM, a logic-based security risk management model for IoT environments, which predicts risks and aims to manage them in real time, making the IoT environment more reliable. It makes use of probability, fuzzy logic and logic programming to implement its features.*

Resumo. *Um grande problema em ambientes IoT é garantir a segurança em todos os serviços e dispositivos. A diversidade de ameaças, em conjunto com a falta de preocupação da maioria de seus administradores e projetistas dos dispositivos, tornou o ambiente de rede IoT vulnerável. Este artigo apresenta o RTRMM, um modelo de gerenciamento de riscos de segurança baseado em lógica para ambientes IoT, que prevê os riscos e visa gerenciá-los em tempo real, tornando o ambiente IoT mais confiável. Faz uso de probabilidade, lógica difusa e programação em lógica para implementar as suas funcionalidades.*

1. Introdução

Sistemas IoT estão por todo o mundo, fornecendo uma ampla gama de serviços aos seus usuários, e aumentando-lhes a qualidade de vida, possibilitando que dispositivos inteligentes, sensores e/ou qualquer coisa que geralmente não seja considerada um computador gerem, troquem e usem dados com o mínimo de intervenção humana [Sabry 2019]. Essa capacidade de incorporar e integrar todos estes dispositivos inteligentes vem ao encontro da evolução da Internet e da tecnologia sem fio, causando um grande impacto nas tecnologias de informação e comunicação (TIC), e na Indústria 4.0 [Lu 2017].

Em paralelo a toda esta tecnologia, problemas de segurança da informação também são parte desta evolução do IoT. Garantir a confidencialidade, integridade e disponibilidade das informações trocadas entre dispositivos IoT também é um grande desafio [Ammara 2018]. Prover segurança para IoT exige esforço, principalmente porque as soluções tradicionais usadas em sistemas computacionais, na sua maioria, não são muito eficazes. Além disso, as limitações de processamento, armazenamento e até de energia de cada dispositivo IoT são fatores que limitam/inviabilizam a implantação de soluções mais robustas de segurança da informação [Rizvi 2018]. Desta forma, este artigo propõe uma nova visão de gerir os riscos de segurança em sistemas IoT em tempo real. Para isso, foi criado o RTRMM (Real Time Risk Manegement Model), um modelo para gerir riscos e mitigá-los, em tempo real, conforme o aprendizado temporal ocorrer. O modelo apresenta novas estratégias de detectar, analisar e avaliar os riscos, usando lógica difusa (Fuzzy Logic) e probabilidade, além de estratégias para buscar soluções para mitigar os riscos avaliados.

2. Real Time Risk Management Model

O RTRMM é um novo modelo que visa à gestão/redução de riscos em ambientes IoT, utilizando procedimentos de detecção de ameaças, análise e avaliação de riscos, além da aplicação de medidas de segurança em tempo real. Ele gerencia os riscos existentes de forma proativa e pode ser aplicado em qualquer ambiente de topologia IoT (centros de saúde, fábricas, ...). Ele trabalha com o principal conceito/problema da lógica probabilística: combinar a teoria da probabilidade com a incerteza. A razão de trabalhar com lógica probabilística é poder usar a teoria da probabilidade para lidar com a incerteza de existir ou não uma ameaça em um fluxo de dados IoT. O processo de detecção de ameaças e gerenciamento de riscos é interativo e contínuo, usando um método com base em probabilidades e sistemático para detectar e gerenciar os riscos de segurança, a fim de mantê-los em níveis considerados aceitáveis (minimizando perdas e maximizando ganhos).

A estrutura básica do RTRMM é composta por um conjunto de módulos (figura 1) integrados entre si, como o módulo Threat Analyzer que visa detectar possíveis ameaças existentes nos fluxos de dados IoT. Estas ameaças que foram detectadas são encaminhadas ao módulo Risk Management para serem analisadas e avaliadas com o objetivo de tomar a decisão de serem ou não tratadas. O módulo Threat Category classifica a ameaça em categorias pré-estabelecidas e as envia para o módulo Controls DB. O objetivo de classificar as ameaças é agilizar o processo de seleção das medidas de segurança a serem selecionadas pelo RTRMM. Caso a decisão de tratar a ameaça (o risco) seja necessária, a informação será enviada ao módulo Controls DB, para que uma ou mais medidas de segurança (controles de segurança) sejam selecionadas e aplicadas no ambiente IoT.

3. Threat Analyser e sua Implementação

O Threat Analyzer utiliza as teorias de lógica difusa (fuzzy logic) e probabilidade como estratégia para analisar o fluxo de dados IoT, sendo que ambas trabalham com a premissa de incertezas. Na teoria da probabilidade o grau de incerteza na tomada de decisão pode ser baseado no modo de pensar ou na interpretação de uma determinada situação. Na teoria fuzzy, apesar de existir um grau de incerteza também, existe todo um suporte para a tomada de decisão, possibilitando qualquer decisão que seja possível com base em aproximação, numa abordagem de percepção e na visão do problema a ser tratado.

A teoria da probabilidade trabalha com probabilidades de resultados, quando um ataque pode ocorrer ou não, e se escolhe com base no modo de pensar ou com base na interpretação de uma situação qual decisão a ser tomada. Já na teoria fuzzy existe um grau de incerteza, mas oferece suporte para decidir se uma ameaça ocorreu ou não [Johnson 2023] [Sanjaa 2007]. Utilizar lógica fuzzy possibilita que tudo seja possível ou permitido, possibilitando modelar um problema de forma aproximada ao invés de precisa, resolver problemas complexos e tomada de decisão e controle por meio de questionamentos e trabalhar com um universo de opções adequadas ao problema a ser tratado [Zadeh 1998]. A figura 2 apresenta a arquitetura do Threat Analyzer, onde no fluxo de dados IoT são coletados os pacotes para selecionar quais campos irão compor as entradas crisps (protocolo, endereço IP, portas, ...), e os parâmetros que irão compor as regras do sistema fuzzy. As entradas crisps passarão pelo processo de fuzzificação e o mecanismo de inferência aplicada as regras de inferência à entrada fuzzy para gerar a saída fuzzy.

No Threat Analyzer, uma regra representa uma anomalia em um fluxo de dados

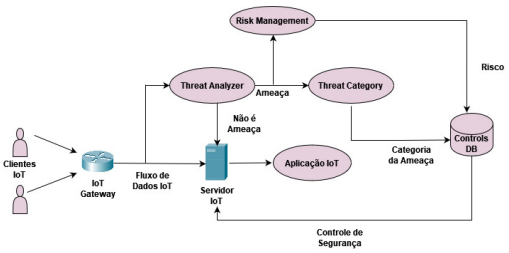

Figura 1. Modelo Lógico do RTRMM

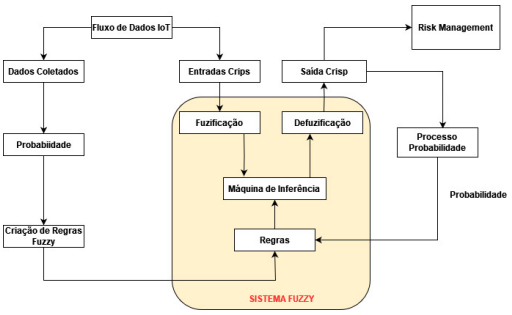

Figura 2. Arquitetura do Threat Analyzer

IoT, realizando a combinação entre os elementos que compõem o tráfego e a probabilidade desta anomalia acontecer em um fluxo IoT. Cada regra está relacionada a um grau de incerteza. Para o Threat Analyzer, inferir um valor inicial para a probabilidade de que exista uma ameaça em um tráfego IoT é um tanto difícil, porque um conjunto de elementos deve ser levado em consideração. Desta forma, a probabilidade inicial é estabelecida com base em uma situação específica, como na teoria da probabilidade [**?**]. O uso do IoT 23 [Lab. 2020], citado na seção 3.2, proporciona uma situação onde vários eventos de segurança são apresentados. Com base nestes eventos pode-se estabelecer um valor de probabilidade de um determinado evento ocorrer. Contudo, o aprendizado da probabilidade das regras de Fuzzy é baseado em redes bayesianas [D'Ambrosio 1999], e aplicado em um novo conjunto de fluxo de dados, buscando uma maior aproximação à realidade da detecção de ameaças.

3.1. Processo de Fuzzificação/Desfuzificação

Os Termos do Threat Analyzer, no processo de fuzificação, são definidos como um conjunto de valores discretos L representando o universo de variáveis fuzzy, em que l_i é um dos valores deste conjunto L $\rightarrow \{0, 1\}$. Com base no universo de variáveis fuzzy, os termos definem S onde existem valores μl_i, em que estes valores de S são: S = $\{(l_i, \mu S(l_i))/l_i \in L\}$, de forma que $\mu S(l_i)$ é a função de relevância, e está contida no intervalo entre 0 e 1: μS: L $\rightarrow$ [0, 1].

Sendo assim, foram especificados quatro grupos para representarem os termos no processo de fuzzificação, possibilitando o cálculo do valor da variável fuzzy (valor atribuído a probabilidade para cada regra e avaliação de riscos).

1. Really - há uma grande probabilidade de que possa ser uma ameaça, e o seu valor de relevância é: $\mu S \geq 0.9$
2. Almost - existe a probabilidade de ser uma ameaça, e o seu valor de relevância é: $\mu S \geq 0.7 \wedge \mu S < 0.9$
3. Sometimes - há uma probabilidade média de ser uma ameaça, e o seu valor de relevância é: $\mu S \geq 0.4 \wedge \mu S < 0.7$
4. Impossible - a probabilidade de ser uma ameaça é mínima, e o seu valor de relevância é: $\mu S < 0.4$

O motor de inferência do Threat Analyzer é o responsável por aplicar as regras de inferência à entrada fuzzy para gerar a saída fuzzy. As regras são definidas juntamente com as entradas fuzzy de acordo com as funções de pertinência (reflete o conhecimento que se tem em relação à intensidade com que o objeto pertence ao conjunto fuzzy)

[Izquierdo 2017]. Para determinar a região resultante, o processo de inferência usou a técnica de Mandami [Mamdani 1975], pois ele é intuitivo, mais adequado para entrada humana, por possuir uma base de regras mais interpretável (IF-ELSE: IF TERMO is X ELSE Y) e por ter uma ampla aceitação.

A técnica de defuzzificação adotada no Threat Analyzer foi a centróide, no qual a sua saída é um valor discreto, isto é, a probabilidade de uma anomalia ser uma ameaça. O cálculo da probabilidade é baseado em uma média ponderada (dos valores), de acordo com o grau de relevância para a distribuição de possibilidades da saída do modelo. [Jantzen 2006]

3.2. Implementação Threat Analyzer

O módulo Threat Analyzer foi implementado em Problog [Raedt 2007] e fez uso do IoT-23 , um conjunto de dados de tráfego de rede de dispositivos da Internet das Coisas (IoT), gerado pelo "Stratosphere Laboratory, AIC group, FEL, CTU University, Czech Republic"[Lab. 2020], que visa oferecer um grande conjunto de dados, infectados por malware ou benigno, de dispositivos IoT reais.

O código desenvolvido fez uso de 6 campos, simulando entradas Crisp: protocolo; data do evento; endereço IP de origem e o de destino; e porta de origem e porta de destino. Inicialmente, foram especificadas 3 anomalias, baseadas na estratégias de regras de fuzzificação, e nos parâmetros de malwares apresentados no IoT-23. Para cada uma das anomalias foram selecionados três (3) parâmetros de identificação do tráfego IoT para a sua composição: protocolo, endereço IP de destino e porta de destino (figura 3). O valor da probabilidade inicial atribuída a cada parâmetro na composição de cada anomalia baseado em um fato, a análise/avaliação dos eventos apresentados no IoT-23, na razão N/M. O valor N corresponde à quantidade de ocorrências de um parâmetro na base de dados IoT-23, e M a quantidade total de fluxos de dados na base IoT-23.

4. Risk Management e sua Implementação

O módulo Risk Management visa analisar e ou avaliar as ameaças no RTRMM, via um processo dinâmico, com base nas informações providas pelo Threat Analyzer em tempo real. O processo de análise de riscos do RTRMM busca conhecer e calcular os riscos, analisando todas as anomalias fornecidas pelo sistema e seu grau de probabilidade. O processo de análise faz uso dos quatro (4) níveis citados anteriormente neste artigo: Really, Almost, Sometimes e Impossible. O valor do risco está baseado na probabilidade de cada anomalia avaliada pelo Threat Analyzer. Será considerada uma ameaça toda e qualquer anomalia α_i, que pertença ao conjunto de anomalias citadas pelo Threat Analyzer, sendo que esta anomalia para ser uma ameaça γ ela deverá possuir uma probabilidade ≥ 0.7. Logo, **ameaça** $\Rightarrow (\gamma \Leftarrow \exists \alpha_i, \alpha_i \in A, \mu S \geq 0.7)$.

O processo de avaliação de riscos tem como objetivo determinar a prioridade de tratamento das ameaças. Para isso, as probabilidades das ameaças são ordenadas na forma decrescente, priorizando o tratamento das ameaças com maior probabilidade.

4.1. Implementação Risk Management

A implementação do módulo Risk Management foi realizada em Prolog, tendo como entrada uma base de dados com as anomalias e suas respectivas probabilidades detectadas

pelo Threat Analyzer. Esta base continha onze (11) entradas com as anomalias e suas respectivas probabilidades, conforme pode ser constatado na figura 4.

```
%loading the database
  :- use_module(library(db)).
  :- csv_load('out_lim1.csv', 'pacote').
%the first anomaly
  0.3::anomaly(A,B,C,D,E,F):- pacote(A,B,C,D,E,23).
  0.6::anomaly(A,B,C,D,E,F):- pacote(tcp,B,C,D,E,F).
  0.7::anomaly(A,B,C,D,E,F):- pacote(A,B,C,'65.127.233.163',E,F).
%the second anomaly
  0.5::anomal_1(A,B,C,D,E,F):- pacote(A,B,C,D,E,49560).
  0.7::anomaly_1(A,B,C,D,E,F):- pacote(tcp,B,C,D,E,F).
  0.6::anomaly_1(A,B,C,D,E,F):- pacote(A,B,C,'147.7.65.203',E,F).
%the third anomaly
  0.4::anomaly_2(A,B,C,D,E,F):- pacote(A,B,C,D,E,60862).
  0.6::anomaly_2(A,B,C,D,E,F):- pacote(udp,B,C,D,E,F).
  0.8::anomaly_2(A,B,C,D,E,F):- pacote(A,B,C,'51.148.125.188',E,F).
%probability of query
  query(anomaly(tcp,_,_,'65.127.233.163',_,23)).
  query(anomaly_1(tcp,_,_,'147.7.65.203',_,49560)).
  query(anomaly_2(udp,_,_,'51.148.125.188',_,60862)).
```

Figura 3. Codificação do Threat Analyzer

```
root@retrimm:/bigfatdisk/otavio/teste# problog te.pl
     anomaly(tcp,'20180509-163031','192.168.100.103','65.127.233.163',51524,23):       0.916
     anomaly(tcp,'20180509-163032','192.168.100.103','65.127.233.163',51524,23):       0.916
     anomaly(tcp,'20180509-163034','192.168.100.103','65.127.233.163',51524,23):       0.916
     anomaly(tcp,'20180509-163038','192.168.100.103','65.127.233.163',51524,23):       0.916
     anomaly(tcp,'20180509-163046','192.168.100.103','65.127.233.163',51524,23):       0.916
  anomaly_1(tcp,'20180509-163033','192.168.100.103','147.7.65.203',34243,49560):       0.88
  anomaly_1(tcp,'20180509-163034','192.168.100.103','147.7.65.203',34243,49560):       0.88
  anomaly_1(tcp,'20180509-163036','192.168.100.103','147.7.65.203',34243,49560):       0.88
  anomaly_1(tcp,'20180509-163040','192.168.100.103','147.7.65.203',34243,49560):       0.88
  anomaly_1(tcp,'20180509-163048','192.168.100.103','147.7.65.203',34243,49560):       0.88
anomaly_2(udp,'20180509-163034','192.168.100.103','51.148.125.188',43763,60862):      0.952
```

Figura 4. Resultado Anomalias Detectadas

O módulo risk management criou uma base de dados em Prolog, composto pelo tipo da anomalia e sua probabilidade, além dos níveis de ameaça proposto pelo RTRMM (Really, Almost, Sometimes, Impossible). Criou-se uma regra em Prolog que compara o valor da probabilidade calculada para cada anomalia com os níveis de ameaça. Os seguintes resultados foram obtidos, e se os mesmos deverão ser tratados:

1. Anomaly - esta anomalia teve 0.916 como resultado, sendo considerada Really, uma alta possibilidade de ser uma ameaça. **TRATAR A AMEAÇA - PRIORIDADE 2**
2. Anomaly_1 - esta anomalia teve 0.88 como resultado, sendo considerada Almost, existe a possibilidade de ser uma ameaça. **TRATAR A AMEAÇA - PRIORIDADE 3**
3. Anomaly_2 - esta anomalia teve 0.952 como resultado, sendo considerada Really, uma alta possibilidade de ser uma ameaça. **TRATAR A AMEAÇA – PRIORIDADE 1**

O RTRMM assumiu que para qualquer ameaça que possua o grau de relevância (probabilidade) $\mu S \geq 0.7$) deverá ser tratada. A escolha deste valor foi baseada na análise / avaliação qualitativa dos riscos no qual o processo prioriza riscos de acordo com os seus efeitos potenciais nos sistemas IoT.

5. Desempenho

Para verificar se o RTRMM é viável, foram realizados alguns testes e uma análise de desempenho com duas diferentes situações, como apresentado na figura 5. Na situação 1 cada anomalia possuía 3 parâmetros (protocolo, endereço de destino e porta de destino), e o sistema utilizou 3, 5 e 7 anomalias para análise de tempo. Na situação 2 cada anomalia possuía 5 parâmetros (protocolo, endereço de origem e destino e porta de origem e destino), e o sistema utilizou 3, 5 e 7 anomalias para análise de tempo.

Os resultados da avaliação do sistema comprovam que o comportamento e o seu desempenho é considerado adequado, pois a taxa de crescimento de tempo foi praticamente proporcional ao crescimento do número de anomalias, tanto com o uso de 3 ou 5 parâmetros na composição da anomalia.

6. Conclusão

Este artigo apresenta uma nova estratégia de gerenciamento de riscos em ambientes IoT, usando lógica probabilística. O modelo é capaz de detectar as ameaças e a probabilidade

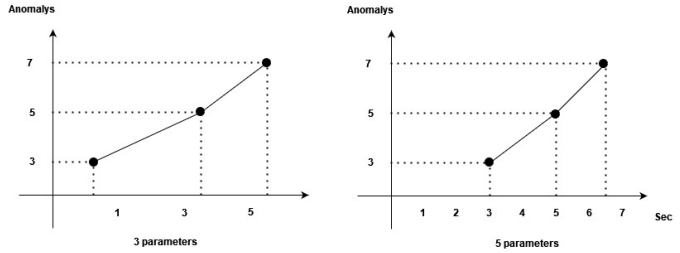

Figura 5. Run-time Comparação

delas acontecerem, além de analisar e avaliar os seus riscos, bem como tratá-los. Nem todos os módulos e funcionalidades foram completamente implementadas e testados, somente parcialmente os módulos de Threat Analyzer e Risk Management. Funcionalidades como aprendizado no Threat Analyzer e a escolha da medida de segurança ainda estão em fase de validação. Atualmete as medidas de segurança aplicadas estão relacionadas ao bloqueio de acesso ao dispositivo IoT. Apesar do RTRMM ser aplicável a qualquer sistema IoT, a sua validação completa será em ambientes IoT Healthcare.

Referências

Ammara, M., R. G. C. B. (2018). Internet of things: A survey on the security of iot frameworks. In *Journal of Information Security and Applications*, pages 8–27. Elsevier.

D'Ambrosio, B. (1999). Inference in bayesian networks. In *AI Magazine*, pages 21–36. PKP.

Izquierdo, S. (2017). Mamdani fuzzy systems for modelling and simulation: A critical assessment. In *Social Science Research Network*, pages 1–18. SSRN.

Jantzen, J. (2006). Tutorial on fuzzy logic. In *Tech. report no 98-E 868*, pages 1–28. Technical University of Denmark, Oersted-DTU.

Johnson, D. (acessado em 2023). Fuzzy logic tutorial: What is, architecture, application, example. In *https://www.guru99.com/what-is-fuzzy-logic.html*.

Lab., S. (2020). Aposemat iot-23. www.stratosphereips.org/datasets-iot23. Acessado em fevereiro de 2023.

Lu, Y. (2017). Industry 4.0:a survey on technologies, applications and open research issues. In *Journal of Industrial Information Integration*, pages 1–10. Elsevier.

Mamdani, E. H., A. S. (1975). An experiment in linguistic synthesis with a fuzzy logic controller. In *International Journal of Man-Machine Studies*, pages 1–13. Elsevier.

Raedt, L. D. (2007). A probabilistic prolog and its application in link discovery. In *IJCAI-07*, pages 2468–2472. IJCAI.

Rizvi, S., P. I. J. K. A. R. M. (2018). Securing the internet of things (iot): A security taxonomy for iot. In *TrustCom/BigDataSE*, pages 163–168. IEEE.

Sabry, Sana S., Q. N. A. O. H. S. (2019). The road to the internet of things: a survey. In *IEMECON*, pages 290–296. IEEE.

Sanjaa, B. (2007). Fuzzy and probability. In *IEEE Xplore*, pages 141–143. IEEE.

Zadeh, L. (1998). Fuzzy logic. In *IEEE Computer*, pages 141–143. IEEE.