Identificação e Ofuscação de Vulnerabilidades de Segurança e de Comportamentos na IoT

Fernando Nakayama de Queiroz

Center for Computational Security sCience (CCSC)

Belo Horizonte – Brazil

20 de Janeiro de 2023

www.ccsc-research.org

Trabalhos Selecionados de AML

Atividades

1) Projetar e implementar uma solução para analisar o tráfego das redes IoT em busca de estatísticas;
2) Projetar uma interface gráfica para a plataforma CAMALEÃO sendo proposta;
3) Modelagem da identificação dos tipos de dispositivos da IoT;
4) Propor modelos de aprendizagem de máquina para identificar vulnerabilidades em dispositivos da IoT;
5) Criar e divulgar uma base de dados com padrões de comportamento das vulnerabilidades de dispositivos IoT;
6) Modelos de AML como princípio para a ofuscação do comportamento dos dispositivos em redes IoT;
7) Implantação de um gerenciador de filas para organizar as requisições e instruções recebidas e enviadas pelo Centro de Inteligência;
8) Avaliação do funcionamento e desempenho da plataforma CAMALEÃO proposta e compará-la às soluções existentes na literatura;
9) Documentar e publicar os resultados do projeto em revistas e conferências especializadas;
10) Reuniões periódicas com os colaboradores.

	1º Ano				2º Ano			
	1º Tri	2º Tri	3º Tri	4º Tri	1º Tri	2º Tri	3º Tri	4º Tri
Atv 1	◉	◉	◉					
Atv 2		◉	◉	◉	◉			
Atv 3	◉	◉	◉	◉	◉	◉		
Atv 4	◉	◉	◉	◉	◉	◉		
Atv 5				◉	◉	◉		
Atv 6	◉	◉	◉	◉	◉	◉		
Atv 7			◉	◉	◉			
Atv 8	◉	◉	◉	◉	◉	◉	◉	◉
Atv 9		◉		◉		◉		◉
Atv 10	◉		◉		◉		◉	

	1º Ano				2º Ano			
	1º Tri	2º Tri	3º Tri	4º Tri	1º Tri	2º Tri	3º Tri	4º Tri
Atv 1	◉	Projetar e implementar uma solução para analisar o tráfego das redes IoT em busca de estatísticas;						
Atv 2		◉	◉	◉	◉			
Atv 3	◉	Modelagem da identificação dos tipos de dispositivos da IoT;						
Atv 4	◉	Propor modelos de aprendizagem de máquina para identificar vulnerabilidades em dispositivos da IoT;						
Atv 5				◉	◉	◉		
Atv 6	◉	Modelos de AML como princípio para a ofuscação do comportamento dos dispositivos em redes IoT;						
Atv 7			◉	◉	◉			
Atv 8	◉	Avaliação do funcionamento e desempenho da plataforma CAMALEÃO proposta e compará-la às soluções existentes na literatura;						
Atv 9		◉		◉		◉		◉
Atv 10	◉	Reuniões periódicas com os colaboradores.						

	1º Ano				2º Ano			
	1º Tri	2º Tri	3º Tri	4º Tri	1º Tri	2º Tri	3º Tri	4º Tri
Atv 1	◉	◉	◉					
Atv 2		◉		Projetar uma interface gráfica para a plataforma CAMALEÃO;				
Atv 3	◉	◉	◉	◉	◉	◉		
Atv 4	◉	◉	◉	◉	◉	◉		
Atv 5				◉	◉	◉		
Atv 6	◉	◉	◉	◉	◉	◉		
Atv 7			◉	◉	◉			
Atv 8	◉	◉	◉	◉	◉	◉	◉	◉
Atv 9		◉		Documentar e publicar os resultados do projeto;				
Atv 10	◉		◉		◉		◉	

Behaviour source analysis

1- Projetar e implementar uma solução para analisar o tráfego das redes IoT em busca de estatísticas

- Packet header statistics
- Network flow statistics
- Combined methods

Externally collected
Universality
Multiple devices (per gateway)
Impersonation
Encrypted data

- Clock drift (skewness)
- RAW quadrature signals
- Signal frequency

Externally/internally-collected
Instance identification
Difficulty of tampering
Comprise composed solutions
Complex data gathering

Estado da arte - Origem dos dados

1- Projetar e implementar uma solução para analisar o tráfego das redes IoT em busca de estatísticas

- **Estatística cabeçalhos**
- **Estátistica fluxos**
- **Métodos combinados**

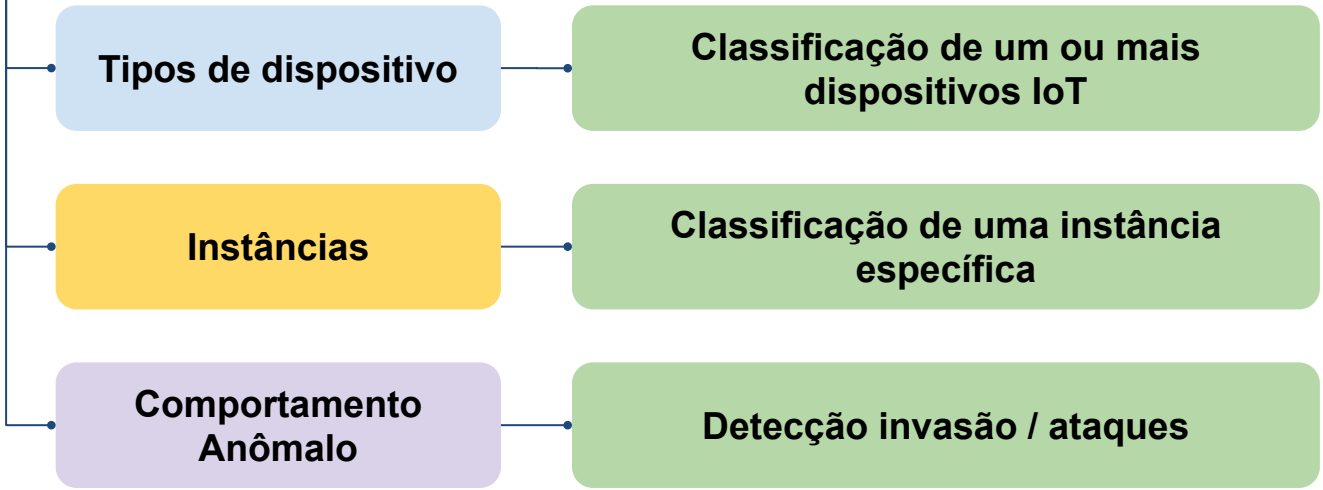
Coletados internamente e externamente
Compatibilidade
Múltiplos dispositivos por gateway
Imitação/clonagem de dispositivos
Dados criptografados

- **Variação do relógio**
- **Sinais de quadratura**
- **Frequência dos sinais**

Coletados internamente e externamente
Identificação de instâncias
Dificuldade de adulteração
Soluções compostas e complexas
Dificuldade na coleta de dados

Estado da arte - Categorias de identificação

3- Modelagem da identificação dos tipos de dispositivos da IoT



Estado da arte - Modelos de AM

4- Propor modelos de aprendizagem de máquina para identificar vulnerabilidades em dispositivos da IoT

Tipos de dispositivo

Objetivos:
Classificação

Datasets:
Públicos
Privados

Instâncias

Objetivos:
Classificação
Análise de dados

Datasets:
Privados

Comportamento Anômalo

Objetivos:
Classificação
Detecção de anomalias

Datasets:
Públicos
Privados

Estado da arte - Modelos de AM

4- Propor modelos de aprendizagem de máquina para identificar vulnerabilidades em dispositivos da IoT

Tipos de dispositivo

Técnicas/Algoritmos:
Redes neurais, Naive bayes, Random forest, Gradient boosting, k-NN, Árvores de decisão, Multilayer perceptron, t-SNE, DBSCAN, C-means, CNN (variações), máquinas de estados, interpolação

Instâncias

Técnicas/Algoritmos:
Estatística, Redes neurais, LSTM, Árvores de decisão

Comportamento Anômalo

Técnicas/Algoritmos:
Mesmas anteriores + modelos lineares, IQR (Interquartile range), Autoregressão

Estado da arte - Modelos de AM

4- Propor modelos de aprendizagem de máquina para identificar vulnerabilidades em dispositivos da IoT

Tipos de dispositivo

Origem:
Rede
Sinais de rádio
Características:
Cabeçalho, intervalo de resposta, estatística dos fluxos, estatística da sequência dos pacotes, análise do DNS, amostras de sinais de quadratura

Instâncias

Origem:
Rede
Processadores
Osciladores
Relógio
Sinais eletromagnéticos
Características:
Voltagem, beacon Wi-Fi, uso da UCP, amostras de sinais eletromagnéticos

Comportamento Anômalo

Origem:
Rede
Sensores
Chamadas de sistema
Logs
Características:
Cabeçalho, estatística dos fluxos, valores de sensores, valores da UCP, registros de hardware, registros de sistema

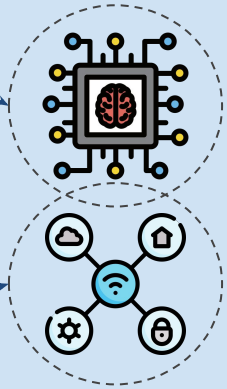
Desafios

Processos estatísticos

Aprendizagem de máquina

Cenário

Identificação de dispositivos



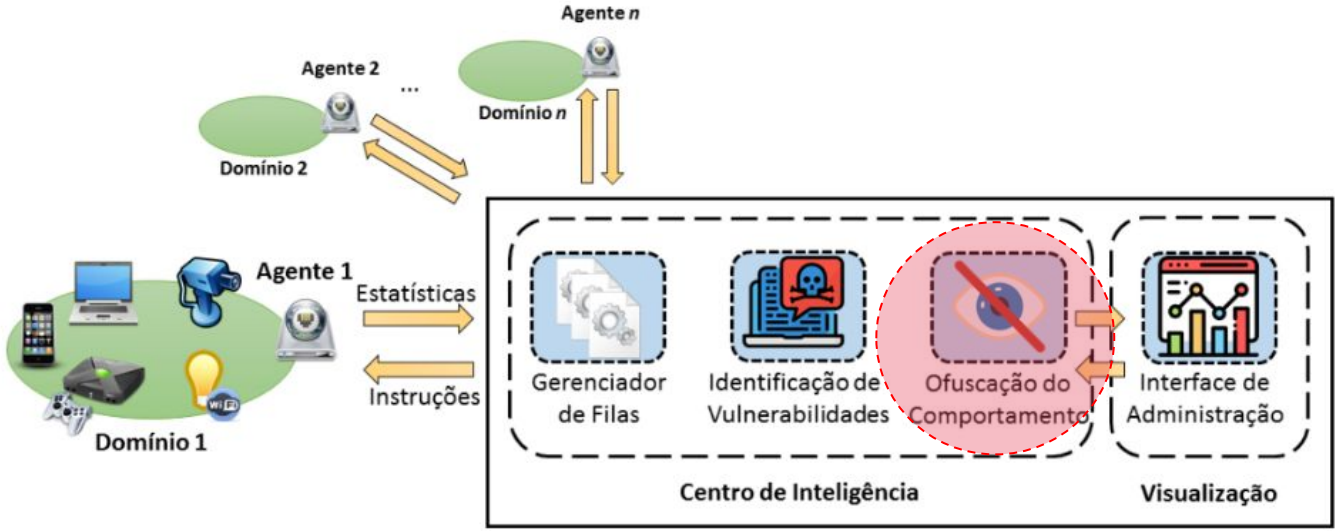
Desafios

- Convergência AM / IoT
- Acesso aos dados
- Soluções escaláveis
- Privacidade
- Contramedidas

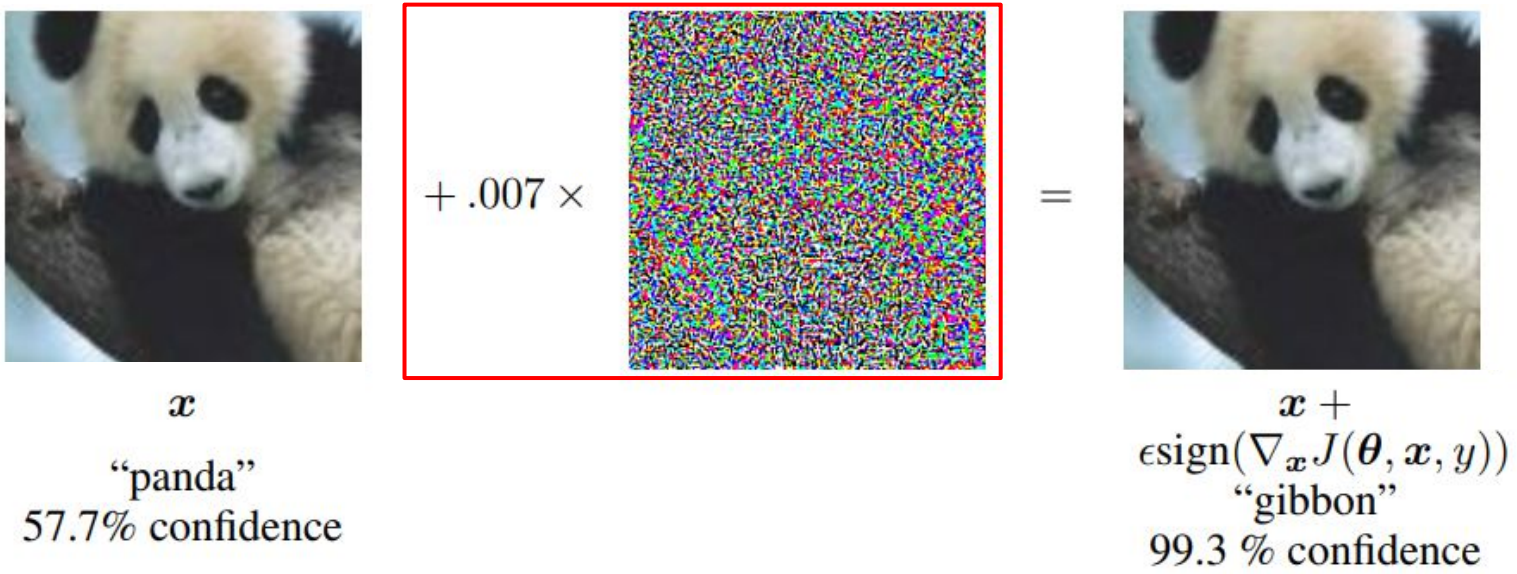
Aprendizado de Máquina Adversário - AML (Adversarial Machine Learning)

“O aprendizado de máquina adversário é uma técnica usada no aprendizado de máquina para enganar ou desorientar um modelo através de uma entrada de dados maliciosa”

Aprendizado de Máquina Adversário - AML (Adversarial Machine Learning)

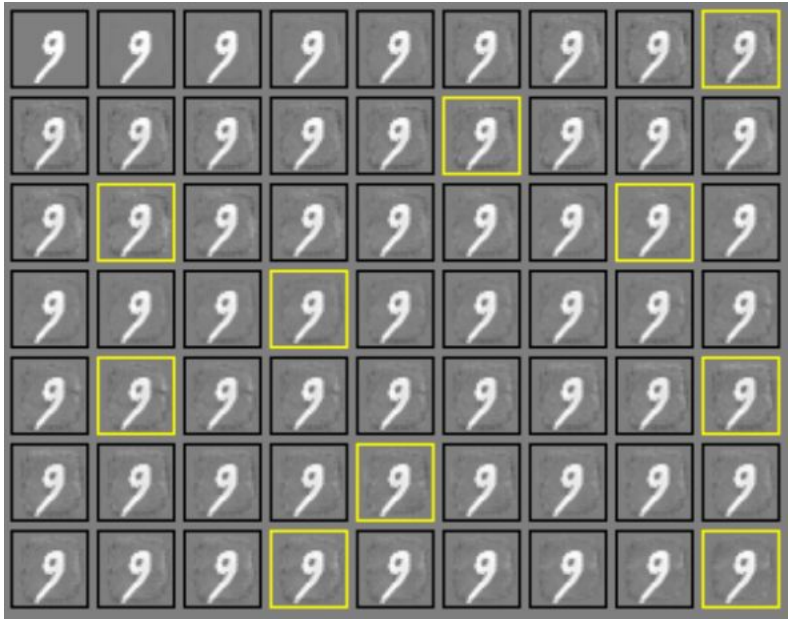


Aprendizado de Máquina Adversário - AML (Adversarial Machine Learning)



Goodfellow, Ian J., Jonathon Shlens, and Christian Szegedy. "Explaining and harnessing adversarial examples." *arXiv preprint arXiv:1412.6572* (2014).

Aprendizado de Máquina Adversário - AML (Adversarial Machine Learning)



Lecture 16 | Adversarial Examples and Adversarial Training - Stanford University School of Engineering Ian Goodfellow - https://youtube.com/watch?v=CIfsB_EYsVI&feature=shares

Aprendizado de Máquina Adversário - AML (Adversarial Machine Learning)

Algorithm 3 Adversarial Burst

Input Flow set F of class l, flow content classifier f_{1D-CNN} with weights θ, selected burst indices vector IND_{SBurst}, number of dummy packets $Num\_of\_dummy\_pkts$, perturbation rate ϵ, number of iterations T, batch size $batch\_size$.

Output UAP ξ

$\xi \leftarrow Rand(Domain(F), Size = Num\_of\_dummy\_pkts)$
for $t \leftarrow 0, T$ **do**
  $F^{batch} \leftarrow$ *sample batch_size flows from* F
  $IND^{batch} \leftarrow$ *selected burst index of* F^{batch} *in* IND_{SBurst}
  for $i \leftarrow 0, batch\_size$ **do**
    $flows\_time\_series_i^{batch} \leftarrow flow\_to\_burst\_seq(F_i^{batch})$
    $Brs_s^i = flows\_time\_series_i^{batch}[IND_i^{batch}]$
    $Brs_{adv}^i = append(Brs_s^i, \xi)$
    $flows\_time\_series_i^{batch}[IND_i^{batch}] = Brs_{adv}^i$
  end for
  $\Delta\xi = \epsilon \times \nabla_\xi J(\theta, flows\_time\_series^{batch}, l)$
  $\xi = Clip_{Domain(F)}(\xi + \Delta\xi)$
end for
return ξ

1- Adversarial PAD
2- Adversarial Payload
3- Adversarial Burst

	Attack	Attack Parameter	Overall Accuracy(%)	Recall(%)					
				Chat	Email	File Transfer	Streaming	Torrent	VoIP
FTSC-IAT	No Attack		69.62	34.95	75.95	73.76	66.51	85.00	73.95
	AdvBurst	7 dummy pkts	31.31	5.83	37.97	19.50	81.65	3.75	20.58

Sadeghzadeh, Amir Mahdi, Saeed Shiravi, and Rasool Jalili. "Adversarial network traffic: Towards evaluating the robustness of deep-learning-based network traffic classification." *IEEE Transactions on Network and Service Management* 18.2 (2021): 1962-1976.

Identificação de dispositivos IoT

- 8 trabalhos (2 revisões)

AML

- 8 trabalhos (1 revisão)