# Projeto INSaNE

Edmundo de Souza e Silva

UFRJ

19º WRNP
Workshop RNP
7 | 8 MAIO
Campos do Jordão | SP

RNP

# Improving Network Security at the Network Edge
# INSaNE
# (UFRJ, UFPA, UFMG , UMASS)

Edmundo de Souza e Silva[1]
(coordenador)

Federal University of Rio de Janeiro
[1]Systems Engineering and Computer Science Department, COPPE

2018

# INSaNE

## Objetivo Geral

Desenvolver técnicas e algoritmos para:

- identificar e classificar comportamentos maliciosos na rede (como ataques DDoS)
- detectar dispositivos comprometidos nas redes domésticas

# Objetivos

- Desenvolver um *framework*:
  - elaborar métodos
  - gerar medições apropriadas

  para deteção e classificação de comportamentos maliciosos na rede;
- A partir de medidas em ambientes reais de ISPs:
  - desenvolver modelos de condições normais de rede
  - desenvolver algoritmos para detetar anomalias e condições maliciosas.
- Desenvolver algoritmos para monitorar e detetar vazamentos de privacidade a partir de medições de rede em gateways domésticos.

# Objetivos

- Desenvolver um *framework*:
  - elaborar métodos
  - gerar medições apropriadas

  para deteção e classificação de comportamentos maliciosos na rede;
- A partir de medidas em ambientes reais de ISPs:
  - desenvolver modelos de condições normais de rede
  - desenvolver algoritmos para detetar anomalias e condições maliciosas.
- Desenvolver algoritmos para monitorar e detetar vazamentos de privacidade a partir de medições de rede em gateways domésticos.

# Objetivos

- Desenvolver um *framework*:
  - elaborar métodos
  - gerar medições apropriadas

  para deteção e classificação de comportamentos maliciosos na rede;
- A partir de medidas em ambientes reais de ISPs:
  - desenvolver modelos de condições normais de rede
  - desenvolver algoritmos para detetar anomalias e condições maliciosas.
- Desenvolver algoritmos para monitorar e detetar vazamentos de privacidade a partir de medições de rede em gateways domésticos.

# Objetivos

- Atacar o problema de segurança de redes domésticas, pelo roteador de borda.
- Aplicar técnicas de aprendizagem não supervisionado de padrões espaço/temporais para identificar comportamento anômalo

# Objetivos

- fazer extensa análise de dados usando séries temporais coletadas
- identificar mudanças estatísticas (tráfego, etc) e inferir automaticamente possíveis causas dessas alterações.
- criar perfis do comportamento normal de dispositivos IoT usar esses perfis/modelos para detectar quando os dispositivos comportarem-se anormalmente
- realizar medições controladas em ambiente de laboratório para estudar comportamento de dispositivos.
- detectar assinaturas de dados transferidos para servidores IoT

# Objetivos

- fazer extensa análise de dados usando séries temporais coletadas
- identificar mudanças estatísticas (tráfego, etc) e inferir automaticamente possíveis causas dessas alterações.
- criar perfis do comportamento normal de dispositivos IoT usar esses perfis/modelos para detectar quando os dispositivos comportarem-se anormalmente
- realizar medições controladas em ambiente de laboratório para estudar comportamento de dispositivos.
- detectar assinaturas de dados transferidos para servidores IoT

# Objetivos

- fazer extensa análise de dados usando séries temporais coletadas
- identificar mudanças estatísticas (tráfego, etc) e inferir automaticamente possíveis causas dessas alterações.
- criar perfis do comportamento normal de dispositivos IoT usar esses perfis/modelos para detectar quando os dispositivos comportarem-se anormalmente
- realizar medições controladas em ambiente de laboratório para estudar comportamento de dispositivos.
- detectar assinaturas de dados transferidos para servidores IoT

# Objetivos

- fazer extensa análise de dados usando séries temporais coletadas
- identificar mudanças estatísticas (tráfego, etc) e inferir automaticamente possíveis causas dessas alterações.
- criar perfis do comportamento normal de dispositivos IoT usar esses perfis/modelos para detectar quando os dispositivos comportarem-se anormalmente
- realizar medições controladas em ambiente de laboratório para estudar comportamento de dispositivos.
- detectar assinaturas de dados transferidos para servidores IoT

# Objetivos

- fazer extensa análise de dados usando séries temporais coletadas
- identificar mudanças estatísticas (tráfego, etc) e inferir automaticamente possíveis causas dessas alterações.
- criar perfis do comportamento normal de dispositivos IoT usar esses perfis/modelos para detectar quando os dispositivos comportarem-se anormalmente
- realizar medições controladas em ambiente de laboratório para estudar comportamento de dispositivos.
- detectar assinaturas de dados transferidos para servidores IoT

# Avanços esperados

- Novas perspectivas para entender o comportamento de redes domésticas e identificar comportamentos anômalos
- Entender a natureza ainda muito desconhecida sobre o tráfego de IoTs e o ecossistema desses dispositivos
- Combinação de habilidades, coleta de dados no mundo real e uma base sólida de aprendizado de máquina e análise
- Potencial para mitigar o problema de botnets/DDoS

# Avanços esperados

- Novas perspectivas para entender o comportamento de redes domésticas e identificar comportamentos anômalos
- Entender a natureza ainda muito desconhecida sobre o tráfego de IoTs e o ecossistema desses dispositivos
- Combinação de habilidades, coleta de dados no mundo real e uma base sólida de aprendizado de máquina e análise
- Potencial para mitigar o problema de botnets/DDoS

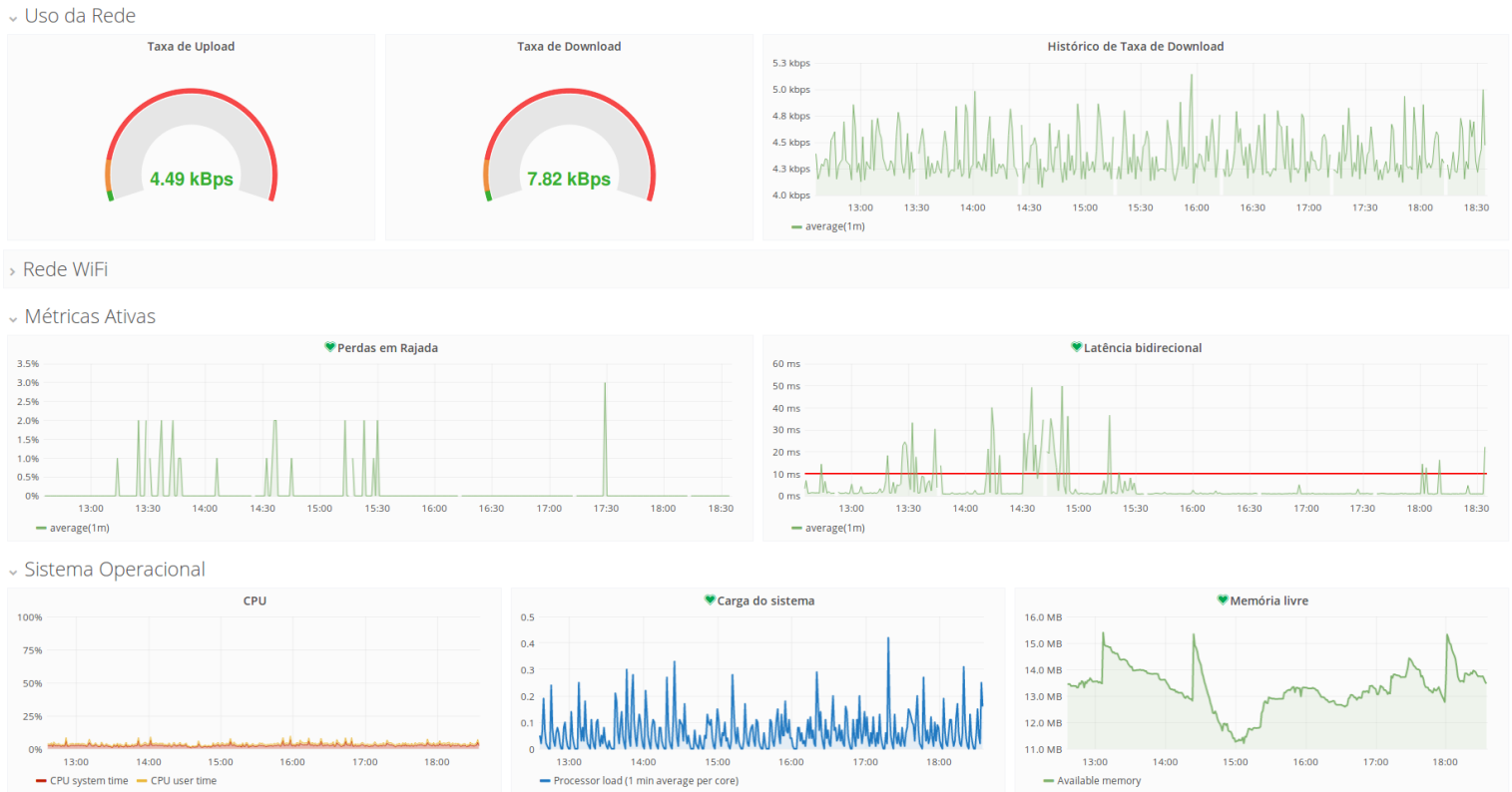
# Avanços esperados

- Novas perspectivas para entender o comportamento de redes domésticas e identificar comportamentos anômalos
- Entender a natureza ainda muito desconhecida sobre o tráfego de IoTs e o ecossistema desses dispositivos
- Combinação de habilidades, coleta de dados no mundo real e uma base sólida de aprendizado de máquina e análise
- Potencial para mitigar o problema de botnets/DDoS

# Avanços esperados

- Novas perspectivas para entender o comportamento de redes domésticas e identificar comportamentos anômalos
- Entender a natureza ainda muito desconhecida sobre o tráfego de IoTs e o ecossistema desses dispositivos
- Combinação de habilidades, coleta de dados no mundo real e uma base sólida de aprendizado de máquina e análise
- Potencial para mitigar o problema de botnets/DDoS

# Exemplo de coleta no campo



# Workshops

- Úteis para:
  - Entender o escopo da chamada, conhecer vários interesses na área
  - Estruturar as ideias para organizar um projeto
- Parcerias internacional:
  - Já estava consolidada muito antes

# Workshops

- Úteis para:
  - Entender o escopo da chamada, conhecer vários interesses na área
  - Estruturar as ideias para organizar um projeto
- Parcerias internacional:
  - Já estava consolidada muito antes

# Parceiro Americano: UMass

- Extensa colaboração há mais de 15 anos.
- Acesso mútuo a dados, laboratórios, experiência
- Dados reais no Brasil - parceria ISP e startup

# Parceiro Americano: UMass

- Extensa colaboração há mais de 15 anos.
- Acesso mútuo a dados, laboratórios, experiência
- Dados reais no Brasil - parceria ISP e startup

# Parceiro Americano: UMass

- Extensa colaboração há mais de 15 anos.
- Acesso mútuo a dados, laboratórios, experiência
- Dados reais no Brasil - parceria ISP e startup

# Parceiros Brasileiros

- UFRJ-UFPA: nova parceria - interação entre alunos, cursos, etc.
- UFRJ/UFMG: parceria antiga

# Parceiros Brasileiros

- UFRJ-UFPA: nova parceria - interação entre alunos, cursos, etc.
- UFRJ/UFMG: parceria antiga

# Conclusões

- Atraso de mais de 6 meses na assinatura do contrato dificultou MUITO o inicio do projeto e integração entre grupos
- Mas já estamos reestruturados!

# Conclusões

- Atraso de mais de 6 meses na assinatura do contrato dificultou MUITO o inicio do projeto e integração entre grupos
- Mas já estamos reestruturados!

# Nosso Grupo

- UFRJ
  - Edmundo de Souza e Silva
  - Rosa M.M. Leão
  - Daniel S. Menasche
  - 1 pos-doc, 3 estudantes doutorado, 1 pesquisador, 2 estudantes mestrados, 3 estudantes de graduação.
  - incubada UFRJ
- UFMG e UPFA:
  - Antonio Abelém (DCC/UFPA): 1 estudante doutorado , 1 estudante mestrado, 4 estudantes de graduação.
  - Ana Paula Couto da Silva (DCC/UFMG) e estudantes;
- EUA:
  - Don Towsley (UMASS/USA)
  - Phillipa Gill (UMASS/USA)

# FIM

**Obrigado!**
**PERGUNTAS?**