LabNet

Laboratório de Redes e Multimídia

Internet das Tretas: como a IoT afeta nossa segurança e privacidade?

Sávyo Morais - FIB10 - Set/2020

Universidade Federal do Rio de Janeiro

Instituto Tércio Pacitti de Aplicações e Pesquisas Computacionais

E agora? Quem poderá nos defender?

A academia tem ajustado os **métodos criptográficos** e de **autenticação**, adaptando-os às limitações de *hardware* e comunicação impostas pelos novos casos de uso trazidos pela IoT.

Além disso, os novos paradigmas de uso e comunicação têm despertado a necessidade de melhores ferramentas de **detecção de incidentes** e **controle de acesso**.

LabNet

Qual meu plano para salvar o mundo?

Tudo começa pela RFC 8520 - Manufacturer Usage Description (MUD).

A MUD define meios para um dispositivo IoT dizer exatamente quais as comunicações de rede ele pode realizar.

Tudo o que não foi informado é bloqueado.

Isto reduz a possibilidade de infecção e exploração de um dispositivo vulnerável.

Porém este ainda é um *Internet Standard* pouco adotado.

LabNet

INXU

Intra-**N**etwork e**X**posure analyzer **U**tility

Uma extensão de segurança à MUD

O INXU permite que especialistas de segurança protejam redes IoT domésticas de ataques conhecidos, sem quebra de privacidade.

Proteção contra ataques conhecidos:

- Botnets, Worms, Ransomwares
- Novos *exploits*
- *Script Kiddies*

Funcionamento do INXU

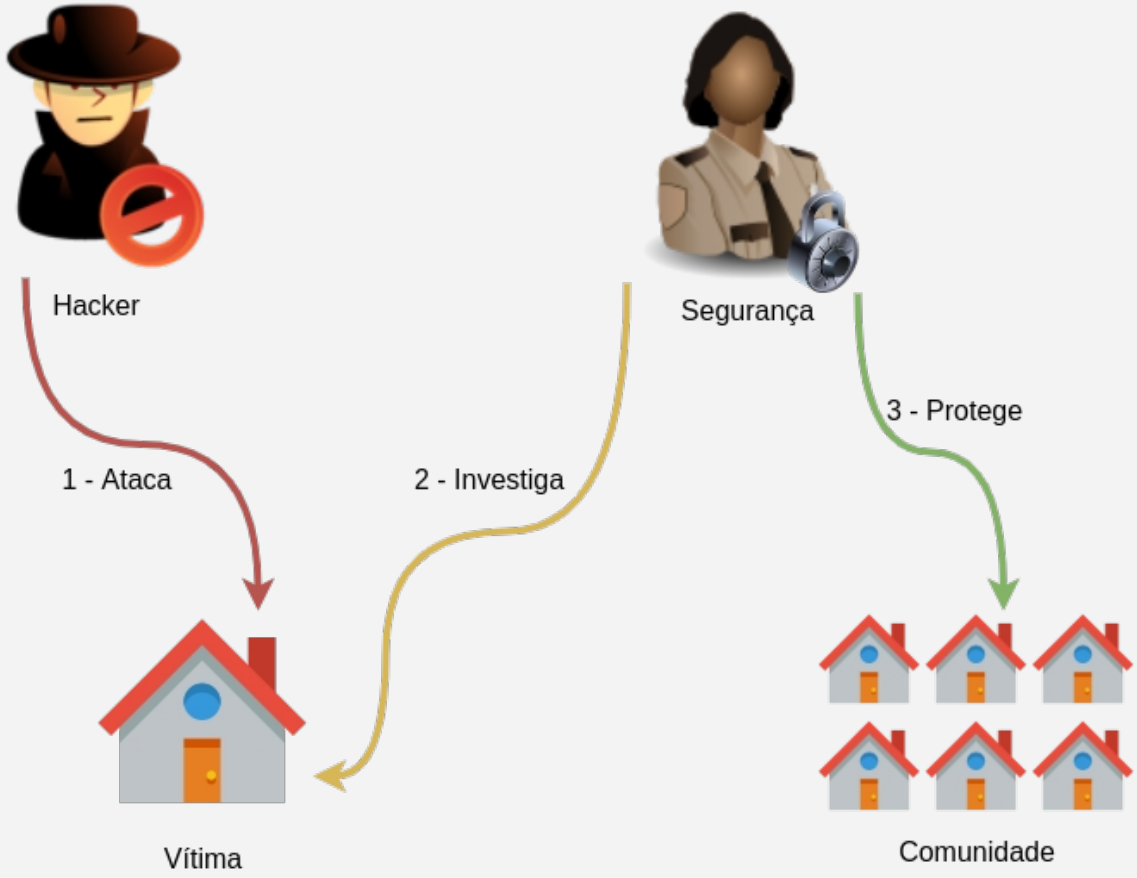
Especialistas em segurança:

1. Coletar informações sobre tráfegos de rede relacionados a atividades maliciosas
2. Descrever os tráfegos maliciosos
3. Distribuir as descrições para as redes domésticas

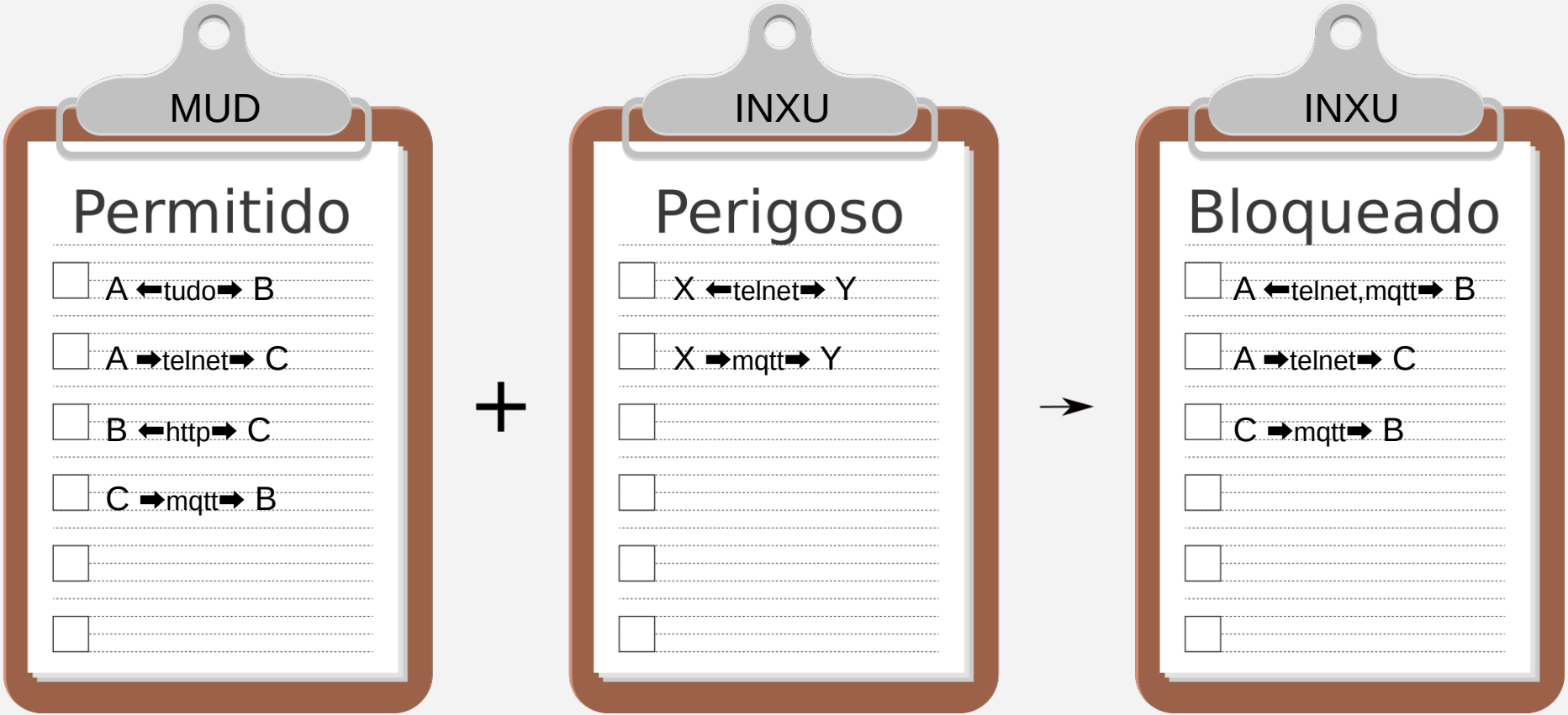
Redes Domésticas:

1. Coletar as MUDs dos dispositivos conectados
2. Coletar as descrições de tráfego malicioso
3. Comparar os dados da MUD com as descrições de tráfego malicioso
4. Bloquear exposições a vulnerabilidades e ataques

Lab Net



Funcionamento do INXU - pt. 1



Funcionamento do INXU - pt. 2

Próximos passos do INXU

- Validar e ajustar a proposta a outros *stakeholders*
  - Usuários Finais
  - Centros de Operação em Segurança
  - Indústria de dispositivos IoT domésticos
  - Cidades Inteligentes????
- Submeter como Internet-Draft no IETF

FIM!

Dúvidas?

Contato:

savyovm@gmail.com

savyo.morais@labnet.nce.ufrj.br

https://www.linkedin.com/in/savyo-morais/