THE DEVELOPER'S CONFERENCE

Trilha: *Internet* das coisas

Privacidade para a *Internet* das coisas: muito além da criptografia

Antônio Janael Pinheiro

Agenda

Quem sou eu?

- Doutorando em Ciência da Computação pelo Centro de Informática da UFPE;
- Pesquisador em privacidade para IoT.

Privacidade

- "Privacidade é a reivindicação dos indivíduos em determinar por si mesmos quando, como e em que medida as suas informações são comunicadas a terceiros."(Alan Westin)

Autonomia e liberdade

Anonimização

Internet das Coisas que te vigiam

- Microfones, câmeras e todo tipo de sensor;
- Dispositivos IoT computacionalmente restritos;
- Fabricantes negligentes.


BIG BROTHER
IS WATCHING YOU

Tráfego de rede criptografado

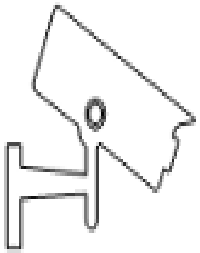
- A criptografia protege o conteúdo do tráfego;
- Variações nos tipos de dados refletem nos metadados;
- A criptografia é insuficiente para ocultar metadados.

Racional

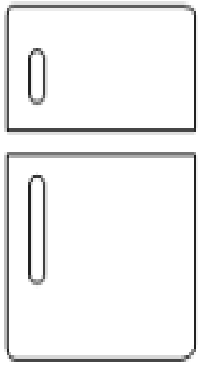
- Diferentes aplicações produzem pacotes com tamanhos distintos;
- Implementações distintas de uma aplicação geram padrões diferentes;
- Tipicamente, dispositivos IoT têm um propósito específico.












Classificação de tráfego com *Machine Learning*

- Identificar padrões expostos por metadados;
- Empregar atributos do tráfego como *features* para a construção de modelos;
- Construir um perfil do comportamento normal de um dispositivo IoT [Pinheiro19].

Avaliação – oportunidades

- Distinguir entre dispositivos IoT e não IoT;
- Identificar dispositivos específicos;
- Determinar os eventos que produziram o tráfego.

Resultados – alguns números...

- Resultados com o *Random Forest*:
  - Precisão de 99% na distinção entre dispositivos IoT e não IoT;
  - Acurácia de 96% na identificação de dispositivos IoT;
  - Acurácia de 99% na identificação de eventos IoT.

Ofuscação de tráfego

- Ocultar metadados do tráfego;
- *Packet padding* [Pinheiro18a];
- *Trade-off privacy-overhead*.

Packet padding – proposta

- Selecionar aleatoriamente o número de *bytes* inseridos nos pacotes [Pinheiro18a];
- Implementar a solução como um *middlebox* no roteador residencial;
- Simplificar a implementação da proposta de *padding*.

Packet padding – resultados

- Reduzir a acurácia do Random Forest na identificação de dispositivos de 96% para 14,5%;
- Elevar o atraso em até 0,05ms, no pior cenário;
- Introduzir uma perda de pacotes inferior a 1%.

Pseudo-anonimização – problema

- Identificação dos dispositivos ativos em uma rede;
- Parceiros de comunicação;
- Hábitos dos usuários de dispositivos IoT;
- Inferir doenças e problemas de saúde.

Pseudo-anonimização – proposta

- Ocultar os endereços dos dispositivos através do equipamentos de rede [Pinheiro18b];
- Solução transparente aos dispositivos e usuários IoT;
- Ofuscar os relacionamentos entre dispositivos IoT e servidores;
- Evitar que observadores identifiquem os equipamentos ativos.

Pseudo-anonimização – resultados

- Mapear 302 endereços IPv4 em 10.602, sem interferir na comunicação dos dispositivos;
- Elevar o número de relacionamentos entre dispositivos visíveis a uma observador de 338 para 5301;
- Cada conexão entre dispositivo e servidor é representada por pseudônimos distintos, que contribui para ocultar os verdadeiros endereços de um observador.

Lições aprendidas

- Adote a privacidade como um requisito do seu projeto;
- Criptografe os dados transmitidos pelo seu dispositivo;
- Além da criptografia, implemente outros mecanismos para aprimorar a privacidade.

Ferramentas úteis

- Protocolos de segurança: TLS e SSL;
- *Packet padding*: TLS e SSL;
- Pseudo-anonimização: projeto TOR;
- Ofuscação de tráfego: protocolo obfs4 do projeto TOR.

Vamos conversar?

- LinkedIn: linkedin.com/in/janael-pinheiro/;
- *WhatsApp* e *Telegram*: (81) 995897449;
- E-mail: ajp@cin.ufpe.br.

Agradecimentos

Agradeço ao prof. Divanilson Campelo, Jeandro Bezerra e Caio Burgardt, co-autores dos artigos citados nesta apresentação.

Conclusão

- Privacidade é um direito natural dos indivíduos;
- A IoT tem potencial para destravar valor em vários setores da economia;
- As ameaças à privacidade introduzidas pela IoT são imensas;
- É possível prover conveniência para os usuários IoT sem violar a sua privacidade.

Obrigado!

Questões?

Referências I

- A. J. Pinheiro, J. M. Bezerra, and D. R. Campelo, *Packet padding for improving privacy in consumer iot*, 2018 IEEE Symposium on Computers and Communications (ISCC), June 2018, pp. 00925–00929.
- Antonio J. Pinheiro, Caio A. P. Burgardt, and Divanilson R. Campelo, *Preservando a privacidade na internet das coisas com pseudônimos usando sdn*, Anais do XVIII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais (Porto Alegre, RS, Brasil), SBC, 2018, pp. 121–128.

Referências II


Antônio J. Pinheiro, Jeandro de M. Bezerra, Caio A.P. Burgardt, and Divanilson R. Campelo, *Identifying iot devices and events based on packet length from encrypted traffic*, Computer Communications **144** (2019), 8 – 17.