IoT-Flows Lightweight Policy Enforcement of Information Flows in IoT Infrastructures

EQUIPE

Coordenador no Brasil
José Augusto Suruagy Monteiro (UFPE)

Coordenadores nos Estados Unidos
Prof. Darko Marinov (UIUC)
Prof. Atul Prakash (UMich)

Parceiro brasileiro
Centro de Informática da Universidade Federal de Pernambuco (UFPE)

Parceiros:
University of Illinois at Urbana-Champaign (UIUC)
University of Michigan Ann Arbor (UM)

SITE
iot-flows.cin.ufpe.br

CONTATO
iot-flows@cin.ufpe.br

DESCRIÇÃO

À medida que sistemas de Internet das Coisas (*Internet of Things, ou IoT*) forem implantados mais amplamente, a sua segurança tem se tornado uma grande preocupação. Por exemplo, o *malware* Mirai comprometeu milhões de dispositivos de IoT e os usou para lançar o maior ataque DDoS até o momento. Trabalhos anteriores mostraram que plataformas IoT para as "casas inteligentes" também são vulneráveis a ataques. A segurança de sistemas IoT é uma grande preocupação em muitos outros domínios, por exemplo, carros autônomos e sistemas de controle industrial. Falhas de segurança nesses sistemas de IoT poderiam levar à perda de privacidade, roubo de dados, perdas financeiras e até danos físicos.

Este trabalho se propõe a desenvolver uma nova abordagem para fortalecer a segurança de sistemas IoT através de uma defesa *cross-layer* na camada de aplicação IoT, camada de rede e nos dispositivos. O conceito central é o de políticas de fluxos: pretende-se inicialmente extrair as políticas de fluxo a partir dos aplicativos IoT, e depois utilizar essas políticas para controlar os fluxos desejados assim como detectar violações tanto no dispositivo como nas camadas de rede. Ao contrário de aplicações de uso geral, os fluxos em aplicativos de IoT são, em geral, previsíveis e suficientemente expressivos para capturar propriedades importantes de modo que as violações detectadas de fluxo indiquem problemas reais e não falsos alarmes.

Uma defesa *cross-layer* é difícil de ser feita em redes de computadores convencionais por causa da complexidade das aplicações dos computadores de mesa e de suas constantes modificações devido a atualizações de *software* e instalação de novos *softwares*. Em contraste, esse tipo de defesa em sistemas IoT pode ser tanto viável como prática. Os ambientes de IoT tendem a ter uma estrutura mais *regular* (interfaces mais claras com os dispositivos com os quais interagem e um modelo de programação orientado a eventos) do que as aplicações que rodam em computadores de uso geral numa rede. Portanto, os ambientes IoT são mais adequados a análises automatizadas. Além do mais, o conjunto de aplicativos IoT instalados tendem a ser relativamente estáveis em comparação a uma rede típica de computadores de mesa. Essa regularidade e estabilidade fornecem uma oportunidade para avançar o estado-da-arte.

IoT-Flows - Lightweight Policy Enforcement of Information Flows in IoT Infrastructures

O trabalho proposto está organizado em três eixos:

Eixo 1: **Extração e especificação de políticas de fluxo** para aplicações IoT. Pretendemos extrair políticas de fluxo detalhadas a partir do código do aplicativo. Por exemplo, num escritório, podemos ter um *app* IoT que permite controlar um projetor a partir de um interruptor em uma dada sala de modo que o projetor liga quando o interruptor é acionado. Neste caso, há um fluxo preciso entre o interruptor e o projetor por uma sequência de eventos de rede, desde o evento de acionamento do interruptor até o app IoT e o projetor ser ligado. Esse eixo tem como finalidade extrair políticas (de baixo para cima) e definir uma linguagem para controlar o atendimento às políticas (de cima para baixo).

Eixo 2: **Controle distribuído do controle de atendimento às políticas de fluxo**. O objetivo é identificar qualquer fluxo que esteja inconsistente com os fluxos especificados. No nosso exemplo do projetor e do interruptor, esses fluxos inconsistentes incluiriam tentativas de controlar diretamente o projetor pela injeção de eventos falsos ou pelo envio de eventos a partir de outros interruptores. Enquanto que o trabalho prévio de membros da equipe tinha focado no controle centralizado das políticas de fluxo, planejamos distribuir os pontos de controle dentro da rede IoT de modo que as políticas possam ser obedecidas fim-a-fim, mesmo quando houver ataques de níveis abaixo. Esquemas de controle baseados em um único *hub* são frágeis pelos seguintes motivos: (i) um dispositivo corrompido pode se comunicar diretamente com a internet ou outros dispositivos ignorando o *hub*, (ii) um único *hub* não consegue hospedar instalações de grande porte ou distribuídos geograficamente, e (iii) um único *hub* pode se tornar um ponto único de falha e de ataques. Pontos de controle podem também incluir um ou mais *hubs*/roteadores dentro da rede pela qual os dispositivos IoT se conectam. Um desafio chave consiste no tratamento desse ambiente dinâmico, em função da entrada de novos usuários e dispositivos no sistema, políticas dinâmicas de fluxo dependentes da localização, assim como atualizações dos aplicativos.

Eixo 3: **Avaliação e testes**. Instalaremos um conjunto de dispositivos na nossa infraestrutura configurado com defesas distribuídas de controle de fluxo. Planejamos realizar testes de ataques para avaliar a nossa abordagem em diversos cenários incluindo a atualização (autorizada ou não) de aplicações IoT, adição de novos dispositivos, ou a instalação de novo *firmware*. Por exemplo, considere que o *firmware* de um dispositivo esteja comprometido, como no caso de um ataque Mirai, que introduz um novo fluxo (não observado em execuções anteriores), com origem em um dispositivo na rede. O novo fluxo pode ser uma tentativa de vazar dados ou atacar máquinas remotas. Nosso objetivo é validar se as políticas de fluxo estão especificadas em um nível de detalhes que permita a detecção desses ataques. Enquanto muitos dispositivos possuem fluxos com a internet como parte do seu funcionamento normal, o fluxo normal não é necessariamente direto (pode ser por *apps* IoT) e não para servidores ou portas arbitrárias. Espera-se que os fluxos estejam de acordo com os *apps* IoT que estejam rodando no sistema. Desse modo, os testes irão verificar se o sistema consegue detectar violações. Além do mais, serão avaliadas não apenas o quão expressivas sejam as nossas políticas de fluxo (do Eixo 1) mas também qual seria a sobrecarga gerada pela verificação das mesmas usando o nosso sistema (do Eixo 2).

Consórcio:

Centro de Informática UFPE — UFPE — University of Michigan