Aspectos de Segurança no Desenvolvimento de *Software* para Internet das Coisas

Evandro L. C. Macedo

[1]Programa de Engenharia de Sistemas e Computação (PESC/COPPE)
Universidade Federal do Rio de Janeiro (UFRJ) — Rio de Janeiro – RJ
Rio de Janeiro – RJ – Brasil

Abstract. *The Internet of Things (IoT) has been gaining increasing visibility among emerging technologies. However, as the number of connected devices grows, responsibility also increases, especially in terms of security, privacy and reliability of information exchanged between devices. Cyber attacks might be possible, for example, due to coding vulnerability, which makes devices potential attack vectors. This article highlights the importance of considering security aspects during IoT applications development. Suggestions are given with respect to each discussed aspect in order to foster guidelines for good practices and design patterns.*

Resumo. *A Internet das Coisas (IoT) vem ganhando cada vez mais destaque dentre as tecnologias emergentes. Entretanto, à medida que o número de dispositivos conectados cresce, as responsabilidades também crescem, principalmente em termos de segurança, privacidade e confiabilidade das informações trocadas entre os dispositivos. Uma forma usual de um ataque cibernético ser possibilitado é por conta de vulnerabilidades de código, o que torna os dispositivos possíveis vetores de ataques. Neste artigo destaca-se a importância de considerar aspectos de segurança durante o desenvolvimento de aplicações para IoT. Sugestões são colocadas de acordo com os aspectos abordados com o intuito de fomentar diretrizes de boas práticas e padrões de projeto.*

1. Introdução

A Internet das Coisas (IoT) [Atzori et al. 2010] vem ganhando cada vez mais destaque dentre as tecnologias emergentes. Como prova disso, diversas pesquisas apontam o crescimento no número de dispositivos conectados à Internet. Estima-se que em 2021 cerca de 28 bilhões de dispositivos ("coisas")[1] estejam conectados à grande rede.

Em relação ao contexto de IoT no Brasil, o desenvolvimento dessa tecnologia ainda se encontra em fase prematura, o que por um lado pode ser bom por permitir que opiniões sejam colocadas em pauta para definições de diretrizes bem fundamentadas. Atualmente já existem esforços por parte do Governo para a criação de um plano de ação, o Plano Nacional de IoT [BNDES 2016], que reúne discussões sobre como o Brasil pode agregar IoT a seu parque tecnológico, a fim de colocar o país em posição de destaque frente aos países que já desenvolvem IoT. Dessa forma, a qualidade dos serviços essenciais para o cidadão pode ser melhorada (saúde, educação, transporte, segurança,

[1]O estudo considera para a estimativa qualquer dispositivo que tenha capacidade de conexão com uma rede, ou seja, que implemente a pilha de protocolos IP.

entre outros), assim como em termos de infraestrutura e logística do país, como as malhas elétricas, processos de produção em indústrias (considerando inclusive a Indústria 4.0), entre outros. O plano está em desenvolvimento, tendo como objetivo destacar características dentro de um modelo de referência para norteamento de ações frente à IoT.

Muitos são os benefícios trazidos pela Internet das Coisas, conforme estudos vêm mostrando ao longo dos anos [Al-Fuqaha et al. 2015], pois permite que novas aplicações sejam desenvolvidas, assim como aplicações já existentes sejam melhoradas. Exemplos bem estabelecidos dessas aplicações são: *home care*, casas inteligentes, computação vestível, cidades inteligentes, Indústria 4.0, redes veiculares, fazendas inteligentes, entre outras. A ideia de ter conectividade a qualquer momento, para qualquer coisa, em qualquer lugar (do inglês, *anytime, anything, anywhere*) é tentadora. Entretanto, é preciso ter atenção para determinadas questões.

À medida que o número de dispositivos conectados cresce, as responsabilidades também crescem, principalmente em termos de segurança, privacidade e confiabilidade das informações trocadas entre os dispositivos. Um dos maiores ataques distribuídos de negação de serviço (*Distributed Denial of Service* – DDoS), ocorrido no dia 21 de outubro de 2016, que afetou um grande provedor de serviço de resolução de nomes (*Domain Name Service* – DNS) nos Estados Unidos, chamado Dyn, indisponibilizou diversos *sites* como Twitter, Reddit, Spotify, PayPal, entre outros. A carga gerada pelo ataque ficou entre 10 a 20 vezes o volume de tráfego normal esperado, em torno de 1Tbps, derrubando os *sites* que dependiam do serviço de DNS da empresa atacada. O mais interessante nesse caso é que os atacantes se valeram da Internet das Coisas para efetivar o ataque, utilizando uma *botnet* formada por dispositivos ("coisas") conectados à Internet, como câmeras e roteadores que apresentavam algum tipo de vulnerabilidade (como configurações com senhas padrão de fácil acesso, ou implementações de código inseguro). Esse fato serve como alerta crítico para que ações sejam tomadas em direção à inclusão de aspectos envolvendo segurança como parte dos projetos de desenvolvimento dos *softwares* para IoT.

Tendo isso em mente, este artigo ressalta a importância de considerar aspectos de segurança durante o desenvolvimento de aplicações para Internet das Coisas, visando obter direcionamentos para boas práticas e padrões, a fim de incentivar a preocupação desses aspectos como parte do desenvolvimento de *software*, que por vezes, são tratados como opcionais.

2. Aspectos de Segurança e Sugestões

A literatura aborda de forma veemente o termo Internet das Coisas, ao passo que o que realmente faz IoT funcionar são as "coisas da Internet", ou seja, as partes que compõem a infraestrutura que viabiliza as diversas aplicações. Podem ser consideradas como as "coisas da Internet" a infraestrutura de rede que permite conectividade física, os protocolos de comunicação que permitem conectividade lógica, os serviços oferecidos, bem como os *softwares* que executam nos dispositivos.

Em termos de segurança da informação, uma forma muito comum de um ataque cibernético ser possibilitado é por conta de vulnerabilidades de código. A princípio, entende-se que *bugs* e erros de programação são comuns de ocorrerem durante o desenvolvimento de *software* e que são tratados em fases como as de teste. Contudo, testes específicos envolvendo cenários de segurança da informação podem não ser abordados

durante os testes de segurança, tanto na fase estática (por inspeção de código, sem sua execução, por exemplo), quanto na dinâmica (com a aplicação em operação). Dispositivos conectados à Internet de forma insegura permitem a formação de *botnets*, habilitando ataques cibernéticos que podem gerar grandes prejuízos, inclusive financeiros, para diversos usuários da Internet.

O que pode ser colocado em pauta é a utilização de auditoria de código, principalmente em termos de desenvolvimento de *software* para dispositivos IoT, a fim de que os códigos desenvolvidos passem necessariamente por uma bateria de testes de segurança. Esses testes iriam além dos testes de funcionalidade, ou testes unitários, por exemplo, tendo o intuito de submeter os programas desenvolvidos a situações de invasão ou tentativas de quebra de segurança, por exemplo. Dessa forma, vulnerabilidades já conhecidas seriam resolvidas, além de permitir a descoberta de novas vulnerabilidades de maneira proativa.

As equipes de desenvolvimento também poderiam ser beneficiadas com treinamentos que capacitem os desenvolvedores com habilidades necessárias para identificação de vulnerabilidades de código, além da aplicação de testes de segurança mencionados. Com isso, padrões de projeto voltados ao desenvolvimento seguro de *software* podem ser estabelecidos, permitindo ter conhecimento prévio sobre *bugs* e falhas de programação que se tornariam potenciais vetores de ataques cibernéticos.

Outro aspecto a ser considerado são as configurações de fábrica (ou configurações *default*), que merecem atenção e que por vezes também atuam como vetores para ataques cibernéticos. Uma proposta inicial para campos de senhas, por exemplo, seria a geração dessas configurações padrão de maneira aleatória durante o processo de instalação dos *softwares* nos dispositivos. De modo geral, a definição de critérios para escolha de parâmetros-padrão para o projeto de desenvolvimento de *software* de IoT pode ser um ponto de partida para também reduzir riscos de vulnerabilidade.

3. Considerações Finais

Neste artigo foi destacada a importância de considerar aspectos de segurança durante o desenvolvimento de aplicações, em particular no âmbito de IoT. Espera-se a definição de diretrizes para alavancar a criação e adoção de boas práticas e padrões de projeto que norteiem o desenvolvimento de *software* que considere os aspectos de segurança apresentados (entre outros), permitindo o uso de IoT de forma segura, privativa e confiável.

Referências

Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., and Ayyash, M. (2015). Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. *IEEE Communications Surveys Tutorials*, 17(4):2347–2376.

Atzori, L., Iera, A., and Morabito, G. (2010). The Internet of Things: A survey. *Computer Networks*, 54(15):2787 – 2805.

BNDES (2016). Internet das Coisas: Um Plano de Ação para o Brasil. http://www.bndes.gov.br/wps/portal/site/home/conhecimento/estudos/chamada-publica-internet-coisas/estudo-internet-das-coisas-um-plano-de-acao-para-o-brasil.