Universidade de Pernambuco
Programa de Pós-Graduação em Engenharia da Computação (PPGEC)

Proposta de Dissertação de Mestrado

Área: Computação Inteligente / Reconhecimento de Padrões

Título:Antivírus para Detecção de Malwares IoT Especializados em Corromper Câmeras de Vigilância

Orientador – Sérgio Murilo Maciel Fernandes (smurilo@ecomp.poli.br)

Co-orientador – Sidney Marlon Lopes de Lima (sidney.lima@ufpe.br)

Descrição

O paradigma IoT (Internet das Coisas) está relacionado à interconexão de objetos usados no cotidiano através da rede mundial de computadores. Nos últimos anos a internet das coisas vem apresentando um grande avanço, tanto em aplicações empresariais, quanto residenciais. A estimativa é de que a Internet das Coisas alcance cerca de 50 bilhões de dispositivos conectados em 2020 (CISCO, 2011). O paradigma de IoT abrange conceitos de inteligência artificial, criptografia, segurança de redes, sensores de baixo consumo de energia, dentre outros, conforme descrito em (GIUSTO et al. 2010). A IoT propicia o entretenimento a exemplo das televisões inteligentes, possibilitando a combinação de filmes, programas de TV e interação através de redes sociais em tempo real. A IoT também foca o cumprimento das responsabilidades profissionais como nos veículos autônomos. Através da visão computacional, a IoT possibilita que milhares de informações possam ser adquiridas e processadas em tempo real. Contudo, um dos grandes desafios da IoT está relacionado a Segurança da Informação, uma vez que seus sistemas computacionais são relativamente recentes. Tal fato possibilita que milhares de *malwares* se manifestem em uma grande quantidade de aplicações legítimas, o que ameaça de forma grave a segurança dos sistemas. "*Malware*" é uma junção dos termos "malicioso" e "software". O *malware* tem como objetivo acessar um dispositivo alheio sem permissão explícita de seu proprietário, coletando, entre outras coisas, dados confidenciais e pessoais dos usuários. Atualmente, as organizações buscam detectar *malwares* através do uso de inteligência artificial, aprendizagem de máquina e ciência de dados (SANS, 2019). Logo, os antivírus do estado-da-arte propõem a extração de características do aplicativo suspeito, de maneira preventiva, antes de executá-lo. Essa metodologia é capaz de obter taxas médias de acertos superiores a 90% na detecção de *malwares* em computadores Windows (LIMA, et al., 2019). De forma adversa, os antivírus para Windows são inválidos quando aplicados para os *malwares* voltados para IoT. A dificuldade diz respeito à natureza multiplataforma dos sistemas IoT. Os dispositivos conectados possuem distintas arquiteturas computacionais (e.g..; arm, mips, powerpc, 8056) em relação ao Windows. Cada uma dessas arquiteturas possui repertório particular de instruções, bibliotecas e APIs completamente diferentes do Windows. Em síntese, um antivírus para Windows não é capaz de identificar *malwares* IoT. Logo, a proposta do projeto de pesquisa visa a criação de um antivírus com o objetivo de reconhecer *malwares* para IoT, especializados em corromper câmeras de vigilância. A motivação é que a corrupção das câmeras de vigilância pode afetar a segurança como um todo, tanto digital quanto física da vítima, uma vez que tais câmeras são empregadas na segurança patrimonial, em regra geral. As câmeras de vigilância também são capazes de monitorar, em tempo real, o tráfego e a logística urbana além do fluxo dos recursos humanos e materiais. Portanto, a corrupção das câmeras de vigilância pode vir a causar prejuízos irreversíveis e irrecuperáveis. Tecnicamente, na etapa de extração de características, devem ser analisados os comportamentos e rotinas suspeitas extraídas dos aplicativos IoT suspeitos. Na etapa de classificação, haverá o reconhecimento de padrão dos comportamentos atrelados a atividades maliciosas, especificamente, através de *Deep Learning* (Redes Neurais Profundas). O macro-objetivo é distinguir os aplicativos suspeitos IoT entre benignos e *malwares*.

Referências Bibliográficas

GIUSTO, D. *et al.* The Internet of Things: 20th Tyrrhenian Workshop on Digital Communications, Springer, London 2010

CISCO. A Internet das Coisas: Como a próxima evolução da Internet está mudando tudo.Disponível em: https://www.cisco.com/c/dam/global/pt_br/assets/executives/pdf/internet_of_things_iot_ibsg_0411final.pdf. Acesso em Junho de 2019, 2011.

LIMA, S. M. L. *et al.* Antivírus dotado de Rede Neural Artificial visando Detectar Malwares Preventivamente. iSys - Brazilian Journal of Information Systems, 11 (4), p. 31-62, 2019.

SANS. Institute InfoSec Reading Room. Out with The Old, In with The New: Replacing Traditional Antivirus, Disponível em: https://www.sans.org/reading-room/whitepapers/analyst/old-new-replacing-traditional-antivirus37377. Acesso em Junho de 2019.