Demonstração experimental de mitigação de ataques em dispositivos *Bluetooth Low Energy*

Ryan M. S. Leal e Iguatemi E. Fonseca

***Resumo*— Este artigo apresenta um estudo experimental do uso de técnicas de criptografia implementadas em dispositivos IoT, em particicular, dispositivos BLE (*Bluetooth Low Energy*). Uma técnica de criptografia, chamada SPECK e que usa cifra de bloco, foi utilizada com sucesso e testada em dispositivos BLE que estão no mercado atualmente, portanto, em cenário real.**

***Palavras-Chave*— Segurança cibernética, Internet das Coisas, Bluetooth Low Energy, criptografia.**

***Abstract*— This paper presents an experimental study of the use of encryption techniques implemented in IoT devices, as BLE devices (*Bluetooth Low Energy*). An encryption technique, called SPECK and which uses block cipher, was successfully used and tested in commercialized BLE devices in the marketplace, therefore, in a real scenario.**

***Keywords*— Cybersecurity, Internet of Things, Bluetooth Low Energy, encryption.**

I. Introdução

A facilidade promovida pela automação e conectividade de dispositivos está cada vez mais presente nas atividades da vida pessoal e nos ambientes industriais. A Internet das Coisas (IoT - *Internet of Things*) torna desnecessária a interferência humana em tarefas que vão desde regular a temperatura de um ambiente até monitorar os sinais vitais de pacientes, todas controladas por dispositivos conectados à internet. Para que esses dispositivos possam operar em conjunto são utilizadas tecnologias de comunicação com foco em eficiência energética, como o *Bluetooth Low Energy* (BLE), que surgiu do Bluetooth e se tornou amplamente utilizado na indústria [1]. Nessa tecnologia, a comunicação entre os dispositivos começa com o envio de pacotes de anúncio contendo suas características e serviços, assim, um outro dispositivo pode visualizá-lo e enviar uma requisição de conexão, começando o processo de pareamento em que ao ser concluído, permite que esses dispositivos formem uma conexão em um modelo semelhante ao Mestre-Escravo. Portanto, é possível que dados dos usuários sejam capturados por atacantes [2].

Esse artigo apresenta uma proposta de uso de técnicas de criptografia leves como forma de melhorar a segurança de dispositivos BLE. Os experimentos realizados em dispositivos BLE reais mostram que é possível proteger a comunicação e dificultar a ação de atacantes.

II. Segurança em Dispositivos BLE

Os dispositivos BLE geram dados sensíveis de usuários e empresas, que são enviados pela internet, gerando aumento no fluxo de dados que trafegam pelas redes e se tornam passíveis a ataques dos mais diversos tipos [3] . Por serem dispositivos de baixo poder energético e computacional, a prioridade no desenvolvimento desse tipo de dispositivo acaba sendo a eficiência energética, assim, a segurança deles e de seus usuários é colocada em risco em detrimento da maior eficiência. Esse cenário se torna mais preocupante ao lembrar de sua utilização em aplicações da área de saúde, que transportam dados sensíveis de diversos pacientes [4].

A. Vulnerabilidades em Dispositivos BLE

A comunicação BLE é feita pelo ar, isso permite que usuários maliciosos utilizando dispositivos específicos possam capturar os pacotes trocados entre as partes e analisá-los usando ferramentas como o Wireshark. Esses ataques são conhecidos como *Sniffing* e caso esses pacotes não estejam criptografados, o atacante tem acesso a todos os dados trocados durante a comunicação, permitindo que ataques mais complexos e perigosos sejam realizados.

Com pacotes significativos obtidos por meio da técnica de *Sniffing*, é possível progredir para um *Replay Attack*, o qual um atacante reproduz os pacotes de forma a se passar pelo usuário legítimo e obter vantagens indevidas.

Outra vulnerabilidade comum é o *Relay Attack*, em que o atacante utiliza dispositivos de retransmissão e um amplificador de sinal para burlar a distância física entre o usuário legítimo e o dispositivo alvo, de forma a parecer que estão próximos o suficiente para gerar a comunicação e fazer uso de seus serviços.

Os ataques de *Jamming* tem como objetivo gerar a negação de serviço em uma conexão IoT legítima, utilizando dispositivos que geram interferências de rádio. Precisam estar fisicamente próximos do alvo para assim impeder que os pacotes sejam enviados e recebidos pelas partes.

O atacante pode ainda personificar ambas as partes da comunicação com os pacotes obtidos na técnica de *Sniffing*, conseguindo observar os endereços de Controle de Acesso à Mídia, possibilitando que torne-se um intermediário na comunicação e controle o tráfego, modificando ou descartando os pacotes que recebeu, sem que os dispositivos alvos percebam, esse tipo de ataque é chamado *Man-in-the-Middle*.

B. Técnicas de Criptografia

Como visto na seção anterior, o ataque de *Sniffing* gera oportunidades para outras vulnerabilidades mais preoucupantes, assim, a segurança dos pacotes se torna um fator crucial para os dispositivos BLE. Uma solução efetiva é o uso de

Ryan M. S. Leal e Iguatemi E. Fonseca, Centro de Informática, Universidade Federal da Paraíba, João Pessoa-PB, e-mails: ryanleal@cc.ci.ufpb.br; iguatemi@ci.ufpb.br. Este trabalho foi parcialmente financiado pelo CNPq.

criptografia, porém, a maioria dos algoritmos mais usados exigem uma alta carga de memória e poder de processamento, consequentemente, exigindo mais consumo de energia. Visando solucionar esse problema, existem algoritmos de Criptografia Leve, que buscam um meio termo entre eficiência e segurança, principalmente para dispositivos IoT. Dentre os principais algoritmos de criptografia simétrica, tem-se o SPECK, o qual possui os melhores resultados em eficiência energética e velocidade, características leves, tornando-se ideal para aplicações de tempo real como os da área de saúde [5].

III. Resultados Experimentais

Como demonstração da utilidade da Criptografia Leve para mitigação de ataques, foi criada uma implementação prática do SPECK, tendo como base sua implementação de referência encontrada em [6]. Além disso, foi realizado um ataque de *Sniffing* para testar na prática sua efetividade. Os detalhes e resultados se encontram nas seções abaixo.

A. Cenários e tecnologias utilizadas

A Figura 1 mostra como o cenário de teste foi montado. A placa WisTrio RAK5010 foi ligada a uma fonte de energia de 12V e então conectada ao J-Link por meio de jumpers para possibilitar o depuração da placa. O J-Link então foi conectado via USB no notebook, o qual executava o J-Link RTT Viewer e exibia na tela a entrada e saída da placa. Além disso, foi utilizado o Ubertooth One, dispositivo que permite a realização do ataque de Sniffing, fazendo a captura do tráfego de dispositivos BLE e que juntamente com o Wireshark, permitiu a análise dos pacotes recebidos e enviados pela placa. No WisTrio RAK5010 foi instalado o sistema operacional Zephyr OS, um sistema de código aberto com suporte para conexões BLE em aplicações de tempo real em dispositivos com baixos recursos em processamento e energia.

Para instalar os códigos de teste na placa foi utilizada a ferramenta West, que possui funcionalidades voltadas para gerenciamento de repositório, construção e atualização de código e depuração de aplicações para Zephyr OS.

B. Resultados

No programa de teste, valores padrões foram inseridos no campo de dados do pacote de anúncio BLE, sendo então criptografados pelo SPECK usando uma chave criptográfica aleatória que era alterada a cada 5 segundos. Assim, mesmo enviando os mesmos valores, os dados dos pacotes não eram iguais. A Figura 2 mostra o valor padrão enviado e o campo de dados depois da criptografia. Enquanto esses pacotes eram enviados em broadcast, um ataque de Sniffing era executado com o uso do Ubertooth One, simulando um atacante em busca dos valores do campo de dados, com a análise dos pacotes usando o Wireshark. Observa-se na Figura 3 que os dados se encontram protegidos pela criptografia, impedindo o atacante de visualizar os valores originais.

IV. Conclusões

Foi possível analisar que com o crescimento no uso de dispositivos BLE em diferentes setores de atividade, a segurança

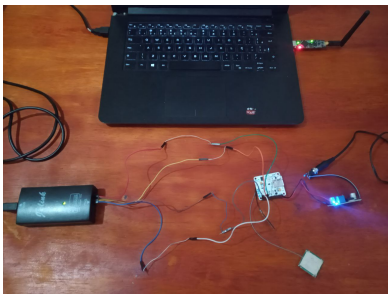

Fig. 1. Cenário de Teste com J-Link, RAK5010 e Ubertooth One.

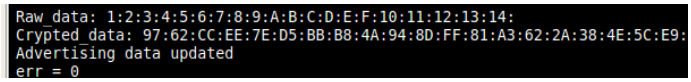

Fig. 2. Captura de Tela do RTT Viewer

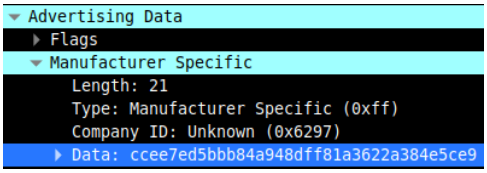

Fig. 3. Captura de Tela do Wireshark

se torna imprescindível em todos os cenários, sendo os algoritmos de Criptografia Leve, como o SPECK, uma ótima solução para mitigar ataques e tornar as aplicações mais seguras, como foi possível observar nos resultados dos testes. Para trabalhos posteriores, a ideia é evoluir a segurança utilizando criptografia assimétrica nas chaves geradas com o SPECK, em uma técnica chamada de Envelope Digital, impedindo que as chaves da criptografia simétrica sejam obtidas pelo atacante durante o processo de comunicação dos dispositivos.

Referências

[1] ABI RESEARCH. Bluetooth low energy market set to triple by 2023, reaching 1.6 billion device shipments. New York, New York, 2 abr. 2019. Disponível em: https://www.abiresearch.com/press/bluetooth-low-energy-market-set-triple-2023-reaching-16-billion-device-shipments/. Acesso em: 2 jun. 2022.

[2] Aellison C. T. Santos, José L Soares Filho, Ávilla Ítalo S Silva, Vivek Nigam, and Iguatemi E. Fonseca. BLE Injection-free Attack: a Novel Attack on Bluetooth Low Energy Devices. *Elsevier Journal of Ambient Intelligence and Humanized Computing*, pages 1–11, 2019.

[3] SILVA, Ávilla I. S.; SANTOS, Aellison C. T.; MONTEIRO, Michael A. F.; GOES, Pablo H. R.; SILVA, Renan M.; NIGAM, Vivek; FONSECA, Iguatemi E. Segurança em Aplicações de Internet das Coisas: Bluetooth Low Energy, casos de uso e vulnerabilidades. In: Livro de minicursos SBRT 2020, Cap. 5, p. 117-142. ISBN 9786587572239. Disponível em: http://editora.ifpb.edu.br/index.php/ifpb/catalog/view/401/209/1168-1. Acesso em: 2 jun. 2022.

[4] Michael Abner, Peter Kok-Yiu Wong, Jack C.P. Cheng, "Battery lifespan enhancement strategies for edge computing-enabled wireless Bluetooth mesh sensor network for structural health monitoring", *Elsevier Automation in Construction*, Vol. 140, 2022.

[5] R. Beaulieu, D. Shors, J. Smith, S. Treatman-Clark, B. Weeks, and L. Wingers. (2013). "The SIMON and SPECK families of lightweight block ciphers"[Online]. Available: http://eprint.iacr.org/2013/404

[6] BEAULIEU, Ray; SHORS, Douglas; SMITH, Jason; TREATMAN-CLARK, Stefan; WEEKS, Bryan; WINGERS, Louis. SIMON and SPECK Implementation Guide. Fort Meade, Maryland, USA: NSA, 15 jan. 2019. Disponível em: https://nsacyber.github.io/simon-speck/implementations/ImplementationGuide1.1.pdf. Acesso em: 2 jun. 2022.