Arranque Seguro de Redes 6LoWPAN para prevenir Ataques Vampiro na Internet das Coisas

Tiago Diogo e Miguel L. Pardal

Instituto Superior Técnico, Av. Rovisco Pais, 1, 1049-001 Lisboa, Portugal,
{tiago.diogo,miguel.pardal}@tecnico.ulisboa.pt

A Internet das Coisas (IdC) pode ser vista como uma teia de dispositivos interligados entre si que vão desde vestuário inteligente (*wearables*) até redes de sensores de gama empresarial. Apesar da enorme variedade e diferenças entre estes dispositivos, algo que todos têm em comum é a sua limitação de recursos. Dada esta variedade de ambientes, uma brecha na segurança destas redes pode implicar uma fuga de informação confidencial ou prover informações sobre as escolhas e paradeiro de um largo número de indivíduos constituindo uma violação de privacidade [1]. Estas são preocupações reais apoiadas por uma gama de ataques que se foca em desativar redes IdC por colocar os seus nós *offline*, conhecidos como ataques "vampiro". Estes ataques focam-se em drenar as baterias – a "vida" – dos dispositivos, atuando ao longo do tempo para desativar completamente a rede [2][3]. Embora existam estratégias de mitigação para estes ataques [2], elas implicam verificações e validações adicionais em cada nó e para cada pacote, colocando um pesado fardo sobre estes nós com recursos muito limitados. Mais ainda, para cada ataque adicional que quiséssemos mitigar, mais validações teriam de ser empregues e mais energia gasta no processo. Para resolver este problema, propomos que um arranque (*bootstrapping*) seguro seja efetuado para cada novo dispositivo da rede onde:

- Não é necessário *hardware* adicional durante a instalação no terreno;
- Não é necessário obter credenciais adicionais após instalação no terreno;
- Não é necessário recorrer a terceiros para gerar ou instalar credenciais;
- Todas as mensagens enviadas na rede são cifradas e autenticadas desde o primeiro momento.

Chamámos à nossa solução *AutoStrap* porque se destina a permitir um processo de *bootstrapping* seguro e eficiente, que tenha o mínimo de interação necessária com os operadores do sistema e não necessite de conhecimento interno do sistema para ser usado. O principio de funcionamento do AutoStrap é a adição de um novo componente na arquitetura da infraestrutura – o *bootstrapper* – que é responsável pela escrita para o dispositivo de todos os identificadores e credenciais de segurança necessários para uma operação que responda aos objetivos e requisitos do sistema, sem necessidade de obter credenciais após o inicio da fase de operação ou de confiar em credenciais criadas por terceiros. As credenciais utilizadas são um identificador único e uma chave de 128 bits usada pelo protocolo Advanced Encryption Standard (AES) [4] no modo Counter with

CBC-MAC (CCM). O uso desta chave e protocolo permite que os pacotes tenham o seu conteúdo cifrado e o seu cabeçalho autenticado com um Message Integrity Code (MIC) também gerado a partir dessa mesma chave. Isto assegura que todos os pacotes que se propagam na rede são confidenciais, íntegros e autênticos. Desta forma, os "vampiros" não serão capazes de se introduzir na topologia, frustrando assim as suas tentativas de conduzir ataques de esgotamento de bateria. Mais ainda, fazemos uso das potencialidades dos protocolos de nível aplicacional para colocar um único cliente na rede. Assim, em vez de termos utilizadores a requisitar novas leituras diretamente aos sensores da rede com recursos limitados, este cliente regista-se junto dos dispositivos existentes e é notificado de cada novo valor ou evento despoletado pelos dispositivos.

Para avaliar o nosso sistema, medimos e documentamos os recursos físicos necessários para suportar os protocolos e estratégias de mitigação escolhidas de forma a entender se são adequados ao *hardware* usado na IdC. Após validar que o sistema era adequado, conduzimos testes de usabilidade ao nosso sistema de gestão de redes para analisar a sua eficiência e facilidade de uso. Analisando os resultados podemos verificar que a introdução destes mecanismos comporta um aumento de 3.02% na utilização de memória *flash* e 1.02% na utilização de memória Random-Access Memory (RAM), permitindo-nos concluir que apenas uma pequena fração de memória adicional é usada. Em relação aos consumos energéticos, a nossa solução mantém um baixo consumo por empregar um protocolo de Radio Duty Cycling (RDC) capaz de manter o rádio, a componente que mais consome energia no *hardware*, desligada durante cerca de 99% do tempo de utilização [5]. O processo de *bootstrapping* em si pode ser conduzido num tempo total de 12 segundos por dispositivo. Desta forma podemos concluir que a nossa solução é prática e adequada aos cenários de utilização IdC.

Como trabalho futuro, salientamos a necessidade de proteção da memória dos dispositivos para impedir o roubo de credenciais de segurança e consequente clonagem dos dispositivos. Deixamos como sugestão o uso de circuitos integrados com mecanismos de impedimento de leitura ou o bloqueio via software de certas regiões de memória dos dispositivos onde residem as chaves de rede.

Referências

1. Ukil, A., Bandyopadhyay, S., Pal, A.: Privacy for IoT: Involuntary privacy enablement for smart energy systems. 2015 IEEE International Conference on Communications (ICC) (2015) 536–541
2. Vasserman, E.Y., Hopper, N.: Vampire attacks: Draining life from wireless ad Hoc sensor networks. IEEE Transactions on Mobile Computing **12**(2) (2013) 318–332
3. Pongle, P., Chavan, G.: A survey: Attacks on RPL and 6LoWPAN in IoT. 2015 International Conference on Pervasive Computing (ICPC) **00**(c) (2015) 1–6
4. Fips, N.: 197: Announcing the advanced encryption standard (AES). ... Technology Laboratory, National Institute of Standards ... **2009** (2001) 8–12
5. Dunkels, A.: The ContikiMAC Radio Duty Cycling Protocol. SICS Technical Report T2011:13 , ISSN 1100-3154 (2011) 1–11