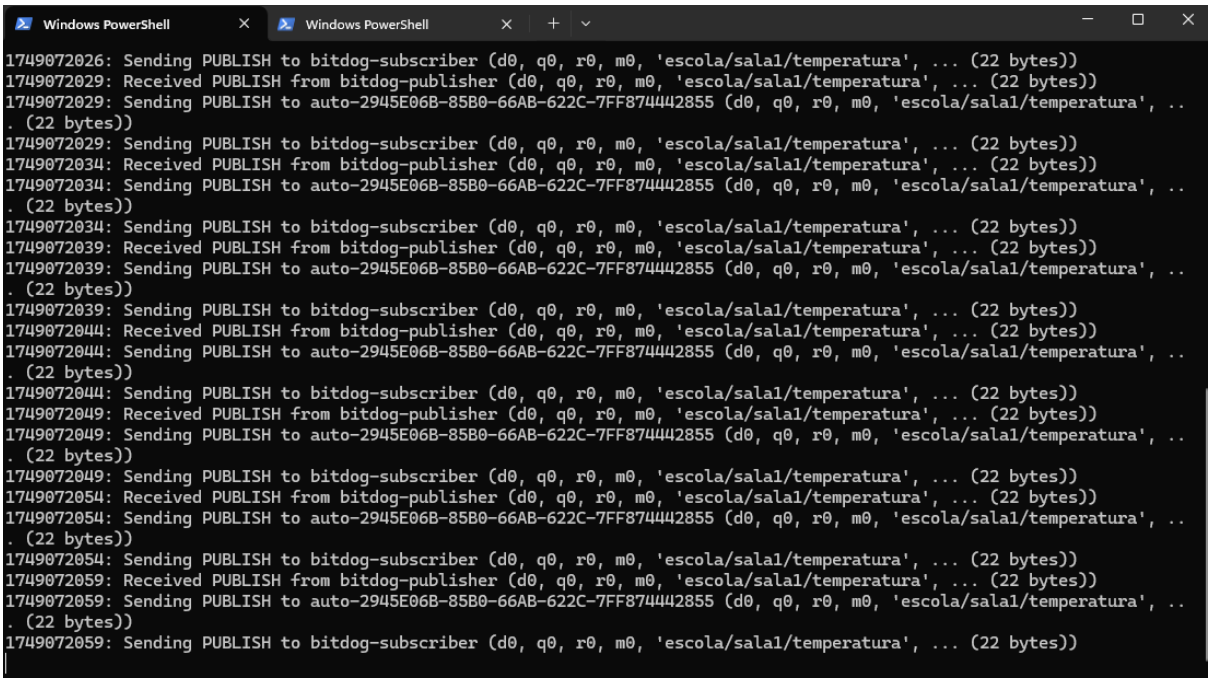
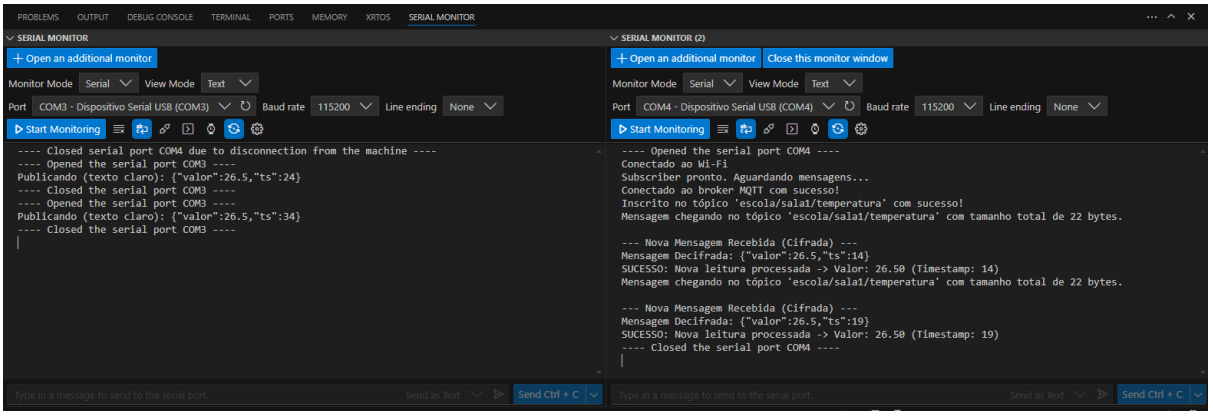
Antonio Crepaldi - Bianca Andrade





Ao levar um projeto como o nosso laboratório com a BitDogLab de um protótipo para uma aplicação real, como uma rede de sensores em uma escola, nosso foco precisa mudar. As técnicas que usamos para aprender os conceitos de segurança são um ótimo ponto de partida, mas em uma escala maior, elas revelam suas limitações.

A nossa abordagem inicial, por exemplo, usou uma senha única e uma criptografia simples de XOR para todos os dispositivos. Para fins de aprendizado, isso funciona bem, mas em uma rede com dezenas de placas, essa estratégia se torna um grande risco. É como dar a mesma chave de armário para todos os alunos da escola; se uma chave for perdida ou copiada, a segurança de todos os armários é comprometida. Da mesma forma, se a senha ou a chave de criptografia do nosso sistema vazar, um invasor poderia não só ler toda a

comunicação, como também se passar por qualquer sensor. Gerenciar o acesso ou remover um dispositivo defeituoso se tornaria uma tarefa impossível.

A solução para um ambiente real é adotar o mesmo padrão de segurança que protege a internet, o TLS (Transport Layer Security), através do protocolo MQTTS. Ele resolve esses dois problemas de uma só vez: em vez da fraca cifra XOR, ele aplica uma criptografia robusta como o AES, e no lugar da senha compartilhada, ele permite que cada BitDogLab tenha seu próprio Certificado Digital. Esse certificado funciona como uma identidade digital única e segura, garantindo que apenas dispositivos autorizados possam se conectar e que cada comunicação seja privada e inviolável.

Enquanto o TLS cuida da confidencialidade e da autenticação, a proteção contra ataques de replay, que implementamos com timestamps, continua sendo muito relevante. O conceito de verificar se uma mensagem já foi recebida antes é perfeitamente escalável, mas nossa implementação precisa de alguns ajustes para o mundo real.

No laboratório, usamos o "tempo desde a inicialização" como nosso relógio, o que não é confiável em um sistema distribuído. Para que a comparação de timestamps funcione, todos os dispositivos precisam "falar a mesma hora". A solução padrão para isso é usar o NTP (Network Time Protocol), que permite que cada BitDogLab sincronize seu relógio com a hora certa pela internet. Além disso, nosso receptor guardava o último timestamp na memória RAM, que é volátil. Em uma aplicação real, esse valor precisaria ser salvo em um local permanente, como um banco de dados, para que o sistema não ficasse vulnerável após uma reinicialização.

No final, a transição para um sistema escalável não se trata de reinventar a roda, mas de integrar de forma inteligente as ferramentas padrão da indústria, como o TLS, e aprimorar as boas lógicas que já desenvolvemos, como a validação de timestamps, para que operem de forma confiável em um ambiente real e dinâmico.