【問 6】 本問は A か B のいずれかひとつに回答ください。

【B】 作りたい作品の提案

(1) あなたが SecHack365 で作ってみたい作品について、いまの時点で想像できる範囲で説明してください。

セキュリティ機能をもたせた Zynq 上で動作する Message Queue Telemetry Transport Protocol (MQTT) プロトコル・スタックを持つ組み込み OS の開発

FPGA と ARM プロセッサが一つにまとまっている Zynq チップ上で動作する組み込みOSを開発したいと考えています。

Zynq で組み込み OS を使用する場合はオープンソースソフトウェアの FreeRTOS というものを使うことが一般的ですが、私はよりミニマルな OS を開発したいと考えています。また、スマートホームなどに用いられている MQTT というものを使えるようにすることで、研究などにおいてセンサなどから取得したデータを MQTT を介して通信することによりシンプルにメトリクスデータを取得できるのではないかと考えています。

将来的には RISC-V プロセッサを自作し、そのプロセッサで自作 OS が実行できるようにしたいとも考えており、実現できた場合はZynq以外のCPU内蔵でないFPGAチップでもスタンドアロンなシステムを動かすことができます。

(2) その作品とサイバーセキュリティの関係について説明してください。

Zynq は、Linux を用いたスタンドアロンシステムとして用いることが一般的です。しかし、Linuxを使用する場合、どうしてもアタックサーフェスが大きくなると考えられます。そこでアタックサーフェスが小さい組み込みOSを使うことが良いのではないかと考えています。

MQTT は TCP/IP プロトコル上で用いられるプロトコルであるため、TLSなどを用いない通信を行なってしまうと、通信が傍受されてしまう可能性があります。そのため今回開発するOSではlight-weight IP stack (lwIP)のTLSライブラリを用いて、セキュアな通信上でデータを送受信できるようにしたいと考えています。また MQTT の通信自体にも暗号化をしたいと考えており、プロトコルを実装する際に、Basic認証や、パスワードフィールドを用いた Bearer 認証を実装したいと考えています。

OS本体についても、ブートローダ上でOSのハッシュを計算し、改ざんされた悪意のあるOSを読み込まないようにするセキュアブート的な機能を実装したいと考えています。さらに On The Air (OTA) アップデート機能も実装したいです。これはIoT機器をネットワークを用いて自動でアップデートする機能であり、この機能を実装することで脆弱性が見つかった場合にすぐにパッチを当てることができるようになります。また、 VPN アプリケーションである wireguard

を OS に導入したく、この wireguard についての実装はもうすでに GitHub に公開されているものが存在するため、その実装を OS に取り込みたいと考えています。