指紋認証モジュールと欺瞞する

学習駆動コース 今岡ゼミ 伊藤 秀敏

1. 指紋認証モジュール

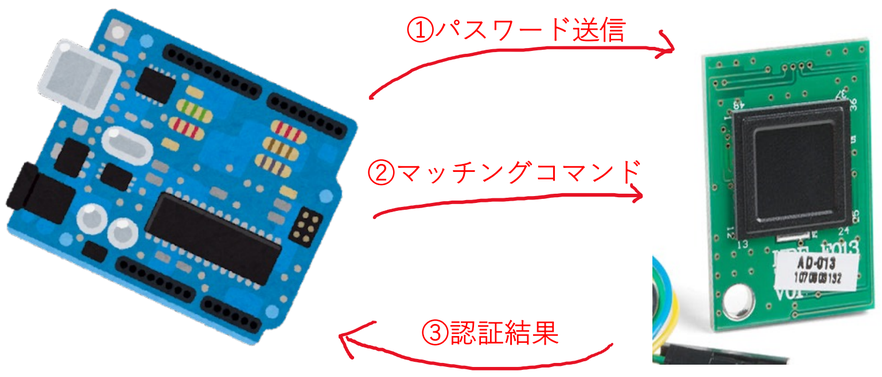
今回対象とする指紋認証モジュールは、Arduinoのようなマイコンと UART,I2Cといったシリアル通信を使って通信する。モジュール上に搭載されたICに指紋登録・照合操作といった機能があり、通信を経由してこれらの機能をマイコンから操作することができる。

指紋認証のために事前に登録するデータはモジュール上に保存され、認証時にモジュール上のセンサから読み取ったデータと事前に保存したデータの照合作業を行い、照合結果をシリアル通信でマイコンへ送信する。

このような指紋認証モジュールはネット上で複数売られているが、データシートを読む限り使い方はどれも同じである。

2. 一般的な(？)使い方

この指紋認証モジュールの使用例として、事前に登録した指紋データをもとにセンサ上の指紋を照合するまでの流れを紹介する。

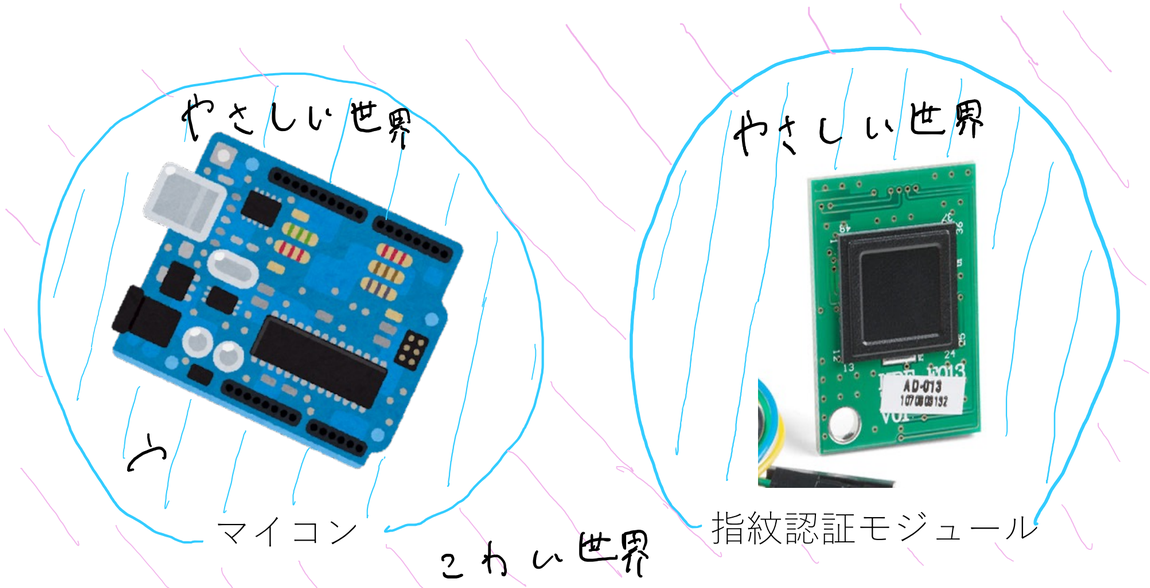


①マイコンからモジュールに32bitのパスワードを送信し、モジュールのロックを解除する。
②マイコンからモジュールへセンサ上の指紋を読み取り、事前に登録したデータとマッチングするようにコマンドを送る。
③モジュールはマッチングの結果を返す。(認証成功or失敗)

＊①の動作を一度行うと、電源を喪失しない限り②③の動作は繰り返し行える。

3. 前提

今回、マイコンと指紋認証モジュール間の通信路は安全ではなく、通信を読み取られたり書き換えられる危険性があると仮定する。



4. 脅威

マイコンと指紋認証モジュールの間に悪意のあるマイコンが入りこみ、モジュールがマイコンへ送るマッチング結果の通信を書き換えることで、指紋認証に成功していないのにも関わらず、指紋認証が成功したように見せかけることができてしまう脅威がある。

マイコンのリクエストに対してモジュールは指紋のマッチを見つけられなかったため、”認証失敗”の結果を返した。しかしながら、悪意のある第三者が結果の通信を書き換え、”認証成功”としてもマイコン側はこの通信がモジュールからのものであるかを確認する手段がないため、認証が成功したと誤認してしまう。

対策: 以下の対策で攻撃を無力化/難化できると考えられる

- モジュールからマイコンへの通信に毎回その通信がモジュールからのものであることをマイコンが認証できる仕組みを取り込む。
- マイコン-モジュール間の通信路を4層基板の内側のレイヤーを通すなどによって、マイコン-モジュール間の通信路に攻撃するには機器全体を破壊しないとできないようにする。

5. まとめ・今後の展望

まとめと感想

指紋認証モジュールにおける脅威をデバイスの検証を行いながら示した。だが、同時に脅威を示す上で前提条件を設定する難しさとその条件をクリアする現実性の点で厳しさを感じた。ただ、１年間でUARTについての理解が進んだことは有益だったと思う。

今後の展望

モジュールからマイコンへの通信を認証する仕組みについて具体的に考えていきたい。また、実際に2つのマイコン間の通信として実装し、TLSのような既存のシステムとの計算速度の比較などを示していきたい。

謝辞: 今岡亭一門の皆さん、コメントをくれたトレーナー・トレーニー皆さんに感謝します。大変お世話になりました。