SecHack365

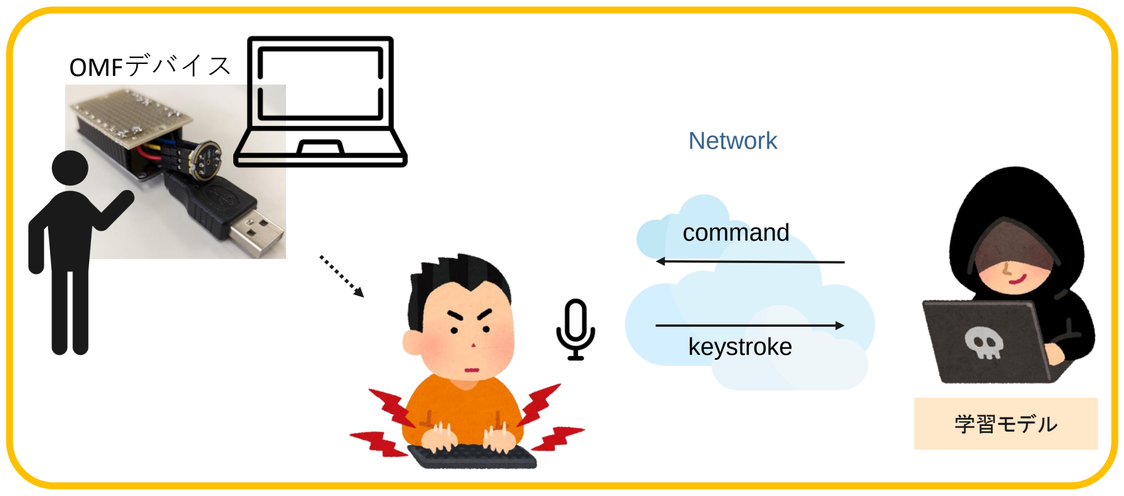
OMF (Oh My Finger)： 遠距離キーボード入力推定

～ 無線マイクによる打鍵音取得で遠距離化を実現 ～

学習駆動コース 今岡ゼミ 首浦大夢

提案する攻撃フロー

① OMFデバイスを被害者付近の
USB Type A or micro Bに挿入し、電力供給
② OMFデバイスがサーバ立ち上げ
③ 攻撃者が録音コマンドを送信
④ 打鍵音を攻撃者PCで取得
⑤ 推定モデルに与える
⑥ 推定結果を得る



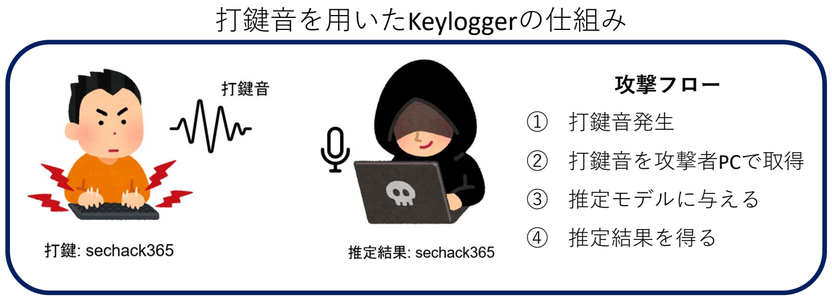
攻撃は難しい！ 脅威レベルを調査・確認するためにデバイスを開発！

- BadUSBによる被害を周知する
- 打鍵音により情報が漏洩する可能性を周知する

以上の目的を達成するためにデバイスを開発し、
脅威レベルを調査・確認、説明する

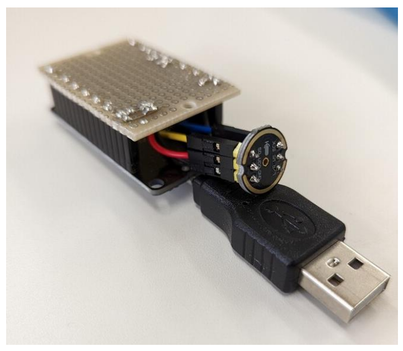
遠距離になっても 打鍵音で攻撃者と被害者を ダイレクトに繋ぐよ♡

打鍵音を用いたKeyloggerの仕組み



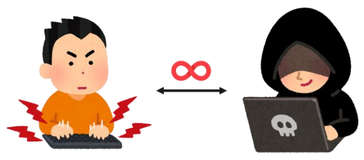
既存手法の弱点

ボイスチャットアプリによる**ノイズ抑制**
攻撃者と被害者の**距離**
内蔵マイクの**性能限界**



OMFデバイスを作成！

ESP32 + MEMSマイクで構成
・ESP32 MEMS間: I2S通信
・OMF 攻撃者間: Socket通信



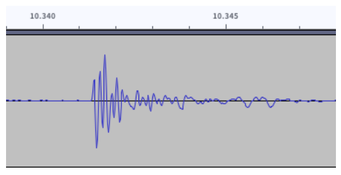
ネットワークに繋がったマイクを**遠隔操作**
無線マイクにより攻撃者と被害者を**無限遠**に

ECMマイクとMEMSマイクの違い

MEMSメリット
① 小型(薄い)
② 省電力
③ ノイズ軽減
④ 複数個の組み合わせによる
指向性強化ができる
↑
1つだと無指向性(まんべんなく音圧を受ける)

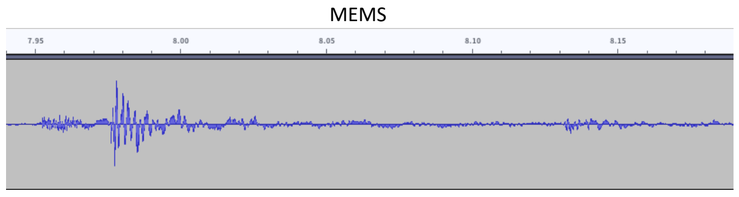
実物(INMP441)と1円玉との比較

ECM



概形は似ているが同一な波形とは言えない
① ECMと比べて**滑らかな波形でない**
② ECMと比べて時間で**引き伸ばしたような波形**

MEMS



各マイクで打鍵音を取った波形

性能評価1:　距離による音圧(dB)低下の調査

	0cm	35cm	55cm	75cm	95cm	115cm	135cm	部屋の端
ECM	-15	-20	-24	-27	-27	-29	-29	-30
MEMS	2	-10	-12	-18	-20	-23	-23	-27
re_ECM	-13	-15	-24	-24	-27	-29	-29	-30
re_MEMS	-15	-17	-22	-26	-26	-26	-26	-30

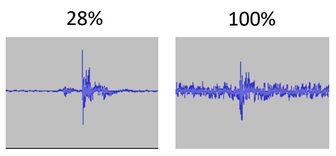
- Audacityによる計測
- reは音源方向に対してマイクを逆方向にしている状態を指す
- MEMSは**ECMより高い音圧**で打鍵音を取っていることが分かる
- reにした場合にECMとMEMSの優劣が少し変わることから
無指向性による特徴を確認できる？

性能評価2:　ファンの回転率によるノイズ(dB)調査

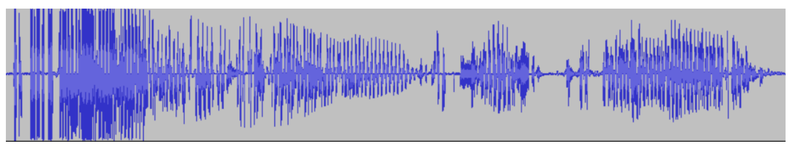
	28%	50%	60%	70%	80%	90%	100%
ECM	-33	-30	-30	-30	-27	-27	-24
MEMS	-24	-22	-21	-18	-12	-12	-6

- ECMはPC内蔵なのに音圧の変化無し
- MEMSはファンの音をかなり得る
- MEMSはファンにより**波形が崩れる**

MEMSでノイズあり打鍵音を取った波形



性能評価3:　MEMSでの声録音結果



- 振幅の幅を設定しないことにより**音割れを発生しやすく**する
- 打鍵音は0cmでも音割れしないことから音割れした音声は打鍵音でないと言える
- ECMでも閾値を決めて編集すればよいが、今回は**音割れの指標で簡単に編集可能**

推定方法

学習データには打鍵音の**push peak**と**release peak**を用いる
MEMSではpushとreleaseの時間幅が大きいことから既存手法よりも探索するpeak位置の幅を離す必要がある
機械学習はロジスティック回帰により行われる
※この手法は既存手法であるKeyboard Acoustic Emanationsと同じ

ECM、 MEMSで各キー(a-z0-9, enter, shift等)200回程度のサンプルを集める

コードの流れは次のようになる
① 学習データのpeakを全列挙
② pushとreleaseのpeakを抽出
③ パディング処理
④ 学習(ロジスティック回帰)
⑤ 推定

ローパスフィルタ、ノイズのみの学習データを使用することで
微小なノイズへの耐久性を上げる

結果

(推定成功した文字数 / 推定データの文字数) × 100 [%]

	ECMで学習	MEMSで学習
ECMの推定	60%	0%
MEMSの推定	0%	60%

※推定結果Top5に存在する場合、推定成功

例(正答: t)
```
-- 3: 0.278
-- #space: 0.105
-- p: 0.075
-- t: 0.0719
-- 0: 0.0639
Actual: t
```

確率的に一番正しいと判定されたのは
3だがTop5にtが存在するため推定成功

OMFデバイスの使用結果

問題なく打鍵音を取得できたもののいくつかの不具合を確認している

1. IPアドレスを得れているが、疎通不可能
2. Wi-Fiに接続不可能

これらはデバイスの**電源を入れる/切るのスパンが早いと発生する**
また同一でないネットワークでの使用は現段階ではできない

対策

以下に示す対策により攻撃可能な前提が成り立たなくなるため無力化ができる

1. 知らないデバイスは安易にPCに接続しない
2. 打鍵音が小さいキーボードを用いる

まとめと展望

まとめ

SecHack365を通してMEMSの優位性の検証やデバイスの検証を行うことができた。
まだ未完成ではあるものの提案手法の実現ができ、前提条件の難しさ・脅威レベルを理解することができた。

展望

指向性を強化するためのビームフォーミング(MEMSの複数使用)がまだできていない。
そのため、耐ノイズの観点が未評価である。今後はデバイス自体の強化と共に前提条件の難易度低下を図る。USBメモリとして使えたり、小型化してその他のUSBポートを利用する機器に組み込むことなどが策である。
また、今後は知名度のあるカンファレンス等で発表・その場でのデモを行うことで当初の目的である脅威の周知を行いたいと考えている。

謝辞: 今岡師匠、灰原さん・今岡亭一門、僕に関わってくれた全ての人類へ感謝します