SecHack365

ペースメーカーを用いた安全な遠隔治療に向けたログ分析手法の提案

研究駆動コース　辻 有紗

1 課題

・分析時のログと分析システムの流出の危険性
分析機関のローカルで暗号化されていないログと推論システムを用いて分析を行っているため、攻撃により情報が流出する危険性がある

・分析機関によるログの閲覧
推論システムで平文のログを使用するため、分析機関によるログの閲覧が避けられない

-> 分析処理を暗号化することで、処理で用いられるログ・推論システムなどの機微なデータを第三者や分析機関から保護する

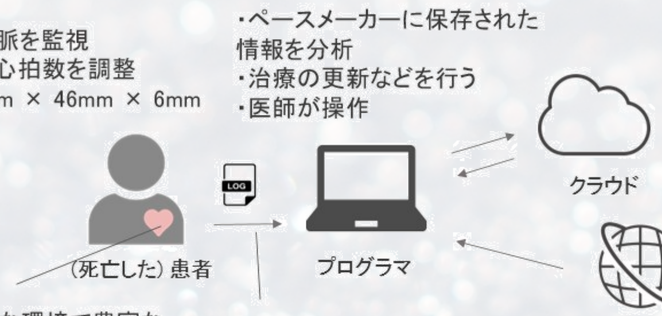
・攻撃の分析を死後にしか行えない
現在は患者の死後に病院が分析機関にログを送信しており、分析機関で処理する流れが自動化されていない

-> クラウドを用いたログ分析フレームワークを用いて、患者の生存中に安全に体調の異常や攻撃を検知する

2 ペースメーカーの通信・脆弱性

・心臓の不整脈を監視
・電気刺激で心拍数を調整
・サイズ：49mm × 46mm × 6mm
・寿命：10年

・ペースメーカーに保存された情報を分析
・治療の更新などを行う
・医師が操作



① 低スペックな環境で豊富なログをとる
② ペースメーカーの無線通信機能・認証機能を悪用したログの書き換え

無線ネットワーク
MICS: ペースメーカーとプログラマ用の通信規格、2mまで
③ 暗号化されていない通信の盗聴によるログの書き換え
④ 通信のスクランブルによるログの破壊

ソフトウェア配信ネットワーク

3 (ログの使用例) フォレンジック調査

患者の死後に，ペースメーカーに保存されているログを分析し死因を特定する．ペースメーカーで記録されたログと，過去の医療的な観察から作成されたライブラリから構成された推論システム，攻撃に関するライブラリから構成された推論システムを用いて，医療シナリオと攻撃シナリオを構築する．2つの推論結果の相関をとり，患者の死因を証明する．

ログの内容
① 患者の身体情報に関するログ
Ex) 脈拍数、過去の病歴
② セキュリティに関するログ
Ex) 通信セッションの確立と終了、時計の更新、治療法の更新、電気ショック・ファームウェアの更新記録、通信トラフィックの記録

4 完全準同型暗号を活用したクラウド上のログ分析フレームワーク

分析機関が保有する死因推論システムをTFHEで暗号化し、クラウドに保存する．プログラマではペースメーカーから送信されたログをTFHEで暗号化し，クラウドの分析システムに送信する．クラウド上で暗号化された状態で分析を行い，結果を病院に送信する．
病院で結果の復号を行う．

(a)
プログラマ- 分析機関- クラウド- 病院間の鍵の送信
a-1. 病院でTFHEの秘密鍵、ゲート鍵を作成
a-2. 病院からプログラマ、分析機関へ秘密鍵を送信
a-3. 病院からクラウドへゲート鍵を送信

(b) クラウド-分析機関間
b-1. 分析期間で秘密鍵を用いて推論システムを暗号化
b-2. 分析機関からクラウドへ暗号化された推論システムを送信

(c) クラウド- プログラマ間
c-1. プログラマで秘密鍵を持ちいてログを暗号化
c-2. プログラマからクラウドへ暗号化されたログを送信

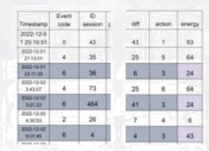
(d) クラウド- 病院間
d-1. クラウドで暗号化されたログと推論システムを用いて分析
d-2. 分析結果を病院に送信
d-3. 病院では受診した結果を秘密鍵で復号

5 評価

1. 暗号化されている状態で正しく分析できる

ex) プログラマの更新(eventcode 6)で消費したエネルギーの総和を計算する

① ペースメーカーからプログラマにログを送信



暗号化されたログについて eventcode 6 を確認し 24+24+43 を計算

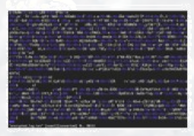
② (プログラマで)TFHEの秘密鍵でログを暗号化

バイナリファイル
ファイルサイズ2000倍 程度

③ クラウド上の暗号化された推論システムを用いて、ログを分析

分析システム内の暗号化された暗号文同士の加算を行う関数を使用

④ 暗号化されている分析結果を復号



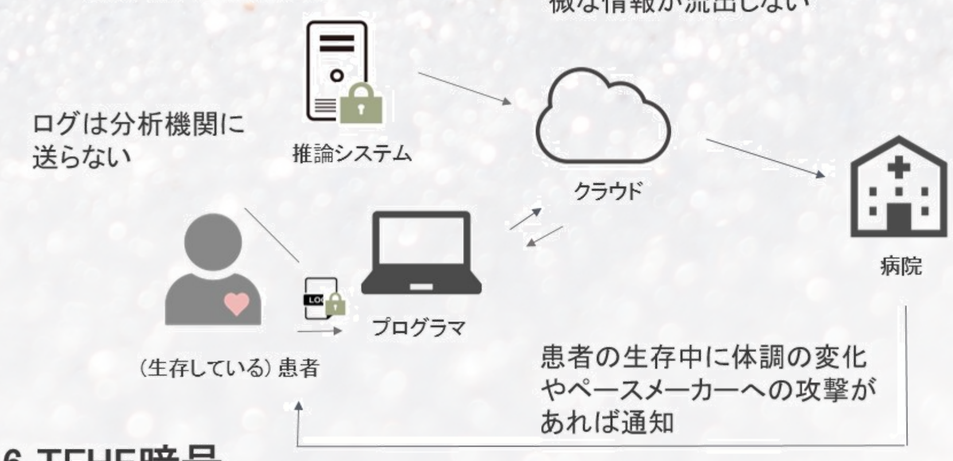
秘密鍵で復号 → 91

Encrypt (24) ⊕ Encrypt (24) ⊕ Encrypt (43) = Encrypt (91)

2. ログ・推論システムの流出を防ぎ，ログ分析を自動化する

ローカルで分析しないため，暗号化されている分析システムを復号する必要はない

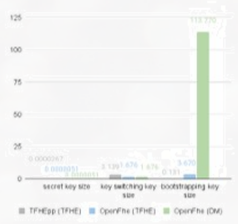
暗号化されたまま分析されるため，攻撃されても機微な情報が流出しない



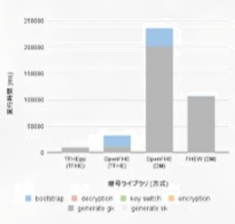
6 TFHE暗号

・利点
- 暗号化した状態で任意回加算乗算が可能な格子暗号
- 1bitごとに論理回路(AND, OR, NANDなど)で評価し、ゲート毎にbootstrapを行うことで高速処理が可能
- LUT(LookupTable)を用いて非線形関数の評価が可能
- 実数の評価が可能

・課題点
- 空間計算量が大きい



TFHE暗号の鍵サイズ



TFHE暗号のBootstrapの速度

7 今後の課題

- 推論システムの暗号化
- フレームワークの自動化
- 空間計算量が小さい他の暗号方式を検討
- 攻撃者と医者を考慮したログで記録する内容を検討

8 学んだこと

伝わりやすい言葉に言い換えること，黙々と進めること，情報の技術でできることが沢山あること

NICT National Institute of Information and Communications Technology