SecHack365

KAMPPHER

Kicking and **A**larming **M**odule for **P**reventing I/O Storage **P**eripheral by **H**ardware from **E**vil **R**ewriting

ケンプファー

ハードウェアによる不正なデータ書き換えの阻止・警報モジュール

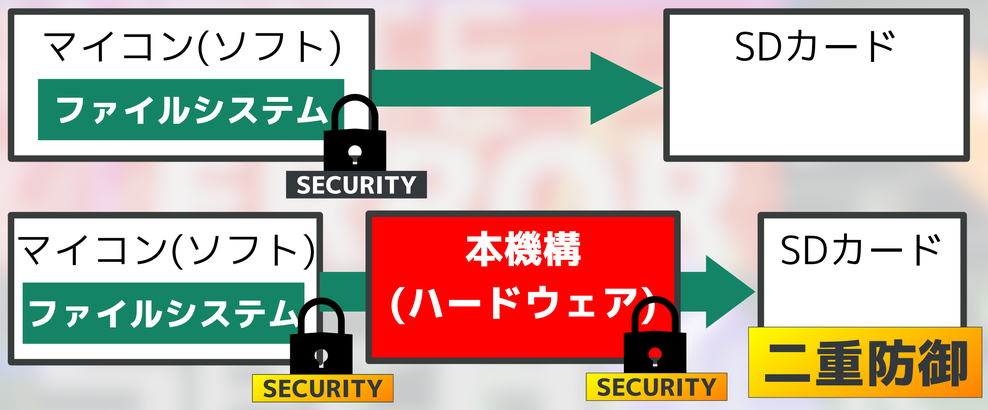
学習駆動コース フィジカルゼミ 鈴木 豪

協力・助言いただいた今岡 道博トレーナー, SecHack365/フィジカルゼミの皆さん, 家族, 松江工業高等専門学校 情報工学科/島根大学 総合理工 知能情報デザイン学科の友人, 先生
ありがとうございました.

背景

IoTのプログラム(Firmware)を書き換える 不正アクセス・不正プログラムへの懸念

「ソフトウェアだけでなく，ハードウェアでもデータの書き込みを検査することでセキュリティを高める（二重防御）」という目標のもと，本セキュリティ機構を作成しました.



さらに，管理する領域数が減るため，ファイルシステムに比べて，人為的ミスも減らせると考えています.

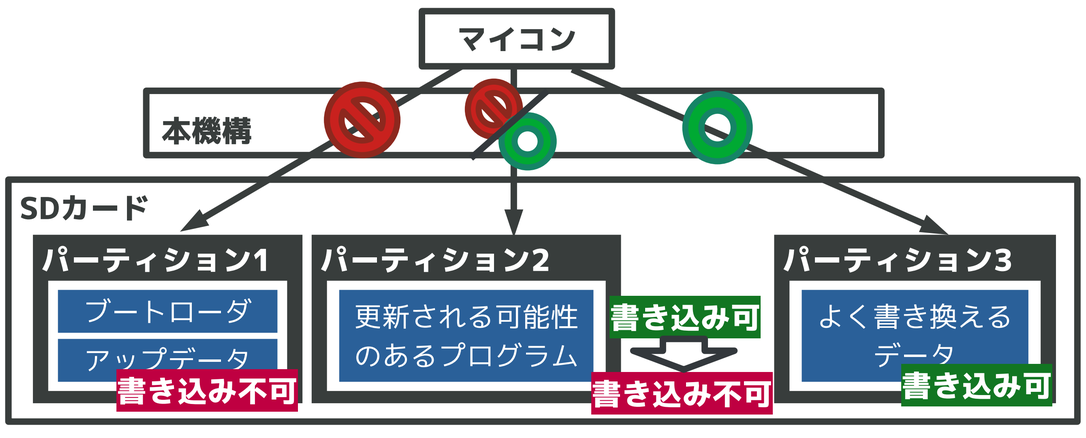
目指す利点

- **既存の装置がそのまま使える**
- **速度低下が少ない**
- **低コスト**
- **誤検知が少ない**

概要

主:ストレージ-マイコン間に挟まるセキュリティ機構の開発

マイコン-SDカード間のSPIの信号を監視する装置を作ります．この装置は書き込み不可な領域に書き込んだ場合に信号を遮断し，マイコンをリセットします.



開発者は書き込みの可能・不可能の領域をパーティションによって分割し，書き込みの可否をデジタル制御線によって入力します.

ブートローダ・アップデータといった絶対に書き換えないプログラム

HIGH（=書き込み不可）を**ハードコード**で入力します.
ハードコードだからリモートからハッキングすることはできないと考えられます.

更新される可能性のあるプログラム

マイコンのピンとつなぎます．マイコンはアップデート完了前まではLOW（＝書き込み可）を入力し，アップデート完了後はHIGH（＝書き込み不可）を入力します.

よく書き換えるデータ

GND（＝書き込み可）をハードコードで入力します.
書き換えられたくないデータを書き込み不可能パーティションに保存しておくことで改ざんを防ぎます.

副:展示向けシステムの開発と本機構の応用例の例示

視覚化：KAMPPHER Inspector

展示向けにKAMPPHERの動きを視覚化してみました.

不正書き込みの通知機能の作成：KAMPPHER Notice

マイコンのI/OライブラリをKAMPPHERに対応するように修正します.
マイコンが不正領域に書き込んだ場合, KAMPPHERはエラーレスポンスを返します.
その情報を用いて，マイコンはWebサーバにエラー情報を送信します.

仕組み(SD card SPI Mode)

起動時

マイコンがMBR（マスターブートレコード）を読み込むときに，データを監視して，SDカードのパーティション構成を把握します.

不正アクセスが無いとき（正常に動作しているとき）

SPIの信号を素通しします.

不正な書き込みがあったとき

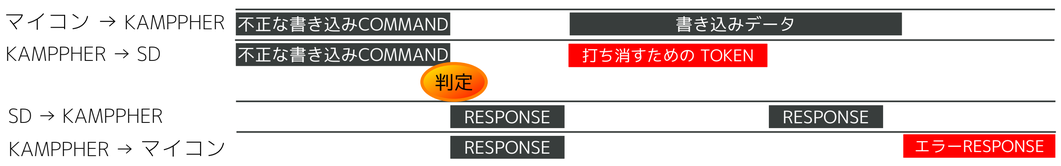
パーティション構成・パーティションの書き込みの不可と照らし合わせて，書き込み禁止であった場合にコマンドを阻止します.

Single Block Write/Multi Block Write

書き込み禁止領域への書き込みを発見した場合にすぐに打ち消すための信号（STOP TRANS TOKEN）を送信します．また，Single Block Writeでも打消しが効くことは，MMC（Multi Media Card，SPIモードの時はSDカードと互換性がある）の規格書の状態遷移図から分ります．バッファリングしないため速度低下は起きません.

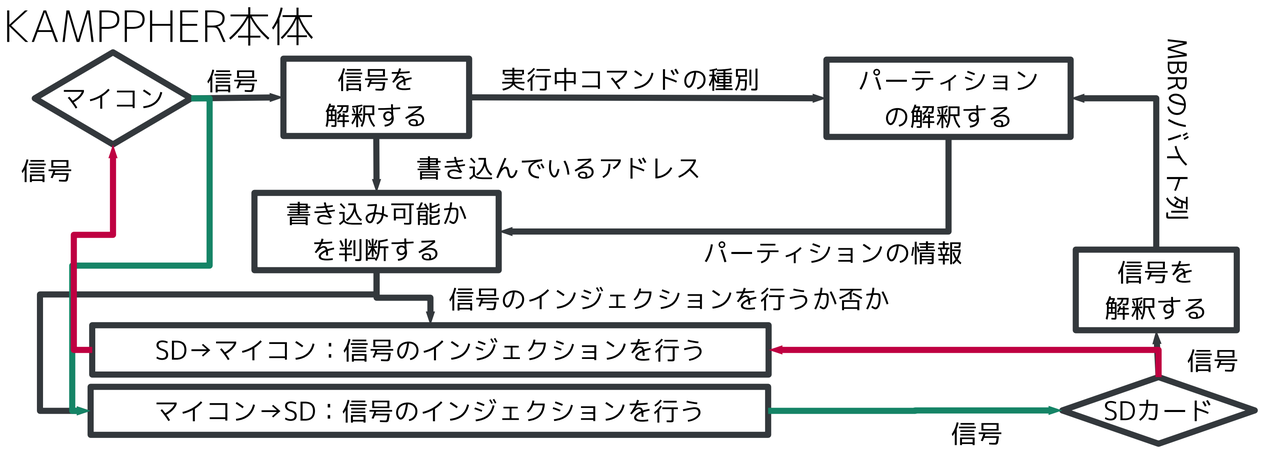
Set Erase Block Count

放置しておくと，Writeコマンドが発行された時点で指定アドレスのデータは不定状態になってデータが失われてしまうので，引数が0になるように信号を改ざんします．この時の速度低下はSDカードの性能によります.
現段階では実装していませんが，これによる性能低下が大きい場合は，緩和策も考えています.

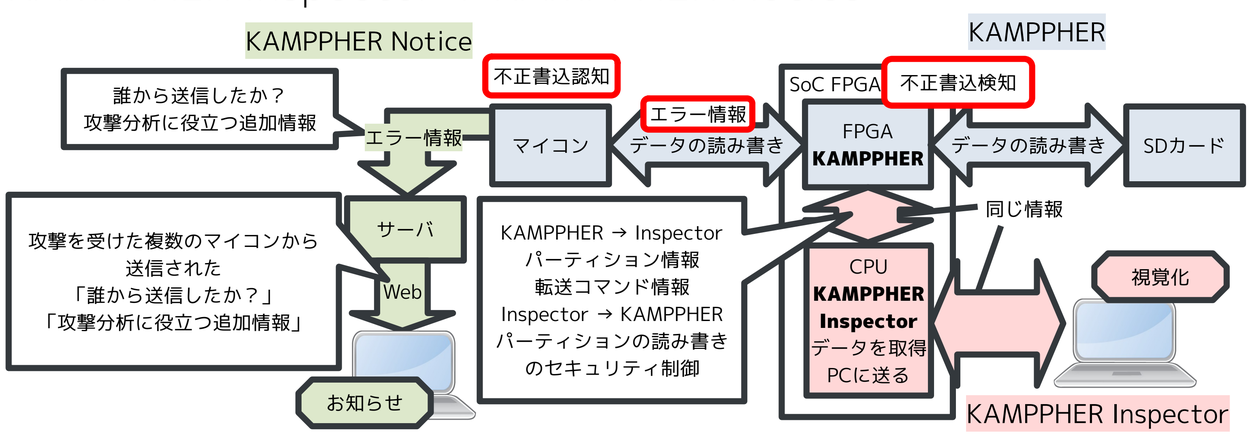


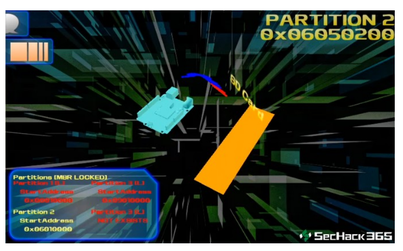
アーキテクチャ

KAMPPHER本体

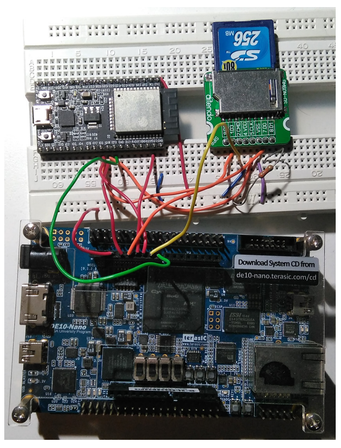


KAMPPHER Inspector + KAMPPHER Notice





Arduino UNO Model(CC-BY) ピボーログ https://sites.google.com/site/bknobiboroku/blender/arduino_uno_board



国立研究開発法人 情報通信研究機構

FPGA	Intel(ALTERA) Cyclone V SoC(Terasic DE10-Nano)
HDL	Verilog(Quartus 18.1/ModelSIM), Chisel 3.2
SDカード	Transcend 256MB SD Card(v2)

マイコン	ESP32-WROOM-32
OS/ライブラリ	Arduino + SdFat