600 Jahre Universität Rostock

Traditio et Innovatio

Bachelorarbeit zum Thema

Sicherheitsanalyse durch Entwicklung eines Rogue Device zur Echtzeitmanipulation maritimer Steuerungssysteme

Studiengang:	Informatik
Vorgelegt von:	Jakob Engelbert Tomahogh
Matrikelnummer:	221201101
Bearbeitungszeitraum:	15. November 2024 – 04. April 2025
Erstgutachter:	M. Sc. Marvin Davieds
Zweitgutachter:	Prof. Dr. rer. nat. Clemens H. Cap

Lehrstuhl für Informations- und Kommunikationsdienste
Institut für Informatik
Fakultät für Informatik und Elektrotechnik
Universität Rostock

Gedruckt auf säurefreiem und elementar-chlorfrei gebleichtem Papier.

Stand:: 22. November 2024

Inhalt

Kurzzusammenfassung

Im traditionellen Sinne bezieht sich der Begriff Typografie auf die Gestaltung von Druckwerken mit beweglichen Lettern (Typen). Anfänglich fand dies insbesondere im Bleisatz bzw. dem Satz mit Holzlettern statt.

In der Medientheorie steht Typografie für gedruckte Schrift in Abgrenzung zu Handschrift (Chirografie) und elektronischen sowie nicht literalen Texten.

Heute bezeichnet Typografie meist den medienunabhängigen Gestaltungsprozess, der mittels Schrift, Bildern, Linien, Flächen und Leerräumen alle Arten von Kommunikationsmedien gestaltet. Typografie ist in Abgrenzung zu Kalligrafie, Schreiben oder Schriftentwurf das Gestalten mit vorgefundenem Material.

Abstract

In the traditional sense, the term typography refers to the design of printed works with movable letters (types). Initially, this was done in lead typesetting or wood typesetting.

In media theory, typography stands for printed type in contrast to handwriting (chirography) and electronic as well as non-literal texts.

Today, typography usually refers to the media-independent design process that uses type, images, lines, surfaces and empty spaces to create all kinds of communication media. In contrast to calligraphy, writing or type design, typography is the design with found material.

Kapitel 1

Einleitung

In diesem Kapitel

1.1 Motivation

Warum ist das Thema wichtig? Warum sollte sich jemand damit beschäftigen? Was ist das Ziel der Arbeit?

1. CanBus ist weit verbreitet in Fahrzeugen, noch nicht ausreichend in Schiffen auf Sicherheit bedacht.
2. In großen Schiffen kann es durchaus vorkommen, dass unbemerkt Personen physischen Zugriff auf Teile des Schiffes haben, die für die Steuerung relevant sind.

1.2 Ziel der Arbeit

1. Entwicklung eines Rogue Device, das in der Lage ist, die Kommunikation auf einem CanBus zu manipulieren.
2. Sicherheitsanalyse der Auswirkungen auf die Steuerung eines Schiffes.
3. Dadurch soll aufgezeigt werden, wie wichtig es ist, die Kommunikation auf einem CanBus zu schützen und Aufmerksamkeit auf die Sicherheit von Schiffen zu lenken.

Kapitel 2

Grundlagen

In diesem Kapitel

2.1 CanBus

Wie wird ein CanBus verdrahtet und wie kommunizieren die Geräte? Was ist ein CanBus:

- Technologie für serielle Netzwerke
- 1983 von Bosch für die Autoindustrie entwickelt
- Ist ein zweiadriger Bus, halbduplex
- konventionellen seriellen Technologien überlegen in Funktionalität und Zuverlässigkeit
- Kosteneffiizienter
- Entwickelt für Echtzeitanwendungen mit 1Mbit/s Baudrate
- Verwendung mittlwerweile allen möglichen Fahrzeugen, auch maritimer Bereich und Luftfahrt
- Medizinische Geräte, Industrieanlagen, Gebäudeautomation

[Vos08, Seiten 2-10]
Aufbau: Alle Knoten sind mit zwei Drähten verbunden und sind gleichberechtigt. [Vos08, Seite 132]
Die Nachrichten werden nach Broadcasting-Prinzip übertragen. Jede Nachricht wird von allen Knoten empfangen, aber nur die Knoten, die die Nachricht benötigen, verarbeiten sie. Diese werden aber nicht bestätigt, da dies zu einer größeren Last auf dem Bus führen würde. Bei einer fehlerhaften Nachricht reagieren die Knoten mit einer Fehlermeldung, die wieder der gesamte Bus empfängt. [Vos08, Seite 80]

2.2 Raspberry Pi

2.2.1 Raspberry Pi als Rogue Device

Was ist ein Rogue Device und wie wird der RasPi als solches eingesetzt

Kapitel 3

Konzept

In diesem Kapitel

3.1 Bedienkonzept Controller

Wahl des Controllers und wie die einzelnen Tasten zum steuern des Schiffes unter Rücksichtnahme auf besonderheiten des Schiffs genutzt werden können.

3.2 Konzept des Rogue Device

Wie soll es mit dem Controller und dem Schiff verbunden sein?
Was muss ich dabei beachten? Muss eine Rückmeldung für die Eingaben geschehen? Wenn ja, wie? (kleiner OLED-Bildschirm oder App)

3.3 Aufbau Schiffsysteme

Wie werden die Motoren im Schiff angesteuert? Welche Angriffsmöglichkeiten gibt es? Wie wird das Ruder angesteuert? Gibt es noch weitere wichtige Systeme?

Kapitel 4

Implementierung

In diesem Kapitel

4.1 Verbindung Rogue Device - Controller

Benutzte Hardware, Protokolle, Libraries

4.2 Übersetzung Signale Controller - Schiff

Welches Dateiformat wird für Controllersignale benutzt? Wie werden diese effizient genug in Motorsignale übersetzt? Kann ich einfach originale Steuerungssignale unterdrücken?

4.3 Eingabe-Interface

Wie wird die Rückmeldung tatsächlich aussehen?

Kapitel 5

Sicherheit

In diesem Kapitel

5.1 Schwachstellen

Welche habe ich benutzt und welche weiteren möglichen Schwachstellen habe ich gefunden?

5.2 Schutzmaßnahmen

Welche gibt es bereits? Was sind weitere Möglichkeiten?

5.3 Generalisierung

Gibt es solche Angriffsmöglichkeiten auch auf anderen Schiffen?

Kapitel 6

Abschließende Betrachtung

In diesem Kapitel

6.1 Fazit

Was wurde geschafft? Was kann damit ausgesagt werden?

6.2 Ausblick

Wo kann noch weiter geforscht werden? Was wurde nicht geschafft?

Kapitel 7

Anhang

In diesem Kapitel

7.1 Quellcode

7.2 Schaltpläne

Abbildungen

Literatur

[Vos08] Wilfried Voss. *A comprehensible guide to controller area network*. Copperhill Media, 2008 (siehe S. 4).

Erklärung

Hiermit erkläre ich, dass ich die vorliegende Bachelorarbeit selbständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt habe.

Alle Stellen, die wörtlich oder sinngemäß aus Veröffentlichungen entnommen sind, sind als solche kenntlich gemacht.

Die Arbeit ist noch nicht veröffentlicht und ist in ähnlicher oder gleicher Weise noch nicht als Prüfungsleistung zur Anerkennung oder Bewertung vorgelegt worden.

Rostock, 22. November 2024