FCK NSA

Requirements

OTP-Cryptomessenger

Torben

Inhaltsverzeichnis

Abbildungsverzeichnis

1 Projektbeschreibung

Im Rahmen dieses Projektes soll eine Möglichkeit für jedermann geschaffen werden, mit der in der Theorie absolut sicheren Verschlüsselungstechnologie „One-Time pad“(OTP) verschlüsselt zu Kommunizieren. Dabei wird durch Hard- und Softwaremaßnahmen auf der Endgeräteseite die Integrität der Nachrichten gewährleistet.

2 Anforderungen

2.1 Anforderungen die Hardware

2.1.1 HW-REQ100: Einplatinen-Computer

Als Grundgerüst für die Bedieneinheit soll ein Einplatinen-Computer vom Typ „Raspberry Pi“verwendet werden. Die Netzwerkbuchse auf dem Raspberry PI wird hardwareseitig deaktiviert, so wird das unauthorisierte Eindringen über das Netzwerk verhindert.

2.1.2 HW-REQ200: Erweiterungskarte für den RasPi

Auf einer eigens entwickelten Erweiterungskarte für den Raspberry Pi werden drei Subsysteme untergebracht:

- Der Zufallszahlengenerator. Als Vorlage hierfür dient das XR232USB-Projekt. Die Platine muss so gestaltet sein, dass der Zufallsgenerator mit aufgelöteten Weißblech-Gehäusen gegen Störeinstrahlung geschützt werden kann.
- Die RS232-Verbindung. Die Erweiterungskarte nimmt Daten über die serielle Schnittstelle entgegen und gibt sie wahlweise direkt über einen dreipoligen Verbinder weiter, oder aber wandelt diese über einen USB-RS232-Wandler in ein USB-Signal um. Dabei muss die Hardware so gestaltet werden, das weder eine USB-Verbindung bei abgeschaltetem RasPi, noch eine nicht mit Strm versorgte USB-Verbindung bei aktiviertem RasPi der Hardware schaden zufügen können.
- USB-Hub. Um die fünf benötigen USB-Buchsen (Tastatur/Maus 2.1.4, Zufallszahlengenerator, zwei SD-Kartenleser 2.1.3) zu verfügung zu stellen, muss ein Hub auf der Erweiterungskarte untergebracht werden.

2.1.3 HW-REQ300: Zufallszahlenspeicher

Die vom Zufallszahlengerator erzeugten Zufallsdaten werden auf zwei SD-Karten gespeichert. Beide sind mit USB an dem Raspberry Pi verbunden.

2.1.4 HW-REQ400: Eingabemöglichkeiten

Die Bedienung des Geräts muss über Maus und Tastatur geschehen.

2.1.5 HW-REQ500: Message relay

Als Message relay ins Internet dient ein standard-Bürocomputer.

2.1.6 HW-REQ600: Server

Als message relay-server dient ein normaler Server mit rootzugang.

2.1.7 HW-REQ700: Funkmodulator

Als Alternative zum Internet sollen zwei Teilnehmer auch direkt mit einer Funkverbindung verschlüsselt kommunizieren können. Der Modulator muss direkt über eine serielle Schnittstelle mit der Erweiterungskarte (**??** verbunden werden können-

2.2 Anforderungen an die Software

2.2.1 SW-REQ100: Betriebssystem

Auf dem unter 2.1.1 definiertem Einplatinen-Computer läuft eine gehärtete Linux-Distribution. Sie ist auf ein Minimum abgespeckt um eine möglichst geringe Angriffsfläche zu bieten.

2.2.2 SW-REQ200: Bootvorgang

Direkt nach dem Booten soll das Betriebssystem automatisch die Chatsoftware starten. Ein Wechsel auf den Desktop des Betriebssystems sowie das Beenden der Chatsoftware muss verhindert werden.

2.2.3 SW-REQ300: GUI

Die grafische Oberfläche des Programms muss folgende Anforderungen erfüllen:

- Anzeige von Freunden
- Anlegen von Freunden
- Zufallszahlengeneration steuern und füllen der zwei SD-Karten mit den neuen Zufallsdaten
- Anzeigen der noch verfügbaren Entropie
- Mit Freunden chatten

2.2.4 SW-REQ400: Zufallsgenerator

Der Zufallsgenerator muss den USB-Zufallsgenerator ansprechen und die Zufallsdaten auf SD-Karte speichern können. Dabei müssen die Zufallsdaten in kleineren Blöcken gespeichert werden.

2.2.5 SW-REQ500: Crypto-Modul

Das eigentliche Cryptomodul beinhaltet folgende Funktionen, die von der GUI aufgerufen werden können:

- Anlegen eines Accounts, festlegen einer eindeutigen User-ID (2.2.6)
- Verwalten von Freunden
- Nachrichten verschlüsseln
- Nachrichten entschlüsseln
- Verwendete Zufallsdaten müssen auf der SD-Karte sofort mit Nullen überschrieben werden

2.2.6 SW-REQ600: User-ID

Für den Endbenutzer ist die User-ID eine Base36-kodierte 32-Bit Zahl. Beim ersten Start der Software wird der Benutzer aufgefordert, an einem Computer mit Internetzugang eine neue Benutzer-ID anzufordern und auf dem Endgerät einzutippen. Der Master-Server hat eine Liste aller noch verfügbaren User-IDs, beim Besuch der Webseite des Projekts wird bei jedem Laden eine neue Generiert und angezeigt.