netidee

PROJEKTE

IoT-Watchdog

Zwischenbericht | Call 14 | Projekt ID 4430

Lizenz: CC-BY-3.0 AT

Inhalt

1 Einleitung

Das Auftreten der Covid19-Pandemie hatte durchaus Auswirkungen auf den Zeitplan des IoT-Watchdog-Projektes. Der eigentlich für Mitte April bei den Grazer Linuxtagen 2020 geplante Release der Beta-Version wurde durch Erkrankungen im Team sowie das Absagen der Grazer Linuxtage sowie aller anderen Veranstaltungen im Frühjahr verzögert.

Der Release der Beta-Version ist nun für Juli geplant – wie im Blogpost zur Projektvorstellung[1] dargestellt, wird dabei die Basisversion veröffentlicht. Die Basisversion kann das Netzwerk analysieren und die Verbindungen aller Geräte darstellen.
In der Betatestphase möchten wir möglichst viele IoT-Geräte unserer Test-User auf verdächtige Verbindungen analysieren, um im Anschluss geeignete Maßnahmen zu deren Sicherung/Einschränkung zu entwickeln.

2 Status der Arbeitspakete

2.1 Arbeitspaket 1 - Backend

Die Recherche zur Tauglichkeit des Netzwerkscanners Wireshark hat folgende Ergebnisse gebracht:

- Die technische Funktionalität ist gegeben, die ersten Ergebnisse des manuellen Tests wurden bereits als Blogpost[2] veröffentlicht.
- Leider ist das eigentlich zur Verwendung geplante Frontend Webshark mit großen Hürden in der Integration in Raspbian verbunden, daher muss wohl auf die c‘t-Lösung gtk-build + broadwayd zurückgegriffen werden – siehe Blogpost[3].

Ein neues Tool ist in der Recherche aufgetaucht: ntop-ng[4]. Es scheint damit sehr einfach möglich zu sein, nicht nur einzelne Pakete, sondern ganze Verbindungen zu analysieren, sowie zu klassifizieren. Es wird gerade intensiv evaluiert und verspricht den Analyse-Teil des IoT-Watchdogs signifikant zu verbessern.

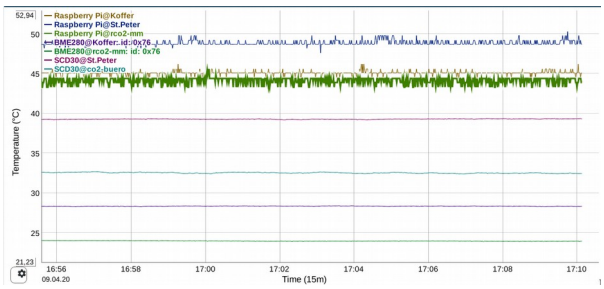
1 https://netidee.at/iot-watchdog/iot-watchdog-projektvorstellung
2 https://netidee.at/iot-watchdog/netzwerkanalysen-ziel-android
3 https://www.netidee.at/iot-watchdog/aktuelle-raspian-images-mit-wireshark-bauen
4 https://www.ntop.org/products/traffic-analysis/ntop

An nötigem Backend-Code wurde die nötige Hotspot-Funktionalität am Raspberry Pi bereits getestet und ins image integriert, sowie der Webserver fürs Bereitstellen des Frontends, der für die Kommunikation mit dem Frontend nötige MQTT-Broker, sowie die Toolchain zum Speichern der aufgezeichneten Daten in die lokale Datenbank.

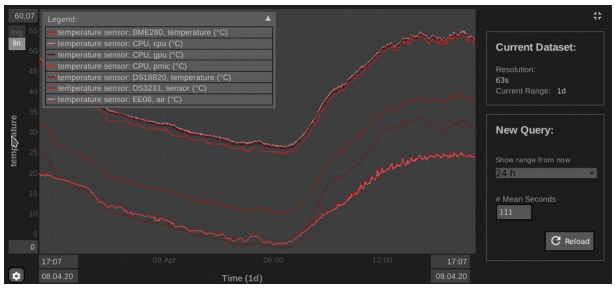
Im letzten Jahr haben sich leider bei der Anfangs gewählten Zeitreihen-Datenbank Prometheus einige Unzulänglichkeiten und fehlende Features als kritisch herausgestellt – darum wurde im Backend inzwischen auf InfluxDB umgestellt. Die InfluxDB bringt signifikante Security-Features wie zB ein User-Management mit, um die aufgezeichneten Daten vor unerwünschten Blicken zu schützen.

2.2 Arbeitspaket 2 - Frontend

Basierend auf dem von UnravelTEC schon für die Visualisierung von Zeitreihen-Sensordaten entwickelten Frontend ng-unrvl wurde ein neues, ansprechenderes Design entwickelt.



ng-unrvl: Basis-Design 2019



ng-unrvl: neues Design 2020

Die API zum Übertragen von Änderungen aus dem Backend ins Frontend wurde auf MQTT umgestellt. Dies verbessert die Reaktionszeit des Frontends wesentlich, so können zB neu dazukommende Netzwerkverbindungen nun ohne Verzögerungen im Frontend angezeigt werden.

Aufgrund der Backend-Datenbank-Umstellung von Prometheus auf InfluxDB im Zusammenspiel mit MQTT mussten auch große Teile im Frontend umgerüstet werden – die Umstellung läuft noch, einige Features wie die Kombination von MQTT und Influx sind im nächsten Monat geplant.

2.3 Arbeitspaket 3 - Updates/Paketsystem

Die Toolchain zum bauen von Debian-Paketen für Updates wurde erfolgreich eingerichtet, siehe Blogpost[5]. Aktuell werden die verschiedenen Softwarepakete gerade in Debian-Pakete umgewandelt.
Die nächsten Schritte sind das Einrichten des Signatur-Systems sowie des Update-Servers.

2.4 Arbeitspaket 4 – Images

Seit Anfang 2020 läuft die Integration der nötigen Pakete in pi-gen. Die build-Toolchain wurde inzwischen erfolgreich von Debian Stretch (9) auf die neue Version Buster (10) umgestellt, und alle daraus resultierenden Bugs behoben.

Inzwischen können erfolgreich angepasste images für den Raspberry Pi Zero sowie den Raspberry Pi 4 gebaut werden.
Der Bau der images wird derzeit noch manuell gestartet, dies soll in Zukunft noch automatisiert werden.

2.5 Arbeitspaket 5 – Doku

Für die Repositories der Einzelteile (Distribution, Frontend, Paketbau-System) ist die Entwickler-Dokumentation in den jeweiligen Repositories als README-Datei veröffentlicht.
Ein Repository für Enduser-Doku wurde eingerichtet, dieses wird vor Beginn der Betatest-Phase noch befüllt.

2.6 Arbeitspaket 6 – Tests

Alpha-Tests wurden im 1:1-Betreuungsverhältnis durch das IoT-Watchdog-Teams bei einzelnen Test“kunden“ durchgeführt – durch die Covid19-Pandemie leider noch nicht im geplanten Umfang.

Die öffentliche Beta-Testphase startet voraussichtlich im Juli 2020.

2.7 Arbeitspaket 7 – Marketing

Die im Frühjahr 2020 geplanten Auftritte auf Community-Events wurden bisher alle aufgrund der Covid19-Pandemie abgesagt – wir hoffen, dass im Laufe des Jahres noch Veranstaltungen zu der Thematik stattfinden.

Sobald die Betatest-Phase startet, werden wir zumindest lokal in Graz auf den Cryptoparties das Projekt vorstellen und um Tester werben.

5 https://www.netidee.at/iot-watchdog/debian-pakete-fuer-raspbian-bauen

3 Umsetzung Förderauflagen

Die Raspberry Pi und Netzteile für den Förderbeirat wurden bereits gekauft, sie werden samt Gehäuse, Netzteil und Speicherkarte verschickt sobald die erste Beta-Version veröffentlicht wird, und uns die Empfänger-adressen bekanntgegeben werden (bereits angefragt).

4 Zusammenfassung Planaktualisierung

Die Corona-Pandemie hat signifikanten Produktivitätsausfall im Team UnravelTEC verursacht, insbesondere durch Krankenstände und die erschwerte Kommunikation. Dadurch haben sich viele Projekte, u.a. der IoT-Watchdog um mehrere Monate verzögert.
Die geplante Öffentlichkeitsarbeit auf Community-Events ist leider bis auf weiteres entfallen, was das so wichtige persönliche Feedback signifikant reduziert hat.
Der Milestone „Beta-Release“ mit Auslieferung der ersten Testgeräte wird sich dadurch auf voraussichtlich Juli verschieben.

Wir bitten daher auch um Verlängerung des Projektzeitraumes von 10 auf voraussichtlich 12 Monate, bis Ende Oktober 2020.

5 Öffentlichkeitsarbeit/ Vernetzung

Im Projekt waren Auftritte auf Messen im Frühjahr 2020 geplant (insbesondere die Grazer Linuxtage im April), welche aber allesamt aufgrund der Covid19-Pandemie abgesagt wurden. Die Grazer Linuxtage 2020 wurden leider endgültig abgesagt, wir hoffen zumindest auf der in den Oktober verschobenen Maker Faire Wien präsent zu sein.

6 Eigene Projektwebsite

Die GitHub-Organisation für alle Quellcode-Repositories:
https://github.com/IoT-Watchdog