Interaktive Visualisierung von Netzwerktraffic

Studiengang: BSc in Informatik | Vertiefung: Computer Perception and Virtual Reality
Betreuer: Prof. Urs Künzler
Experte: Prof. Dr. Torsten Braun (IAM Uni Bern)

Grundstein zur einfachen und intuitiven Visualisierung von Netzwerkdaten und Netzwerkteilnehmern, welche mit dem persönlichen Computer kommunizieren. Während Fachfremde die Netzwerkteilnehmer und deren logische Distanz verständlich dargestellt bekommen, erkennen Fachkundige daraus Verhaltensmuster und Fakten.

Ausgangslage

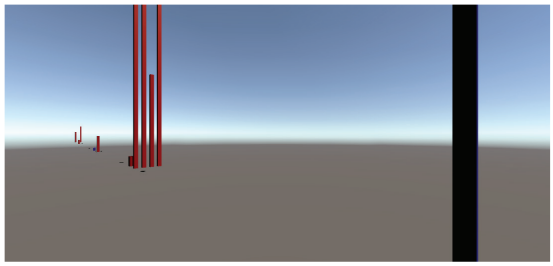
Die Vernetzung von Geräten erlebt im privaten sowie im kommerziellen Sektor grossen Zuwachs. Das Netzwerk gewinnt so an Komplexität. Eine anwendende Person verliert schnell dasVerständnis und das Interesse daran. Der Datenaustausch zwischen den Netzwerkgeräten in einem kommerziellen Netzwerk wird von Routern und Firewalls gesteuert. Diese Steuerung setzt voraus, dass minimale Kommunikationsregeln bekannt und festgelegt sind. Anwendungen wie WireShark bieten Einblicke, um Unstimmigkeiten in der Netzwerkkommunikation aufzudecken. Solche Anwendungen sind aber erst erfolgversprechend, wenn man weiss wonach zu suchen ist.

Ziele

Im Rahmen dieser Arbeit wurde ein Prototyp einer Visualisierung in **VR** (Virtual Reality) entwickelt welcher die folgenden Punkte abdecken soll:

- Einen verständlichen Einblick in das eigene Computernetzwerk für fachfremde Personen geben
- Eine Analysemöglichkeit im eigenen Computernetzwerk für fachkundige Personen bereitstellen
- Generelle Möglichkeiten der Netzwerkdatenvisualisierung aufzeigen

Durch die Umsetzung in VR soll ein „Eintauchen“ ins Netzwerk möglich sein. Eine anwendende Person soll abgeschottet von der Aussenwelt ihren natürlichen Seh-Sinn dazu nutzen, um kommunizierende Geräte im Netzwerk als greifbare Objekte zu identifizieren und zu untersuchen.



Ausschnitt von Prototyp in Entwicklungsstadium. Zeigt IPv4- und IPv6 kommunizierende Sender/Empfängergeräte

Architektur

Der Prototyp besteht aus drei Hauptkomponenten. Die PcapPlusPlus-Bibliothek stellt Funktionen aus dem Npcap SDK (Paketverarbeitungs-Komponente) und der pthread-win32-Bibliothek (Threading-Komponente) zur Verfügung. Die Kombination ermöglicht das Aufzeichnen der Netzwerkdaten. Eine SQlite Datenbank (betrieben im Arbeitsspeicher des Computers) dient zur Datenanlage während Laufzeit des Prototyps. Unity wird zur Visualisierung verwendet und gelangt über eine selbstgeschriebene DLL an die nötigen Funktionen zum Zugriff auf die Datenbank.

Workflow

Zur Aufzeichnung wird eine Netzwerkkarte durch die Angabe der IP-Adresse definiert. Die Rohdaten welche über die gewählte Netzwerkkarte fliessen werden verarbeitet und die gewünschten Daten daraus in der Datenbank abgelegt. Der Start der Aufzeichnung beginnt zusammen mit der Visualisierung von Unity. Die benötigten Werte zur Visualisierung werden mittels Scripts in Unity aus der Datenbank abgefragt.

Zusammenfassung

Der erstellte Prototyp belegt, dass sich eine Visualisierung von Netzwerkdaten wie geplant umsetzen lässt. Durch Hinzufügen zusätzlicher Einstellungsparameter lässt sich die Visualisierung ausbauen. Die Datenbank lässt sich durch weitere Paketinformationen anpassen. Um auch entfernte Geräte zu analysieren ist eine Client-Server Architektur anzustreben. So würden auf dem Client gesammelte Netzwerkdaten an den Server geschickt und zentral verarbeitet.

Andreas Krebs
chef@chraebe.li