IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

Technology and Innovation

GTP and the Evolution of Roaming

Anthony Webb

Anthony Webb
Vice President of EMEA Sales
A10 Networks

Biography

Anthony Webb is the Vice President of EMEA Sales at IT security specialists, A10 Networks (https://www.a10networks.com).

A motivated business leader with a high level of drive and determination, Anthony has more than 20 years experience in engaging with C-level executives throughout his career in the IT, data communications, and telecom industry.

With a proven ability to deliver vision and strategic direction, Anthony has previously worked at Juniper, Cisco, IXIA and Siemens, using this knowledge to drive A10 networks' success in the EMEA market.

Joining A10 Networks in June 2018, Anthony is heavily invested in training the next generation of IT industry professionals. He has significant experience in coaching, developing, retaining and motivating teams to perform at their very best, ultimately helping his colleagues to deliver strong results, within a multicultural environment.

Keywords 5G, GPRS Tunnelling Protocol (GTP), Encryption, Mobile roaming, Roaming security, Cybersecurity
Paper type Research

Abstract

Mobile traffic using GPRS Tunnelling Protocol (GTP) has exploded over the last couple of years, largely due to elimination of international roaming price barriers that previously discouraged subscribers from using the service. Global international roaming traffic – voice and data – is expected to grow 32X by 2022 and to reach over 1.5 Mb per subscriber annually. How ill GTP and roaming change with 5G and what will operators need to do to secure that traffic and their network? In this article, the author discusses roaming an its use of GTP and the evolution of GTP and roaming in 5G, rise of new threats and utilizing a GTP firewall solution.

Introduction

The 5G evolution will impact all aspects of "mobile roaming", including the network requirements, the subscriber usage, and business models.

The roaming network specifications were created to enable subscribers to move seamlessly between networks and to provide operators a mechanism to recoup costs from traffic generated by non-subscribers. In 4G networks, roaming partners are connected through the S8 interface using GTP.


IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

According to 3GPP[1], a global initiative that unites telecommunications standard development organizations in roaming architectures for 5G standalone networks, the GTP user plane is separated from the control plane. The user plane will still use GTP, but for the control plane, the home roaming partners are connected through a new function, the Security Protection Proxy (SEPP), using http/2 protocol.

The embedded application layer encryption at the SEPP will provide additional protection against the known inter-exchange/roaming vulnerabilities which exist in SS7 and DIAMETER protocols, but an L7 firewall will still be required to protect the SEPP control plane.

5G will also add native support for a secure steering of roaming (SoR). The 5G SoR solution enables the home network operator to steer its customers while roaming to its preferred visited partner networks to enhance roaming customers' experience, reduce roaming charges and preventing roaming fraud.

Subscriber traffic and usage

Over the next five years, mobile subscriptions will increase a modest 2% annually to 8.9 billion according to Ericsson, but cellular IoT connections will quadruple to over 4 billion. Data traffic per smartphone will increase six-fold to 21 GB/month[2]. This includes all types of cellular devices – smartphones, IoT wearables, tablets and others – which will all roam with the subscriber.

5G is needed to carry the volume and diversity of this traffic, with seamless interconnection everywhere a vital part of every MNO value proposition.

The 2017 EU Roam Like at Home legislation[3] now prohibits excessive roaming fees, and many other non-EU countries are following suit. With worldwide international tourist arrivals (overnight visitors) reaching a 1.4 billion in 2018, mobile operators have realized that their subscribers expect a seamless (and reasonably priced) experience – wherever they travel and whatever devices they use.

Roaming business model

Besides the technical interconnection requirements, roaming includes a contractual arrangement between operators who agree to carry traffic for each other's subscribers through bi-lateral peering agreements or through agreements with GRX/IPX providers.

In roaming scenarios, generally the subscriber is billed by his home network operator for roaming use and the visited network bills the home network operator for carrying the traffic – per the roaming agreement. If a GRX is used, then there is a settlements process. This type of interconnection model and the mobile charging models (originator or calling party pays) is very different than that adopted by the internet ecosystem. This model is based on bandwidth consumption and uses peering agreements where both origination and termination parties are charged.

There is debate in the mobile industry about the inefficiencies and complexity of the roaming model. Concerns with this model include the high cost of international calls where a home network effectively pays for termination into its own market and the


IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

administrative costs for volume forecasts and commitments, base rates, incremental rates and manual accounting that often lead to settlement disagreements.

As mobile networks move closer to the all-IP internet model and operators compete with OTT and other service providers for subscribers and traffic, the roaming interconnection model as it is can put mobile operators at a competitive disadvantage.

According to the GMSA[4] there could be an opportunity to shape a next-generation interconnection model in a less complex way and therefore reduce costs for implementation of charging. The next generation interconnection regimes (IP peering and transit), at least for any service beyond voice.

Roaming security

Roaming was originally designed based on a trust model. That is, it assumes that the operator has at least a moderate trust relationship with any roaming partner. Otherwise, why would they allow that operator's subscribers to use the network? It was a reasonable assumption since originally, roaming traffic was not that high; the number of potential roaming partners was relatively small, and they were limited to like-minded mobile network operators.

Although GTP used in roaming has known vulnerabilities, the authentication mechanisms of each roaming partner plus the roaming agreement were considered adequate by many operators to prevent unintentional or malicious peer activity. As such, many did not deploy a GTP firewall in their 4G implementations.

However, the mobile roaming ecosystem, traffic dynamics and threat landscape have dramatically changed over the last few years and will continue to change as 5G progresses. For 5G, as described earlier, the roaming interconnection model defined by 3GP includes additional security measures, but GTP will continue to be used.

What is GTP?

GPRS Tunnelling Protocol (GTP) is an IP-based communications protocol, including control and data plane components, that is used to carry general packet radio service (GPRS) within GSM, UMTS (3G) and LTE (4G) networks as specified by 3GPP in various interface points. In LTE networks, these interfaces include roaming (S8), RAN-SGW (S1-U), and between core network elements SGW-PGW (S5), and MME-SGW (S11). GTP includes a user plane component (GTP-U) and a signaling or control plane component (GTP-C). GTP is used to establish a GTP tunnel or channel between user equipment and mobile network nodes (serving gateways and packet gateways) in order to exchange user and control data.

Risks and vulnerabilities of GTP

GTP is extremely useful in facilitating the transmission of mobile data traffic within and between mobile networks and it has been used in 2.5G, 3G and 4G networks. However, it was designed when mobile networks were considered unbreachable, and so it has no inherent security. GTP depends instead upon security provided

IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

through the authentication or authorization of the UE and subscriber from the home network operator. As a result, GTP has several security vulnerabilities which can be exploited by malicious actors or careless roaming partners.

Most operators have experienced the common GTP attacks. Attackers try to exploit vulnerabilities by abusing GTP interfaces exposed to the network. These attackers can include cybercriminals or malicious peers which have been able to control the GRX/IPX roaming links. These attacks target both mobile subscribers and mobile network infrastructure. Common GTP security issues include confidential data disclosures, denial of service, network overloads, and a range of fraud activities. As traffic volume and usage has grown in 4G and soon in 5G, so do the risks.

In 5G additional security measures have been added, but GTP will continue to play an important role, especially in roaming.

In conclusion

As operators move towards 5G, with a 4G common core for many years, the risks inherent in GTP continue to grow against a much larger volume of traffic and applications. Roaming traffic, with its high complexity and large number of interconnect partners and hubs, can be especially vulnerable and attractive target for malicious actors.

A GTP firewall protects networks and subscribers against the GTP vulnerabilities identified by the GSMA. A highly scalable 5G solution is available in physical, virtual, and container forms and so assures operators that they can protect their networks and subscribers, and maintain the high performance demanded by subscribers throughout the entire 4G to 5G journey.

Reference

1 https://www.3gpp.org/about-3gpp
2 Ericsson, Mobility Report, November 2018, https://www.ericsson.com/491e34/assets/local/mobility-report/documents/2018/ericsson-mobility-report-november-2018.pdf
3 https://ec.europa.eu/digital-single-market/en/roaming
4 GMSA, Next-generation Interconnection and Roaming Analysis for Mobile Services, July 2016, https://www.gsma.com/futurenetworks/wp-content/uploads/2017/03/IPX-Business-Analysis-V1-0-061016-1.pdf