Providing Optimization of Encrypted HTTP Traffic

Problem Space

One of the objectives of the Internet community of this decade is to provide universal broadband internet access to everyone by 2020. Today, the population that still lacks connectivity –referred to as the "Other 3 Billions" by some- are located in the most part in areas only served by satellite, and in their large majority are also the lowest income population. Which means cost of access (transmission costs) is essential.

Mobile Network Operators [MNOs] have been so far taken up on this task, combining wireless cellular technologies and satellite backhaul as the most effective and lowest cost to reach out to those populations.

However, satellite resources are and remain expensive, even with the venue of newer technologies (HTS, MEO, LEO), and both satellite and wireless cellular spectrum is limited.

Therefore, MNOs deploying such solution have traditionally relied on application-aware bandwidth management, optimization technology and network devices to reduce the cost of delivering such services and mitigate the inherent limitation of satellite based backhaul transmission.

Recently, the sharp increase of encrypted HTTP web traffic, spurred by the main content providers and the evolution of the web browsers and protocols (Chrome, HTTP2) is threatening the current eco-system economics and hence the ability to achieve the 2020 objective of providing universal broadband internet access to everyone. Optimizations techniques & bandwidth management commonly used by MNOs in the Radio Access Network (RAN)and across satellite transmission links become un-operative, in particular application level compression and content caching (object caching, byte caching), thus increasing cost of service delivery by a factor two or more.

In order to be able to access an encrypted user session content for performing such tasks like optimization or bandwidth management and without access to the content provider's SSL certificate, an intermediary has to present either a self-signed certificate or possibly a certificate that is signed by a root certificate that has to be installed in an end-user's CA store. However, both these approaches are not ideal:

- A self-signed certificate, while providing equally strong encryption, will not be implicitly trusted in a browser. End users will be prompted to 'accept' some unknown certificate. This may lead them to distrust their internet service or mobile provider, or else render the end-user vulnerable to attacks compromising his security and integrity.
- Similarly, an ISP or mobile provider asking end users to install a certificate in their browsers may also lead to distrust as end users might be suspicious of the reasons behind *why* their provider is proxying their HTTP sessions and why they need access to the clear text communication.
- In both approaches, it creates additional complexity in providing services to the end-user which might be a deterrent for the end-user and be contradictory to the goal of granting universal internet access, in particular to population with lower knowledge.

Those have started to be addressed by the IETF in the draft RFC 7258 "*making networks unmanageable to mitigate PM (Pervasive Monitoring) is not an acceptable outcome*", but we believe the urgency of the matter requires a more aggressive approach.

Exploring Solutions

Today, the MNO provides the infrastructure and interfaces between radio and Internet which is core to the delivery of service, and is already a trusted party through the identification and authentication process: the end user already trusts the MNO to provide the access for mobile, to meter and bill customers, enforce policy, act as a bank (Mobile Payment), etc... Therefore, it would be seen quite natural for the MNO to also play a role as a **trusted** entity in the content delivery authentication process. In addition to enable continuing to provide the necessary bandwidth management and optimization solution, this will allow potentially the MNO to assert and further increase their value instead of being reduced to a dumb pipe role in the content delivery path. We believe this could lead to a 3-way win-win solution to the eco-system: the end-user, the service provider and the content provider: ensuring QoE, better services, lower service costs, hence larger user community out-reach to content providers, etc…, in addition to provide opportunities to the MNO for implementing value added differentiated services and solving other issues like, for example, Legal Interception.

Some form of a Trusted Intermediary seems to hold the most promise. We propose that the operator be granted a trusted certificate: one that is ideally pre-installed in popular web browsers, or one that chains to a pre-installed certificate. If the mobile operator certificate is not one that is recognized by the browsers, there would be a one-time install for each end user’s device. We also further suggest that the 3GPP be implicated in the role of granting such certificates, in co-operation with existing certification authorities, and in performing the necessary checks and audits leading to a mobile operator obtaining such a digital certificate.

The 3GPP would have the responsibility of ensuring that certain constraints and business standards are respected and adhered to; and they would also possess the authority to revoke such certificates if any violations are discovered. Although, this may entail an additional cost to the operator, we feel that the potential gains are significantly greater, for the MNO itself and the telecom community in general.

Acting as a Subordinate Certificate Authority, an **Intermediary** (trusted media proxy) server or appliance would obtain a certificate from a trusted certificate authority. This certificate would then be used to sign a generated digital certificate which would then be presented to the user-agent.

This appliance or software used to perform the trusted intermediation should be compliant to certain security standards and the provider of such software or server appliance should adhere or comply similarly with those standards and business conducts, subject to certification & auditing by the same certification authority enlisted to audit and certify the MNO, thus creating a trusted chain and eco-system.

As an example, the Intermediary could be obligated to support the very latest TLS specification so as not to downgrade the level of security used by origin servers. They could also be obliged to perform the same type of validation regarding the digital certificates that most popular browsers do, requiring their certificate store be kept up to date and perform checking of Certificate Revocation Lists. Other limitations on what such a proxy may do are also desirable. Relating this to caching and to compression, no end-user data needs to be saved; or even inspected by the proxy. Such optimizations only need access to the content from origin servers – any data from the end-user is of no interest and holds no value to these optimization platforms. They would be required to build a robust platform to prevent unauthorized access.

Final Thoughts

We have read other proposals describing some kind of opt-in system where the end-user would be given the choice as to whether or not the mobile operator could have access to the clear text content. Although we do feel that the end user should be engaged, this kind of solution may only solve partially the issues at hand. In addition to creating additional complexity which can be a deterrent to the service delivery itself, and result in significant cost increase of such appliance solutions compared to the inexpensive costs of bandwidth optimization solutions available today to MNOs.

Rather, we suggest that the MNO be granted to extend his role as a **trusted entity** for content delivery between the content provider and the end-user, through being granted a **trusted certificate**, for the purpose of managing the delivery of content, understanding the MNO is already a trusted entity for the identification & authentication of the end-user and certain applications (Mobile payment, Mobile banking).

Also, it could and would be entirely up to each MNO to choose to apply the kind of appropriate policy with regards to end-user awareness. For example either through subscription contract policy, or opt-in/opt-out policy, depending of the context (terrestrial or satellite backhaul for example), and purpose of the Intermediary, MNO policy, in-country legal framework, agreements with content providers, etc… and grant the end-user with opt-in behavior or not. This will reaffirm the importance of the role of the MNO in content delivery chain, which we believe is paramount if; ultimately, we want MNOs to play their role in providing affordable internet access to everyone and also ensure a safer & better world. For example, while a content optimization Intermediary might be implemented with an Opt-In / Opt-Out policy, according to various parameters, an Intermediary used for performing Legal Interception should not have such policy.

We feel that there is room for *both* the protection offered by encrypted HTTP and for optimizations of such encrypted content. We believe that service providers will be willing to implement mechanisms and to respect the constraints placed upon them in order to continue to manage their network efficiently. We look forward to learning what other institutions have done or plan to do regarding this problem; and to sharing our thoughts and ideas on this topic.

Yves Hupe, President/CTO Memotec Inc.

Claude Rocray, VP Engineering

Mark Santelli, Senior Software Developer