Priva-Stream: Private Collaborative Live Streaming
Simon da Silva

To cite this version:
Simon da Silva. Priva-Stream: Private Collaborative Live Streaming. 19th International Middleware Conference Doctoral Symposium (Middleware ’18)., 2018, Rennes, France. hal-02181024

HAL Id: hal-02181024
https://hal.archives-ouvertes.fr/hal-02181024
Submitted on 11 Jul 2019

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L’archive ouverte pluridisciplinaire HAL, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d’enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.
Priva-Stream: Private Collaborative Live Streaming
Simon da Silva

To cite this version:
Simon da Silva. Priva-Stream: Private Collaborative Live Streaming. 19th International Middleware Conference Doctoral Symposium (Middleware '18)., 2018, Rennes, France. hal-02181024

HAL Id: hal-02181024
https://hal.archives-ouvertes.fr/hal-02181024
Submitted on 11 Jul 2019

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L’archive ouverte pluridisciplinaire HAL, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d’enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.
**PRIVA-STREAM: Private Collaborative Live Streaming**

Simon Da Silva  
Univ. Bordeaux, LaBRI, UMR 5800, F-33400 Talence, France  
simon.da-silva@labri.fr  

**Abstract**  
Video streaming currently accounts for more than 75% of overall Internet traffic. However, Content Delivery Networks, which are commonly used to deliver video content, are costly to setup and do not scale well for live video streaming services.  

We introduce Priva-Stream, an edge-assisted content delivery system allowing to aggregate video content from multiple edge peers in addition to existing delivery servers. Priva-Stream uses incentive mechanisms to reward participating users, and trusted execution environments such as Intel SGX to enforce privacy. Our experiments using a complete prototype show that Priva-Stream increases the quality of experience end-users can expect while at the same time providing strong privacy guarantees.  

**Keywords** streaming, privacy, trusted execution environments  

**ACM Reference format:**  
DOI: 10.1145/nnnnnnn.nnnnnnn  

1 Introduction and Background
Video streaming is already the first source of Internet traffic and is forecast to more than double by 2020. Content Delivery Networks (CDNs) are essential to the scalability and quality-of-experience of large-scale video delivery. The use of commercial CDNs comes however with significant costs. An alternative is caching video content on end-users devices and leverage direct connections for edge-assisted collaborative CDNs. This approach comes with two important challenges. End users must have an incentive to contribute their resources, or may not be interested in bearing the associated costs. Caching and serving previously-consumed video content is an important threat to user privacy, potentially allowing to map their personal interests.  

We introduce Priva-Stream, an edge-assisted content delivery system allowing to aggregate video content from multiple edge peers in addition to existing delivery servers. Priva-Stream uses MS-Stream, a multi-source adaptive streaming solution, trusted execution environments such as Intel SGX to enforce privacy, and incentive mechanisms to reward participating users.  

**Adaptive Streaming** Among the many existing on-demand and live video streaming architectures and techniques, the DASH standard [11] has emerged and is currently widely used by most big industry players such as Netflix or Youtube. The MS-Stream [2] solution was introduced. It is an extension of DASH wherein a client can simultaneously utilize multiple servers in order to aggregate bandwidth over multiple links while being resilient to network and server impairments. For each video segment, the client simultaneously instructs several servers to generate and deliver complementary sub-segments, and merges the received sub-segments so as to reconstruct a playable video segment with the highest possible visual quality over time.  

**Trusted Execution Environments** Trusted execution environments (TEE) offer the guarantees of isolation, confidentiality and integrity of data and computations performed in untrusted environments by leveraging custom microprocessor zones. In the same line as ARM TrustZone [1], Intel designed Software Guard Extensions (SGX) [3] first introduced with the Skylake generation of processors, as an isolated execution space. SGX defines an enclave as an authenticated secure container that encapsulates private data and computations.  

**Privacy-preserving live streaming systems** Most private content consumption systems rely on content and metadata encryption, often relying on Private Information Retrieval protocols. For instance, Popcorn [5] manages to enforce privacy for Netflix-like streaming systems. Other approaches consist in encrypting data at the CDN side [4] or introducing encrypted communication channels between anonymous participants [8]. However, all these solutions come with a high cost and performance overhead.  

**Rewarding for collaborative systems** Without incentive to contribute, many users will selfishly consume resources (eg. content or bandwidth) without contributing back to the system. To try and solve this issue, some incentive and free-riding control mechanisms were designed. A few systems reward upload capacity or storage in P2P-VOD systems [12, 13]. But most mechanisms implement either direct [10] or indirect [6] reciprocity schemes. For instance, SVC-TChain [7] incentivizes good behavior in layered P2P video streaming through a triangular reciprocity scheme TCChain [9]. However, in our case, the clients download video segments from other peers to obtain QoE improvements in addition to streaming from the public servers, and do not exclusively obtain data from peers. The incentive can thus not be based on reciprocity.  

2 Priva-Stream  
As shown on Figure 1, the Priva-Stream system is composed of four distinct entities. The **client** host an MS-Stream client. The **tracker** server fully runs inside an SGX enclave. The **MPD server** delivers manifest files. The **public server** delivers video segments.  

The **tracker** hosts a key-value RAM database inside the SGX enclave. It contains the video contents identifiers (unique random ID and segment numbers), and keeps track of peers possessing the contents. When clients receive a new video segment, they post the information to the tracker which will then advertise the peer to other requesting clients. The **MPD server** delivers the manifest file, which contains technical details on the video contents, and the addresses of public servers hosting them. The **public server** is an
When an end-user is willing to watch a video content, he starts a tracker to setup a realistic environment, we implement bandwidth limits, startup delay. We experiment with and without SGX enclaves, and plot QoE metrics: end-to-end delay, packet loss, and aggregated to reduce distributions noise.

In this setup we evaluate the scalability of the system in terms of number of simultaneous clients. To do so, we stress the content server, tracker server and peers with multiple simultaneous requests, and keep track of failures.

Obfuscating requests impact We analyze fake queries impact on privacy and QoE to quantify the eventual trade-off between quality and privacy.

### References


### 4 Conclusion

**Priva-Stream** enables better scalability for live video streaming, while solving some of the main issues of edge-assisted systems, i.e. lack of privacy and free-riding. **Priva-Stream** uses Intel SGX to enforce privacy, and incentive mechanisms to reward participating users. Our experiments using a complete prototype show that **Priva-Stream** increases the quality of experience end-users can expect while at the same time providing strong privacy guarantees.