blust ™
FILL YOUR SCREEN

WHITE PAPER

SECURE PEER ASSIST
and how it works in
THE BLUST SYSTEM

GT Systems, Rhett Sampson, 18 December 2015
Update v1.1 28 June 2017
v1.2 7 february 2018

BACKGROUND

Secure Peer Assist is a network technology invented by Rhett Sampson and assigned to GT Systems pty. ltd. as part of Australian and international patent application number PCT/AU2015/000661 "Media Distribution & Management System & Apparatus". It has been, as the patent states, built for security from the ground up.

Secure Peer Assist is a wholly new network technology. It is completely separate, secure from and invisible to BitTorrent. It does, however, combine and build upon some of the best features of peer to peer networking and content distribution networks (CDN). Secure Peer Assist combines these features to produce a secure network system that delivers optimum streaming and download performance, regardless of file size, at any Internet speed. In combination with an Intel 7TH generation or later architecture, tightly coupled with Windows 10 or later, it is one of the most secure and effective content distribution systems in the world. This paper begins to elaborate on how we achieve that. Further details are available on request. They may require non-disclosure agreements.

LIMITATIONS OF ADAPTIVE BIT RATE

Until now, Adaptive Bit Rate has been the universal solution to legal delivery of video on the Internet. As the name suggests, Adaptive Bit Rate (ABR) reduces the bit rate of video if the Internet is congested. Because of the exponential growth of video, the Internet is very often congested[1,2]. This manifests as fuzzy pictures and picture freeze, the "spinning wheel of death". What that means for consumers is an often severely degraded video experience. It also means they aren't getting the quality they paid for.

DESIGN OBJECTIVES

Secure Peer Assist has been designed to meet the following objectives:

1. Deliver content (movies, games, VR etc.) at full resolution, regardless of file size, Internet speed or congestion
2. Do that securely, to meet and exceed content owner requirements
3. Optimized for user bandwidth and network congestion
    3.1. Streamed if user bandwidth permits
    3.2. Otherwise progressively downloaded
    3.3. Maximizing use of customer connection
    3.4. While allowing normal Internet use
4. Using standard Internet protocols
5. Minimising transmission and distribution costs

It has been specifically designed to avoid the following:

1. Any use of BitTorrent protocols
2. Any reduction from optimum transmission bit rate (i.e. no adaptive bit rate)

---

[1] http://www.channelnews.com.au/news/94YPG73G-millions-face-slow-internet-over-easter-as-consumers-log-onto-free-netflix.aspx
[2] Point 12 of http://www.cnet.com/news/13-things-you-need-to-know-about-the-fccs-net-neutrality-regulation/

COMPATIBILITY

Secure Peer Assist has been designed and engineered to maximize use of, and compatibility with, the massive existing infrastructure supporting Adaptive Bit Rate (ABR) streaming, while maintaining all the benefits of Secure Peer Assist. Because Secure Peer Assist is a new protocol at an auspicious time in the development of streaming technology and platforms, it is able to take advantage of emerging standards that provide a foundation for wide compatibility and openness.

THE BLUST™ MACHINE

Secure Peer Assist has been designed to work closely with the Blust app running under the new Intel/Windows security architecture to form the Blust media machine. Every Blust machine is a peer in the Secure Peer Assist network. The Blust machine is built on an open, Intel 7th generation or later processor and Windows 10 (or later) platform. The user interface is built in the Universal Windows Platform framework and takes advantage of the groundbreaking security and open standards integrated within that environment. The Blust application has been built as a Universal Windows Platform app. This allows extremely simple operation across platforms with full use of Windows apps alongside the Blust app.

The latest generation Intel architecture implements a full Trusted Execution Environment (TEE), including secure boot, as required by studios for high value content such as Ultra High Definition (UHD). The security architecture includes the new Secure Guard Extension (SGX) instructions that enable processes to implement Secure Enclaves which cannot be accessed by the Windows 10 operating system. Instead of relying on encryption and software, Secure Enclave technology is hardware-based, and is so secure that an NSA "red team" were unable to penetrate it.[3]

The Blust architecture implements native, hardware based Digital Rights Management (DRM). This conforms to studio requirements for high value type 1 content. It also incorporates a full HEVC hardware codec. The Blust system provides the power required for the highest quality delivery and playing of premium UHD 4K movies, TV, AAA games, VR and AR. The initial Blust machines have been co-operatively designed with Intel and Gigabyte to implement the GT Systems secure architecture. The media pipeline is robustly secure to studio requirements. The Blust app will run on any Windows PC.

OPERATION

Secure Peer Assist uses a synchronous, event-driven network application framework for large file transfers, protected with transport encryption and anchored in Secure Enclave applications. The protocol is a high performance UDP based data transfer protocol. It is designed for data intensive applications over high speed wide area networks, to overcome the efficiency and fairness problems of TCP. The protocol is built on top of UDP and provides reliable data streaming.

Secure Peer Assist manages all Internet transmission of content files, from content servers (e.g. CDN origin store) to client device, e.g. the Blust machine. It is designed to work with encrypted content and to inter-operate transparently with existing Internet protocols and streaming technologies. In effect,

---

[3] 2014 National Security Innovation Competition Proceedings Report, Secure Enclaves-Enabled Technologies, UNITED STATES AIR FORCE ACADEMY

Secure Peer Assist transparently transforms Adaptive Bit Rate content streams into optimum bit rate progressive downloads.

Secure Peer Assist manages the network of Blust CDN servers, machines and content in real time. It maintains the state, status and location of every content segment in the network. It responds to "play" requests and provides the required encrypted content segments to the requesting device and service. Sourcing of content segments is optimized for performance, quality of experience and cost, giving viewers better video quality (higher bitrates), fast loading speeds and no picture freeze. The Blust network can be viewed as a giant, distributed server with software defined networking.

SECURITY

Secure Peer Assist has been designed for security from the ground up. All network communications are secured by encrypted protocols. Content keys are managed within highly secure trusted environments rooted in hardware security. All payloads are encrypted with robust Digital Rights Management (DRM) approved by the content owners. Secure Peer Assist is only implemented on highly secure platforms with hardware based encryption/decryption, hardware DRM, trusted execution environments and secure media pipelines. All core applications are protected by Secure Enclaves.

Network management systems are closed and secure. All communication is within the Secure Peer Assist network. It is designed to inter-operate with secure digital content asset management, ecommerce and publishing systems.

Secure Peer Assist is designed to operate transparently with DRM (initially Microsoft PlayReady set to hardware-based DRM), as required by studios for high value UHD content. Payloads are encrypted, with headers left in the clear as specified in the Common Encryption Scheme (CENC). This enables Secure Peer Assist to securely move video segments around the network as required.

QUALITY

Secure Peer Assist has been designed to deliver content at the highest quality possible. It has been designed to overcome the limitations of distributing video via the Internet in order to deliver True HD and UHD, all the time[4]. It does this by optimizing throughput on the users' home Internet connection and by intelligent distribution of video segments securely within the network.

INITIAL PROTOCOL STACK

Secure Peer Assist has been implemented first using MPEG-DASH. DASH is MPEG's standardized Dynamic Adaptive Streaming over HTTP. Secure Peer Assist transparently transforms DASH content streams into optimum bit rate progressive downloads. This forms the basis of a widely compatible architecture that utilizes open, standard implementations of world's best practice streaming technology. DASH is specified in the following international standards:

---

[4] "True HD and UHD, all the time", "Blust", the Blust device and logo are trademarks of GT Systems pty. Ltd. All other trademarks are the property of their respective owners.

ISO/IEC 23009-1 specifies the overall DASH architecture and the XML syntax for the MPD (Media Presentation Document)

ISO/IEC 23001-7 specifies the Common Encryption for MP4 fragments

ISO/IEC 14496-12/AMD 3 specifies the extensions to 14496-12 that are necessary to support DASH with fragmented MP4 media

Secure Peer Assist via DASH (DSPASH) supports W3C Encrypted Media Extensions (EME) and Common Encryption (CENC). This enables operation with the latest Digital Rights Management regimes, particularly hardware DRM required for high value type 1 content such as UHD (4K).

FUTURE PROTOCOL STACKS

Secure Peer Assist can be adapted to any ABR protocol, such as HLS, HDS and Smooth Streaming. These will be evaluated on a case by case basis.

CONTACT

Rhett Sampson, CEO & CTO

GT Systems

rhett@gtsys.co

Paramount House

55 Brisbane Street, Surry Hills, NSW

2010 Australia

Phone +61 2 9280 4822

www.blust.tv