DATA BROADCASTING TO A TRUSTED CLIENT

AUTHOR: BHAVAN SHAH, MARC DUVIVIER

Wavexpress
One Pennsylvania Plaza, Suite 2400
NY, NY 10119
(917) 339-9000
TABLE OF CONTENTS

1. INTRODUCTION .................................................................................................................. 3

2. END-TO-END CHALLENGES ................................................................................................. 4
   2.1 ARCHITECTURE ................................................................................................................. 4
   2.2 CHALLENGES AND SOLUTION ....................................................................................... 5
      2.2.1 Content Preparation ...................................................................................................... 5
      2.2.2 Content Type ................................................................................................................ 5
      2.2.3 Content Scheduling ...................................................................................................... 6
      2.2.4 Data transport .............................................................................................................. 6
      2.2.5 Multi-tier Network ....................................................................................................... 6
      2.2.6 Data Reception ............................................................................................................. 6
      2.2.7 Cache Management ..................................................................................................... 7
      2.2.8 Platform Performance ................................................................................................. 7
      2.2.9 Customer Service ......................................................................................................... 7
      2.2.10 Business Model ......................................................................................................... 8
      2.2.11 Security & Privacy ..................................................................................................... 8

3. MULTIMEDIA CLIENT ............................................................................................................. 10

4. TRUSTED CLIENT AND CONTENT ...................................................................................... 11

5. FUTURE DIRECTION ............................................................................................................. 16

6. SUMMARY .............................................................................................................................. 17
LIST OF FIGURES

Figure 1: End-to-End Network for Content Distribution, Consumption, and Reporting...........4
Figure 2: Client Security and Privacy..........................................................................................9
Figure 3: Secure Multimedia Client Architecture.......................................................................10
Figure 4: EMBASSY Architecture..............................................................................................13

1. Introduction

The Internet has had enormous growth in the 1990s, analogous to the broadcast industry in the
1950s [television], 1970s [cable], and 1980s [satellite]. It has suffered from seven challenges that
need to be addressed in the next stage of its development.

Speed
Scale
Quality of Service [QOS]
Operational Cost
Business Model
Security
Privacy

There are discrete efforts underway on each of these individual items, but data broadcast is one
method that has the potential to allow services to be offered that address all of these items in a
way that is compelling to service providers and customers alike.

It increases the apparent Speed by allowing for the pre-delivery of content (at high rates of speed)
to client devices, and making these services available to customers who may not otherwise have
access or budget for high speed services.

Scale is inherent in the broadcast distribution to many individuals, rather then on demand
services.

It provides QOS by allowing for the controlled scheduling of a fixed pool of bandwidth, with
managed services for opportunistically available bandwidth.

For popular content, the Operational Cost of broadcast distribution is substantially lower due to
savings of data transportation costs and low marginal customer costs.

Business Model, Security and Privacy are topics that need to be comprehensively addressed in
order for data broadcast to achieve its potential in providing the prior benefits to customers,
particularly for consumer markets. This paper will identify and address core issues, challenges,
and solutions in a data broadcast network to provide high quality, private, and secure services.

In addressing these challenges, data broadcasting is complementing, enhancing, and extending the
capabilities of the Internet, not competing with it.

Wavexpress has created a compelling end-to-end solution that uniquely combines TV, Internet,
and data broadcast with security and commerce, allowing services not previously possible.
2. End-to-End Challenges
This section explains the end-to-end system required for the data broadcasting to a secure client and then addresses the challenges.

2.1 Architecture
The end-to-end system for data broadcast content distribution network is shown in Figure 1:

![Figure 1: End-to-End Network for Content Distribution, Consumption, and Reporting](image)

The content provider prepares the content for the mass distribution by transcoding it into proper formats, tagging it with meta information, and packaging it according to its intended business model, such as a purchasing scheme incorporating digital rights management. Prepared content is uploaded to the content distribution server and scheduled for delivery using automated tools. Content may be distributed to distribution partners throughout a nation-wide footprint, either by satellite or fiber optic networks using MPEG or IP based transport.
Distribution partners include content networks, cable MSOs, specific broadcasters (cable, satellite, or terrestrial), or a combination thereof. At each stage content can be inserted or removed, as well as cached for later transmission and re-transmission. If the format and protocol of such a cache is based on a HTTP proxy, it can also serve as distributed cache/proxy to reduce traffic and speed up the content delivery using a point-to-point network (Internet). In this capacity distribution partners can act as both a broadcast/multicast distribution agent and as an Internet service provider (ISP).

The end client receives the content broadcasted over the cable, satellite, or terrestrial broadcast. The content can be consumed “live” (A/V streaming) or cached in the storage device for later retrieval. A smart caching mechanism is used to determine how content is filtered, stored, cache managed, and presented. The content must be secured from un-authorized usage, and users must be guaranteed the authenticity of the content. Both of these requirements benefit from a secure client platform, discussed in the Section 0.

Content providers would like to be able to construct their content with the maximum flexibility of content types and supported business models. The traditional content protection schemes of subscription or conditional access (CA) systems are primitive forms of such models. The challenges and solutions to allow such flexibility are discussed further in this paper. Once the content is consumed and paid for, the transaction must be reported, but broadcast networks do not always lend themselves to “always connected” applications. The key is to use a back channel sporadically to securely exchange transaction and related information.

Once the transactions are reported, the associated content provider and distribution partners are paid appropriate royalties, and data warehousing type applications are used to support marketing functions.

2.2 Challenges and Solution

To achieve the end-to-end data broadcast system with commerce capability we recognized the following challenges:

2.2.1 Content Preparation

Data must be prepared before the broadcast distribution. The most important aspect of this is securing the content to protect against its unauthorized viewing or distribution. Numerous digital rights management technologies exist, but it is important to employ a solution that can work with multiple DRM systems and provides a high level of security. The content must be transcoded into appropriate formats and prepared with various parameters/tags. Such tags include information regarding scheduling, caching, rating, content path, datacast channel, subscription, etc., as well as generalized tags that may be interpreted by the specific content channel within the client application.

2.2.2 Content Type

Data broadcast systems allow for a variety of delivery methods for various content types. The minimum required types include: Internet type file delivery with associated URL information, reliable file delivery (using carousal and back channel), streaming (for A/V and other continuous content), event, broadcast guide, and metadata.
2.2.3 Content Scheduling
The scheduling system must allow for fixed bandwidth, variable bandwidth, and opportunistic bandwidth.

The fixed bandwidth allows for scheduling content at a specific time at a specific rate. This will provide a rectangular box on a two dimensional graph with time and bit-rate as two axes.

The variable bandwidth allows for scheduling content at a specific time but with variable (known at schedule time and changed at transmission time) bit rate. This will make a free form object on the two-dimensional graph.

The opportunistic bandwidth allows sending data during the unused portion of the bandwidth resulted from variable bit rate (VBR) encoding of the MPEG-2 A/V signal. The most practical way to achieve opportunistic bandwidth is using queuing buffer with priorities.

Some combination of such scheduling provides various QOS (Quality of Service). This will allow for guaranteed delivery (using fixed bandwidth), best effort delivery (using opportunistic with priority queue), guaranteed delivery no later than a specific time (using variable bandwidth optimizing un-used bandwidth). For the priority based queuing, pre-emption should be available during a large file transfer.

2.2.4 Data transport
Most digital broadcast systems are based on the MPEG-2 (or similar) transport, which allows for the bit loss over the network. While various methods (data piping, data sections, data carousel) are possible for sending data over MPEG-2 transports, the popularity of IP based networks makes IP encapsulation using Multi Protocol Encapsulation (MPE) the most practical.

UDP multicast on IP is well suited for broadcast networks but does not offer any flow control. At a minimum, flow control is necessary between data servers and the IP encapsulator. This can be achieved by sending UDP datagram within TCP, if the IPE supports the repacking, or using proprietary UDP based flow control mechanism between the IPE and the multicast server system.

2.2.5 Multi-tier Network
In a digital broadcast network, it must be possible to have multiple stages of content collection. For example, a network distributes a national feed of content to local broadcast affiliates. The local broadcast station, after adding (and possibly removing some) content, originates the final content stream. The solution must allow for such capabilities, and the bandwidth used by the content that is removed must be usable for other purposes. The program guide (and meta data) must correctly reflect such addition/deletion.

Content coming from the upstream must be allowed to pass through each stage or allowed to store-and-forward, allowing for distributed caching and proxy service.

Finally, the content tags for all content must be modified for the customization at each stage. For secure content, this must be performed in a trusted and secure manner.

2.2.6 Data Reception
The receiver hardware must allow the extraction of data coming over the MPEG-2 transport. For IP data, a LAN driver should be provided – treating receiver hardware as a NIC (network interface card). It may also allow for programmable Ethernet address (for point-to-point delivery).
The receiver must allow for error correction and packet recovery for reliable/guaranteed delivery. Once the packets are assembled, the missed packets can be retrieved via back channels or during the successive transmission of the same content/module. The re-transmission happens based on a client request via the back channel or automatically according to a pre-defined configuration. If the missed packets/content is pulled from the back channel, a distributed content proxy must be employed for load balancing and faster access. Such proxy servers can reside at the edge of the broadcast network (local broadcast station, cable head end, or any other ISP).

The received content must be filtered out based on user criteria and subscription. Various mechanisms could be used based on PID, IP address, and content type/tag.

2.2.7 Cache Management

The content delivered over the broadcast is cached on the client machine’s storage device. The storage capacity on a PC is doubling every nine months, and hard disks with terabyte storage capacity are anticipated within a few years. Nonetheless, the available storage must be used wisely. The content must be cached using various parameters including cache size, end user choice, behavior, business models, content tag, etc. The cache manager must provide for garbage collection to free up the storage appropriately.

2.2.8 Platform Performance

Data reception may put a tremendous burden on the receiver platform. Various tasks that require CPU and other resources are:

1. Data extraction from MPEG-2 stream, IP de-encapsulation, forwarding IP packets through TCP/IP stack, packet re-assembly, and content collection;
2. Channel, service, or content filtering at the PID or IP level;
3. The error correction (like FEC) used to recover lost bits from the acquired bits;
4. Software based MPEG decode, multimedia stream/file playback;
5. Cache management;
6. Security related processing; and,
7. Other concurrently running programs.

Receive hardware and software must be carefully tuned to ensure proper function. MPEG PID/Section level filtering (especially performed in hardware) or IP filtering, for example, prevents the CPU from being consumed processing unwanted content.

2.2.9 Customer Service

In addition to Standard Call Center support, it is usually necessary to provide for community administration and service provisioning through a centralized system. With a registered trusted client, users can administer and provision their own services without contacting customer support. This is more convenient for users and substantially lowers operational costs for the service provider.
2.2.10 Business Model

Traditionally, service providers have been able to execute only a severely limited number of business models. The primary models available today in cable and satellite systems are subscription and pay-per-view. Ideally, a content provider should be able to choose any business model and execute it in a way convenient to the user. This is a particular challenge in broadcast systems, since not all models exist, scale well, or are economical if the users connect to the Internet to execute the service.

For example, a content provider might want to provide the newest version of their first person shooter computer game (e.g., Quake), where the game is free but bullets cost 1/1000th of a penny, with the consumer owning the game when they reach the retail price.

Another model might be to broadcast 10-minute movies, and charge $0.05 for watching them.

You could also create an interactive television game show, with thousands or millions of consumers paying an entry fee and playing for cash prizes against each other.

These are some examples of the variety of models that could be conceived. The challenge is to provide a secure way to enable any model to be developed and executed, while limiting the customer acquisition cost and eliminating the marginal cost of executing those transactions. This enables content providers to focus on the experience and opportunity they wish to create, without being limited by the platform or the availability and economics of server side transactions.

2.2.11 Security & Privacy

Security encompasses a host of inter-related and complex issues. All systems must be developed with specific threat models in mind, where the threat model encompasses both the type of attack and the resources the attacker can or will make available to defeat it. Commercial pirates, for instance, have significantly greater resources available than consumers for attacking content security.

Privacy is a specialized form of user security, but creates a set of thorny issues that must be addressed. A system that provided absolute user privacy for purchases, for instance, would be unable to allow for proper customer support, since the service provider could not verify that the transaction had occurred. Likewise, the system provides unique user service IDs to different service providers to prevent the unauthorized sharing of user information data, but it cannot prevent the user from providing both services identifying information, such as a social security number.

The Internet suffers from a host of security and privacy challenges, and there is substantial evidence that because of this consumers hesitate in using the Internet as freely as they might. The most common reasons consumers cite in surveys for not shopping on the Internet, for example, are [in order] privacy, security, and convenience. Common issues cited by merchants include ineffective merchandising [advertising], creating trust with the consumer, and making the users experience convenient. A secure datacast network should address all these issues in a compelling manner.

An ideal security solution is low cost, convenient, flexible, renewable, and strong against a wide variety of threat models. Key areas to be addressed include platform security, content security, network security, application security, and user security.

An ideal privacy solution is flexible, protects data according to a rule system, is self managing, allows for private relationships between one or more parties, and is convenient and transparent to the parties involved.
Figure 2 displays core elements that need to be brought together for a complete security and privacy solution:

![Figure 2: Client Security and Privacy](image-url)
3. Multimedia Client

This section discusses the characteristics of the multimedia client that combines TV, Internet, and data broadcasting. The client architecture is shown in Figure 3, below:

![Figure 3: Secure Multimedia Client Architecture](image)

The secure multimedia client needs essentially three components: a secure execution environment, multimedia capabilities (Audio, Video, Graphics), and networking.

The secure execution environment consists of a security co-processor, a secure real time clock, electronic funds, tamper resistant hardware, and crypto acceleration. This is further discussed in Section 4.
The networking component is required for (1) delivery of broadcast data, (2) certain types of interactive services, and (3) sporadic access to the Internet for a secure environment. The data coming over the broadcast (within the MPEG-2 transport) is extracted from the digital TV card and forwarded to the network stack. The best practice is to use the IP based network stack as it offers a robust implementation, separating application development from the networking stack, and using a back channel to enhance reliable delivery when necessary. In this case, the IP data is encapsulated as sections in the MPEG-2 transport using multi-protocol encapsulation (MPE) syntax. The multicast UDP data is the most suitable for point-to-multipoint data broadcasting. It is possible to extract the relevant data and forward it directly to the middleware (dotted line in the figure). The received data is subsequently forwarded to the datacasting middleware, which offers:

1. Reliable delivery data over the unidirectional broadcast data. While the data can be made highly available by data carousel (multiple transmission of the same data) or re-broadcasting missed packets, the reliability can be achieved by the delivery of missed packets over the back channel.

2. Streaming. This is used for continuous stream of A/V. When IP-based data is carried within MPEG-2 transport, such streaming offers web-like streaming, but reaches a vast audience with guaranteed bandwidth and high quality.

3. Internet file delivery. Such files can be cached on the client and offered to the web browser (using HTTP proxy). This provides faster access to the Internet data if it would be sent over the broadcast and cached locally. If it is not available, the web browser can pull such data using the back channel. In either case, the end user will have a seamless experience, the difference being speed.

A rule system allows for content cache management. The rule system works with the parameters like the end user choice, available storage capacity, business models, smart detection of preferences, and flexibility for content author/providers.

The multimedia component provides the capability for A/V presentation. The digital TV card receives the MPEG-2 A/V PES stream of the digital broadcast, which is decoded in the software or hardware depending upon the card. The A/V control software provides various controls and allows the proper rendering using the graphics sub-system. The control software also connects various decoding elements together. Using the proper plug-in and script interface, the TV rendering and navigation is achieved like a web page.

The A/V streaming coming from the datacast part of the MPEG-2 transport or A/V file (downloaded using datacasting) playback. It may (but is not required to) use the same decoder as MPEG-2, and uses hardware or software based decoding. It works with the security sub-system to ensure proper digital rights. Using the web browser as a navigation system, various channels are created as a series of web pages. The content downloaded using the datacast are grouped under various channels, or services within the channels. Each channel is a collection of web pages with related content, and a web browser application makes it easy and intuitive to browse through web sites (internet), streams, channels created using datacast content, and TV.

4. Trusted Client and Content

A general usage datacast service imposes more stringent operating conditions than many traditional distribution networks that offer controlled content to a controlled environment. Broadcasting to devices that may not be connected to a network requires the rights to travel with the data, and permissioning and transactions to occur in the client. If the datacast network is to support content from multiple providers without requiring them to adopt the packaging systems
of the network provider, and prepare their content accordingly, then the client must be capable of executing whatever permissioning system the content provider has adopted. Clients not authorized to receive the data must be prevented from unauthorized usage, and malicious users with potential access to a piece of the network [cable modem, DTV] must be prevented from sending unauthorized and potentially damaging content to receivers.

All platforms have inherent security risks, but the PC platform is generally acknowledged as particularly insecure. Platform security is generally required before other security issues can be addressed, the exception being when trusted servers are used to provide the secure services. There are inherent costs and limitations to server security models, which is why it was deemed critical to create a local secure execution environment as a pre-requisite to enabling a trusted client. Hardware is widely acknowledged to be vastly more secure then software, and is required to provide certain features such as local electronic money.

A security co-processor named EMBASSY<sup>™</sup> anchors our secure execution environment. The EMBASSY device is a 32 bit ARM processor with electronic funds, clock, public key (PKI) and 3DES cryptographic support and accelerators, random number generator, tamper resistant hardware and design, flash memory, up to 32 MB of volatile memory, and a secure operating system. All aspects of processing, including key management, validation, authentication, permissioning, transaction, and decryption functions are performed within the secure environment, with no data or process exposed in an insecure manner in the PCs memory, bus, or peripherals.

The EMBASSY Device is a platform independent coprocessor intended to be attached as a peripheral or embedded within computer systems, PDAs, cell phones, Internet appliances or set-top-boxes. It provides interfaces for smart card readers, biometric devices, keyboards and displays for implementing secure login, secure input and secure output.

Unlike most available hardware security devices, such as traditional CA hardware, EMBASSY is a flexible device that executes secure ‘applets’ to provide its high level functions. Applets are small programs, suitable to being broadcast or downloaded from the Internet. They can also be pieces of other programs, where the piece provides a critical function that needs to operate securely. Each applet is secured by a trust authority against tampering, via a digital signature that is validated as part of the EMBASSY operating systems load function. Upon loading an applet, EMBASSY appears to be an application specific security processor.
Platform security can be initialized by a secure boot function, whereby digital signatures are used to validate that the PC BIOS has not been tampered with, and to provide for the secure update [flashing] of the BIOS to adjust platform features or correct problems. The general architecture of EMBASSY is displayed in Figure 4, where this [optional] feature is incorporated. Secure boot provides protection against BIOS virus attacks, allows for secure managed upgrades of the PC, creates a stronger “root” of trust within the system, and also allows a service provider to authorize and provision services based upon some criterion, such as whether the consumer has paid their bill.

A second component of platform security is the augmenting of security for other devices, such as providing key management by acting as a secure key server to local devices. One of the PC applets currently under development is a MS CAPI [Microsoft Crypto API] application, allowing devices to execute both symmetric and public key algorithms and related higher order functions through a PC industry standard interface using a local client resident server.

Another example of augmented platform security is a keyboard smart card reader, whereby an EMBASSY device embedded in a secured keyboard, through which a PIN is entered, enables digital cash to be downloaded from the Internet into a smart card that has been inserted into the reader.

Figure 4: EMBASSY Architecture
A third type of platform security is providing application security, by using the EMBASSY device to authorize the execution of the application and authenticating the application user. Home banking applications, for example, benefit from this type of security. A single platform or application sign on is provided to a user, authenticated by the presence of the EMBASSY device and their PIN. Each service provider creates their own relationship using a service specific user identifier that is not exposed outside the EMBASSY device, and therefore prevents service providers from sharing user information without permission.

Network security is generally provided by protocols such as SSL or IPSEC. While these are widely implemented and capable protocols, they are reliant upon both the client and the server being secured by the policies and procedures of their administrators. The tremendous empirical evidence that even well managed sites are vulnerable to compromise is a key impediment to user adoption and trust of Internet services, and the implementation of the next generation of services that is being made possible by new technologies.

The ability to authenticate the identity of a registered client securely is an example of a simple but extremely important function that the EMBASSY device can provide. A secure server side publishing system generates a unique secure token, published for a specific known client as part of a challenge-response interrogation. The ability of the client to use their PIN to decrypt the message and return the secure token is an effective form of authentication. If the decryption of that token requires a payment to be made by the consumer, the ability of the consumer to present that token back to the service provider verifies that the local purchase has been made.

In conjunction with the broadcast of an advertisement, or the datacast of a HDTV quality multimedia catalogue, a secure, private, and convenient shopping experience has now been created. A merchant does not need to know anything about the customer except the order and the shipping information, since they can verify that they have already been paid. The customer does not need to enter credit card information or provide personal identifying information such as phone number, and the browsing of the shopping catalogue is quick and convenient because it was already datacast.

Content security encompasses the protection during distribution, authorization to process it, license rule execution, persistent protection, local distribution, and digital watermarking. Content for a broadcast network is protected under a global key, though the EMBASSY architecture allows content providers to publish under as many keys as they choose. For symmetrically keyed content, the decryption process allows the client to possess a client specific decryption key. This requires the client specific keys to be broadcast out, or the client to connect to the Internet briefly, when publishers change their keys and clients wish to purchase their content. In return, this method prevents a single point of failure in the security network, such as occurred when the North America key for DVD protection was hacked and published on the Internet. In practice, users are rarely inconvenienced by this as the high level of hardware security and the client keyed basis of the EMBASSY system alleviates the need for publishers to change their keys on a frequent basis.
For a general purpose datacast system, it is advantageous to support multiple methods of protecting content, since independent content providers have different requirements. The most traditional form of security is CA, which protects a data stream in a binary (authorized/unauthorized) manner. While this works to provide basic subscription functionality for streaming content, such as a cable movie channel, it does not provide the capabilities or flexibility necessary for datacast services. In the digital age, there are many other types of content that need protection, such as music, electronic books, software programs, computer games, and interactive television programs. For a datacast system to achieve its full potential, it is critical that it address content protection issues for all types of content it could be asked to deliver.

An active area of content protection for this digital age has developed under the moniker Digital Rights Management (DRM). There are a number of DRM systems available, with each supporting a unique feature set and architecture but generally trying to address the breadth of issues involved in protecting both the content provider and users rights. No DRM systems are currently available for the PC platform that do not rely on software entirely for their implementation. This creates a serious security breach, because a software system is unable to hide “secrets” in the unprotected PC platform in a way that a determined hacker could not discover. The most critical of these areas is the storage and application of keys, the necessary components of any cryptography system.

Using the hardware key management available, the EMBASSY device provides a metering applet that allows for a superset of CA systems to be built. The most important advantages of this applet are the addition of a payment system and the execution of rules to determine the licensing available for content. Through the metering applet, rules such as content rental or rent-to-own can be enabled. We have developed a Java scriptable interface to the application that allows content providers to securely embed digital content into their interactive programming. The execution of the content, its licensing, payment, and user authorization is fully automated for the content provider, such that they can incorporate the secure content from standard web pages.

We have also developed methods of securing files that need to be locally streamed, such as video files, using the metering application. In this case, the file is prepared using tools that scramble the file. To play the file, a transaction occurs [which may be zero cost] that opens a decrypt channel though which the file is streamed. In the absence of the EMBASSY device, the player will open and play the video file, but it will display as video noise, with optional [but intentional] perfect sound.

User Security at a minimum must address how a user accesses functions of the system, prevents others from accessing those functions unless authorized, and protects user data and privacy. The EMBASSY device provides standard username/password binding, where the password is verified within the device. Optional interfaces allow for higher security, such as combining username/password with biometric identification.

A secure keyboard has been built for Cyber-COMM, the French banking consortium, that is FinRead level 5 [highest level] certified. This keyboard incorporates a secure display and secure keypad under control of the EMBASSY device. The keyboard is necessary to prevent the interception of a password (or the playback of a password by a virus). The secure display ensures that a charge cannot be made (by a web site, for instance) with a price different then the one displayed to the user.

Prototype biometric keyboards have been built as well, though cost and false positive/false negative issues remain that may keep this technology out of mainstream usage for the coming year.
The EMBASSY device can be used to protect data just as it does content, and a scriptable API (Java Script) has been created that allows applications to control this function. The XNS applet will provide an easy mechanism for a service provider to implement privacy functions in line with their policy.

5. Future Direction

There are many initiatives underway, both by Wavexpress and a variety of partner companies. Some of the most important that will be incorporated into our datacast offering are discussed below.

For end-to-end content security on the client, both the player and the end point [e.g.: display, speakers] must be secure. There are a number of important initiatives in both of these directions that will be incorporated as they become available.

We are working on incorporating a variety of industry accepted content protection mechanisms to use the EMBASSY device. For example, an applet supporting InterTrust, a popular and sophisticated DRM, is being developed.

Another applet under development implements XNS, an open standard for privacy and digital contracts built upon XML and incorporating the W3C P3P privacy policies. This application will make it simple for users to manage their data and permissions to third parties using industry-supported methods.

Enhancements to the security of the metering content protection are being made. The most important enhancement is key transmutation, allowing for content to be re-keyed locally within the hardware from a global publisher key to a client specific one, substantially improving the security between the EMBASSY device and the player. This is an important issue on PC platforms, where players are implemented in software in an insecure environment. While the EMBASSY architecture already provides this localization for a specific content publisher and each of their key hierarchies, this goes further by keying every piece of content to that client. Were that client specific key to be compromised, the hacker would be unable to publish that key to allow other users to view that specific content. They would still have to ship the entire hacked file to other users, which is a substantial barrier for large files such as movies or games.

Industry initiatives such as HDCP are also underway to secure the connection between client components, such as video cards and displays. This will provide a true end-to-end solution for content protection.

The security of peer-to-peer communications can be assured by implementing a peer-to-peer Virtual Private Network [VPN] using the EMBASSY device. We are working to incorporate an implementation of this solution into our client software.

Users residing at the same household have security and privacy concerns as well, and it is necessary to be able to create profiles that control access, security, and privacy. For example, a parent may want to create a profile for their children, where an allowance is granted, with allowable content rating guidelines (G, PG, PG-13) attached. While this type of functionality has not been widely used by consumers in TV, it is anticipated to be more popular in the datacast environment where money may be spent.

Our client currently is available on a Windows PC platform, and work is underway to create a number of Set Top Boxes incorporating our architecture and solutions.
6. Summary

Data broadcasting offers a remarkable opportunity to industry and consumers alike. While many challenges must be addressed, it has tremendous potential to extend the Internet, whether for dial up or broadband connected users. Datacast, if implemented and secured properly, can address all of the shortcomings inherent in using Internet for mass-market content distribution.

Wavexpress has worked to address end-to-end datacast challenges, with a particular emphasis on what we believe are the most difficult, yet most important, aspects of this challenge. For users to want these services, they must receive a rich experience that encompasses the breadth of content types, assembled in compelling ways. They must also have a convenient experience and a high degree of trust in the service and application provider.

For content and service providers to offer a complete service, they must be assured that their products will be protected and their customers will pay for the services provided. They also want mechanisms to reduce the operational costs of running their services, and to provide maximum flexibility in the business models they can offer.