Network Working Group
Internet-Draft
Intended status: Informational
Expires: November 13, 2019

P. Hallam-Baker
May 12, 2019

Business Models for Content Aggregation
draft-hallambaker-iab-aggregation-00

Abstract

This document is also available online at http://mathmesh.com/Documents/draft-hallambaker-iab-aggregation.html [1] .

Table of Contents

1. Where the Web failed

Many if not most technologies that came to define the era in which they were created owe a large part of their success to the failed expectations of the technologies that immediately preceded them. The telegraph and canals demonstrated the potential, but radio and the railways defined their age. The World Wide Web was fortunate to arrive at the exact moment that home trials of Interactive TV had shown it to be an expensive flop.

Apart from the name, the only part of Interactive TV that was 'interactive' was the ability to buy branded merchandise associated with a program. Interactive TV did little more than add a 'purchase' button to the remote control. The Web in contrast offered much more because any user of the Web could become a content provider.

It is with no little irony therefore that thirty years later, the Web has largely become the thing it was meant to destroy and a large part of the reason we have come to this point is the lack of a 'purchase' button on the remote control.

1.1. How users pay for content

Producing high quality content is an expensive business. The question therefore is not whether users will pay for content but rather how they will pay for content. They can pay directly, they

can pay by giving their attention, they can pay by giving up information they own but they will pay one way or another.

At the time the Web was begun, the dominant business model for television was paid advertising and so it was perhaps natural that the early evolution of the Web followed this model. This choice was not for want of consideration of other choices, proposals for Web micropayments were made as early as 1993 and presented in technical form in 1995. But advertising was the model understood by the established content providers and so advertising was the business model that they assumed they would eventually turn to when it finally came time to monetize the audiences they were developing. The HTTP referer field was originally introduced as a means of supporting advertising through a performance-based model before the addition of client-state (cookies) to the protocol.

In the event of course, the Web cannibalized classified advertising and many of the other revenue streams that established content providers had built their business on. By the time the need to monetize was understood it was too late to develop new protocols or infrastructures to support new business models. Having trained Web users to expect that content is free, many content providers turned to increasingly aggressive advertising presentations. Even today it is not unusual to find Web site designs that leave the user trying to read articles a few sentences at a time on a screen where 90% of the pixels are occupied by advertising.

The crucial flaw that the content providers did not anticipate is that content discovery is a vastly more attractive platform for advertisers than content provision. Web search engine providers offer a predictable, verifiable return on an advertising investment that can be tightly focused to specific audiences. Few content providers can compete and even those that can are at a disadvantage because click-fraud and other scams are rife in the content provider advertising market.

1.2. Concentration and its Consequences

According to the Interactive Advertising Bureau, online advertising saw a 22% year on year growth in 2018 [iab-avertising-2019] . As in previous years, the headline numbers show great potential, but the details show a market that is dysfunctional and ultimately unsustainable. Ten companies account for three quarters of all the advertising revenues in 2018 and desktop revenues are actually declining. Examination of the earnings reports of Facebook and Google over the same period indicate that the concentration is even more pronounced, and that content discovery is responsible for the

majority of advertising revenues and this portion is rising while revenues for content providers are flat or falling.

While the current situation is certainly good for the dominant content discovery services in short term, it is clearly unsustainable. Content discovery is worthless unless there is content to be discovered.

Whether this dysfunction in the market is ultimately resolved through regulatory action, technical changes or both, it is clear that change is inevitable. Nor are the opinions of one particular legislation in one particular country constrained by one particular ideology going to be dispositive in this regard. The Web is a global infrastructure and is regulated as such. The deployment of GDPR in the EU has proved that regulatory arbitrage works in both directions and especially so when control is concentrated in a small number of enterprises.

1.3. User experience

When Cascading Style Sheets were first proposed in 1994, the design goal was to enable users to control the presentation of information to best suit their needs. Needless to say, this goal is long since forgotten as the user has been transformed from customer to product.

This conception of user-as-product is most apparent in the design of social media properties such as Facebook where the ability of the user to interact is ruthlessly constrained. Users are given the absolute bare minimum of control over their environment possible so as to maintain the illusion of participation.

Limiting the modes of user interaction was probably one of the essential innovations required for social media to scale before users were used to the modality. But is it necessary now? When social media was new to most users, an environment that only allowed favorable responses to posts provided a welcoming impression. Today it means that there is no tool I can use to tell facebook that I do not wish to see material that is bigoted, ignorant or intentionally misleading unless the material is so egregious as to merit a report.

The core failure here is that the Web only allows Web designers to create compelling user experiences for their users. The Web does not allow users to create compelling user experiences for themselves.

1.4. The wider context

IETF Working Groups are traditionally established with a charter focused on a scope that is as narrowly focused as possible so as to minimize both the time taken to arrive at consensus and the implementation burden. While well intentioned, it is important to recognize that narrowing the problem scope necessarily reduces the incentives for early adopters.

One of the chief difficulties in developing any new Web technology is that the incumbent technology and content providers are focused on serving a global market of several billion users. New technologies are of little interest unless they provide immediate access to millions of users at the very least. It is useful therefore to consider non-commercial applications with similar requirements and in particular specialist applications serving small communities that may be highly motivated to deploy.

One area that is currently poorly served is the basis for most IETF work: mailing lists. While mailing lists represented the pinnacle of technology in the 1980s, they are long past their prime. Every member of a mailing list receives a copy of every message on every one of their devices that reads mail through a dedicated MUA. The affordances for subscribing to (and unsubscribing!) from mailing lists are ad hoc contrivances and there is no support for end-to-end security with respect to either confidentiality or integrity.

Another area that is underserved is bulletin boards and forums. One of the reasons that social media has become highly concentrated is that bulletin boards represent isolated islands which many users only ever encounter by chance. It is unlikely many people would discover that a site called Dewback Wing is the place to find plans for building an copy of the original Enterprise Captain’s Chair unless someone who already knew this told them. It is highly unlikely many people would know that such a guide even existed.

2. The Technology Gap

That the Web does not provide an ideal user experience for users is proved by the fact that most major content providers have developed special purpose mobile apps to view the content they provide. Such apps allow the content provider to control every aspect of the presentation of the content to the user but rarely provide much if any incentive for the user. Randall Monroe’s summary of the user proposition is still accurate: "Want to visit an incomplete version of our Web site where you can’t zoom? Download our app!".

Equally problematic is the fact that few mobile apps support hypertext linking and those that do rarely refer the user to the corresponding mobile app if installed. So, despite the fact that most mobile apps are merely a thin veneer on a captive browser, they are a dead end as far as the network hypertext model goes.

One of the few benefits that some mobile apps provide is the ability to read content in offline mode. But this is rarely implemented in

2.1. Content Interaction

One of the core technology advances that is implicit in the workshop scope is the development of a generic application that serves as a reader for aggregate content. For the purposes of discussion, it is assumed such an application would be separate from but tightly coupled to Web and News clients and share the same library foundations.

Such a client should provide for user interaction and not just passive consumption of content and should put the user in direct control of their user experience selecting the information sources and the filtering criteria for content delivery.

It is important to remember that just as Facebook is merely USENET on steroids, the next major advance in social networking might be merely a new twist on an old theme.

For example, shared bookmarking has been explored in the past but is currently in abeyance. Let us imagine that Alice, Bob and a few thousand close friends use a browser that allows them to bookmark Web pages as they view and nominate pages of interest (with optional annotations). The users might make their trails publicly visible or limit distribution through access control. The curated feeds generated through such a system might in turn be read by a separate constituency of curators who would use them to predict content that their subscribers might be interested in on the basis of their trails.

This model is very close to what we see in social media today but with one crucial difference: the user chooses their feed curators and can switch at any time. This might be a step towards restoring the balance between content provision and content discovery since users can subscribe to multiple curations of their feeds and drop those which provide too little that is of interest or too much that is objectionable.

2.2. Payments

The biggest gap in current Web technology is that payment for content is largely limited to supporter and subscription models. This provides a viable business proposition for content providers offering material important enough to be worth $30 a year or more. But there is little support for the far more numerous content providers publishing individual articles.

Credit card payment for individual articles disrupts the user experience. But payment systems that are too seamless become rife with fraud as the situation with premium rate telephone calling demonstrates.

One mechanism that might grow the market for paid content is a model in which subscribers to one content provider would receive no-cost access to normally paid content on other sites with a system of settlements to share revenues. For example, Alice subscribes to Bob’s Boy-Band fanzine which has a link to an article on Carol’s Concert Club reviewing the band. Since she is a subscriber to BBB, Alice doesn’t need to pay to view the article, but Carol receives a small settlement from Bob.

The precise details of the settlements system can probably be left to market forces, provided that the technology provides the necessary information and security controls.

3. Mathematical Mesh

The Mathematical Mesh is a cryptographic infrastructure designed to make the Internet easier to use by making it more secure.

Many if not most of the frustrations users suffer when using Internet applications today can be traced back to use of security systems that are poorly designed and woefully implemented. Passwords are difficult and expensive for users to use at the best of times.

Correctly applied, public key cryptography offers the highest level of practical security with no compulsory impact on the user experience. A security protocol that requires user effort is a protocol that isn’t going to be used. A security protocol should provide security without getting in the user’s way or demanding their attention. The only time when a security protocol should affect the user experience is when the user has a security concern at which point the application should provide the user with the information they need to make a security decision in a form they can understand.

Like the Web, the Mesh is a collection of interdependent technologies, some of which are outside the scope of this workshop. The features of the Mesh that are relevant to the workshop scope include:

- The ability to provision keys to all the Mesh-enabled devices owned or controlled by the user. These include desktop, laptop, mobile and IoT devices.

- The ability to share 'catalogs' comprising sets of data entries between devices. These include catalogs of bookmarks, passwords and calendar items.

- A cryptographic container format that may be used as either an archive format or as a syndication format.

- A end-to-end secure infrastructure for short messages.

Realizing these capabilities securely requires the use of cryptographic techniques not currently supported by OpenPGP [RFC4880] or CMS [RFC5652] . Rather than attempting to construct end-to-end security guarantees as a layer on top of an application protocol (e.g. S/MIME over SMTP), the Mesh is built on a presentation layer (DARE) that provides end-to-end security by default.

The academic field of cryptography has grown exponentially as a result of the Web and as a result of the market for commercial cryptography. But the cryptographic repertoire employed in IETF protocols remains unchanged since the closure of the PEM working group. We have improved signature, digest and encryption algorithms and we have formalized the definition of key wrapping and key derivation. But we do not use any new cryptographic primitives beyond the original canon.

Moving from one key cryptography to two revolutionized the information security field. Use of separate keys for encryption and decryption enables the encryption role to be separated from the decryption role. The Mesh makes use of public key protocols that make use of three keys and more.

The Mesh enforces cryptographic hygiene making use of separate keys for separate purposes and for separate applications and for separate devices. This results in a lot of keys but the consistency of requiring every system to apply a common set of best practices affords the simplicity necessary to make the system practical.

3.1. Management of private keys across devices

The core of the Mesh is the ability to securely manage sets of cryptographic keys across multiple devices with minimal user interaction. Almost every well-formed information security problem has a simple cryptographic solution provided that every device belonging to a user has a unique public key pair and the public keys belonging to the devices are known.

The chief obstacle to using public key-based authentication in place of password credentials is that while every device that a user might use to surf the Web has an affordance for password entry, almost none allow entry of a private key. Nor is this likely to change as devices become smaller and less likely to provide a standardized means of introducing a smart card or token.

The Mesh provides a personal PKI which allows the user to provision device-specific authentication credentials to every device they 'connect' to their personal Mesh. This is combined with an end-to-end secure password manager which permits devices connected to a personal Mesh to access the user's legacy credentials.

Public key pairs are provisioned in the Mesh using a co-generation approach based on work by Matt Blaze and Torben Pedersen. Every device has a unique set of device key pairs that are either generated on the device itself or provisioned during manufacture. When a device is connected to a user's profile, a second set of key pairs is generated by the user's administration device. It is the combination of the two sets of keys that is used to perform every Mesh function on the device. This provides protection against a single point of failure.

3.2. Dare Container

Data At Rest Encryption [draft-hallambaker-mesh-dare] is a cryptographic message syntax based on JSON/JOSE that provides a set of capabilities that may be loosely described as 'blockchain with encryption'. As with Certificate Transparency [RFC6962] , incremental integrity checking may be provided by a Merkle Tree. Incremental encryption is also supported allowing a single key exchange to be applied to multiple container entries by means of a uniquely salted Key Derivation Function [RFC5869]

Dare Container is used within the Mesh to support creation of catalogs (which contain sets of items) and spools (which contain queues of messages). The features it supports are also well suited for use as a syndication format or an archive format.

There are clear advantages to employing an archive format designed to support encryption and authentication. The Dare format allows large numbers of entries of any size (up to 2^63 bytes) to be encrypted under a single public key exchange and authenticated by means of a single signature. Furthermore, containers may be redacted to drop entries that are irrelevant or have been updated without affecting confidentiality or integrity.

This approach allows the same technology to be applied to package as a single file:

- A Web page consisting of a base HTML document, CSS style sheets, scripts and transcluded images.

- A Web site consisting of multiple base HTML documents referencing a shared set of images and scripts.

- Entries in a discussion on a Web page.

Furthermore, containers may be aggregated or redacted as required. A container describing an individual page may be extracted from a container describing a site and containers describing multiple pages may be combined to form a site.

3.3. Creator-to-consumer end-to-end Web security.

Since the release of TLS in 1994, Web security has focused on securing data in transit. HTTPS is used to protect the provisioning of new content to Web servers and for distribution of the content from the Web server to the reader. But the content itself sits in the clear in the cloud. As a result, almost every disclosure breach is a breach of data at rest.

The Mesh provides true Data At Rest security by applying key splitting techniques to the private key used to decrypt data. As with existing CRM schemes, these techniques allow an administrator to grant or remove access privileges to data stored on a remote server. Unlike existing techniques, no decryption keys are stored on the server itself. A breach of the server only results in disclosure of encrypted data and some random numbers.

3.4. Deployment strategy

The first stage in that strategy is focused on applications that deliver value to individual users even if there are no other users of the Mesh. Management of credentials and keys across multiple devices is such an application. Management of usernames and passwords is tedious for everyone. Commercial password managers are expensive and

currently offer vague security guarantees at best. The Mesh is an open specification that offers true end-to-end security with seamless ease of use. Management of OpenPGP, S/MIME and SSH keys pose similar challenges. While every system manager uses SSH it is a very rare administrator who bothers to generate separate keypairs for each of their devices and even rarer that they delete device keys after a device is decommissioned.

The second stage is to focus on applications that deliver value to compact groups of users within a niche community. The CRM capabilities of the Mesh are likely to be of interest within enterprises focused on health care, defense and other industries where maintaining confidentiality is more important than direct interoperation with other enterprises. The Mesh also provides an improvement on traditional second factor authentication schemes which allows the relying party to ask for confirmation of specific actions for specific purposes and for a non-repudiable audit trail of every interaction to be maintained.

The final stage of the deployment strategy is to join up the communities of users established in phase two to form a sufficient critical mass to change the Internet as a whole.

3.5. Shared Bookmarks

The shared bookmarks environment described in this paper is a part of the second phase of the Mesh deployment strategy. A large part of the value proposition offered by Facebook to users is the ability to share links to Web content and to comment on them.

The Mesh allows bookmarks to be shared and commented on within closed groups of users such as a group of employees within a company or researchers within a field.

While existing social media allows users to establish closed groups, ownership of those groups ultimately rests with the social media platform and not the members of the groups themselves. Vesting ownership of the group in its members allows the membership to have control over the selection of administrators and moderators and the criteria for posting and admission to the group.

Furthermore, selection of articles to view may be made by each individual member using the tools and platforms of their choice that best serve their needs.

The content that is prioritized on such platforms today is the content that maximizes engagement and mouse clicks. The hatemonger,

the crank and the disinformation warrior are chosen because their lies generate more engagement than facts or expert opinion.

4. References

4.1. Informative References

[draft-hallambaker-mesh-dare]
Hallam-Baker, P., "Mathematical Mesh Part III : Data At Rest Encryption (DARE)", draft-hallambaker-mesh-dare-01 (work in progress), April 2019.

[iab-avertising-2019]
"[Reference Not Found!]".

[RFC4880] Callas, J., Donnerhacke, L., Finney, H., Shaw, D., and R. Thayer, "OpenPGP Message Format", RFC 4880, DOI 10.17487/RFC4880, November 2007.

[RFC5652] Housley, R., "Cryptographic Message Syntax (CMS)", STD 70, RFC 5652, DOI 10.17487/RFC5652, September 2009.

[RFC5869] Krawczyk, H. and P. Eronen, "HMAC-based Extract-and-Expand Key Derivation Function (HKDF)", RFC 5869, DOI 10.17487/RFC5869, May 2010.

[RFC6962] Laurie, B., Langley, A., and E. Kasper, "Certificate Transparency", RFC 6962, DOI 10.17487/RFC6962, June 2013.

4.2. URIs

[1] http://mathmesh.com/Documents/draft-hallambaker-iab-aggregation.html

Author's Address

Phillip Hallam-Baker

Email: phill@hallambaker.com