Preventing Data Leakage in Web Services

by

Frank Yi-Fei Wang

B.S., Stanford University (2012)
S.M., Massachusetts Institute of Technology (2016)

Submitted to the Department of Electrical Engineering and Computer Science
in partial fulfillment of the requirements for the degree of

Doctor of Philosophy in Computer Science

at the

MASSACHUSETTS INSTITUTE OF TECHNOLOGY

September 2018

Signature redacted

Author .....
Department of Electrical Engineering and Computer Science
July 26, 2018

Signature redacted

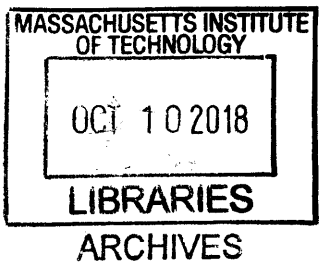
Certified by .....
Nickolai Zeldovich
Professor of Electrical Engineering and Computer Science
Thesis Supervisor

Signature redacted

Certified by .....
James Mickens
Associate Professor of Computer Science at Harvard University
Thesis Supervisor

Signature redacted

Accepted by .....
Leslie A. Kolodziejski
Professor of Electrical Engineering and Computer Science
Chair, Department Committee on Graduate Students



Preventing Data Leakage in Web Services

by

Frank Yi-Fei Wang

Submitted to the Department of Electrical Engineering and Computer Science
on July 26, 2018, in partial fulfillment of the
requirements for the degree of
Doctor of Philosophy in Computer Science

Abstract

Web services like Google, Facebook, and Dropbox are a regular part of users' lives. However, using these applications can cause sensitive data leakage both on the server and client. On the server-side, applications collect and analyze sensitive user data to monetize it. Consequently, this sensitive data can leak through data breaches or can be accessed by malicious service providers. On the client, when a user accesses a web service through the browser, sensitive user information may leak outside of the browser, e.g., to DNS interfaces or the swap space. An attacker who accesses the user device after a session has terminated can view this information.

This dissertation presents two practical, secure systems, Veil and Splinter, that prevent some of this data leakage. Veil minimizes client-side information leakage from the browser by allowing web application developers to enforce stronger private browsing semantics without browser support. Splinter allows the server to properly respond to a user query without the server learning any sensitive information present in the query.

Thesis Supervisor: Nickolai Zeldovich
Title: Professor of Electrical Engineering and Computer Science

Thesis Supervisor: James Mickens
Title: Associate Professor of Computer Science at Harvard University

Acknowledgments

I have many people to thank in this dissertation. It's been a long journey, but I've met and learned from so many awesome people along the way. It goes without saying that this dissertation was the result of work and mentorship from many people.

First and foremost, I want to thank my advisors, Nickolai Zeldovich and James Mickens. I've learned so much from the both of them along the way. I want to thank them for providing me the independence and support to work on ideas that I thought were interesting.

Next, I want to thank my collaborators, Vinod Vaikuntanathan, Shafi Goldwasser, Matei Zaharia, and Catherine Yun. I also want to thank my research family at MIT, specifically Jen Gong, Amy Zhao, Amy Ousterhout, Tej Chajed, Guha Balakrishnan, Jon Gjenset, David Lazar, Taesoo Kim, Xi Wang, Haogong Chen, Neha Narula, Ravi Netravali, Silas Boyd-Wickizer, Jean Yang, and everyone else in the PDOS group. I've learned a lot from you, and you made my time at MIT very enjoyable.

I want to thank my friends who have provided me great advice and support along the way. I want to thank everyone I met at Rough Draft Ventures, all the mentors at Highland Capital and Cybersecurity Factory, and my friends in Sidney Pacific. Your friendship has allowed me to stay grounded during my PhD.

Finally, I want to thank my parents for allowing me to live on a different coast for the past six years. They have always been supportive of my life choices and adventures.

* * *

This work was partially supported by an NSF Graduate Research Fellowship (Grant No. 2013135952) and by NSF awards CNS-1053143, CNS-1413920, CNS-1350619, and CNS-1414119.

The dissertation incorporates and extends work published in the following papers:

> Frank Wang, James Mickens, and Nickolai Zeldovich. Veil: Private Browsing Semantics Without Browser-side Assistance. In *Proceedings of Network and Distributed System Security Symposium (NDSS)*, 2018.
>
> Frank Wang, Catherine Yun, Shafi Goldwasser, Vinod Vaikuntanathan, and Matei Zaharia. Splinter: Practical Private Queries on Public Data. In *Proceedings of Networked Systems Design and Implementation (NSDI)*, 2017.

Contents

Figures and tables

ONE

Introduction

1.1 Motivation

Consumers are increasing their usage of web services. Whenever users interact with these applications, the web service collects their data, which can contain sensitive information, such as their medical conditions, political preferences, and income [77, 78]. Unfortunately, this data can leak through numerous channels on both the server and client. As web systems become more complex, the number of these channels continues to grow. Not only is there more data but also the number of applications that handle and access this data is growing. Here are some examples of the data leakage. On the server side, data can leak through breaches or be accessed by malicious service administrators. On the client side, sensitive user information can leak from the browser whenever a user accesses a web application. These scenarios raise an important question: how do we build practical, secure mechanisms to prevent this data leakage?

Much research has focused on building systems [34, 61, 96, 97] that protect sensitive user data stored in web application databases or cloud providers from leaking as a result of data breaches or malicious service providers. However, the focus of this dissertation is different. We are not protecting sensitive user data that already exists on the server. Instead, we build systems that prevent data leakage on the client (Veil), specifically from the browser, and that protect sensitive data in queries (Splinter). In the section below, we provide an overview of these two systems.

1.2 Our Systems

1.2.1 Veil: Private Browsing Semantics without Browser-side Assistance

All popular web browsers offer a "private browsing mode." After a private session terminates, the browser is supposed to remove client-side evidence that the session occurred. Unfortunately, browsers still leak information through the file system, the browser cache, the DNS cache, and on-disk reflections of RAM such as the swap file.

Veil is a new deployment framework that allows web developers to prevent these information leaks, or at least reduce their likelihood. Veil leverages the fact that, even though developers do not control the client-side browser implementation, developers do control 1) the content that is sent to those browsers, and 2) the servers which deliver that content. Veil-enabled web sites collectively store their content on Veil's *blinding servers* instead of on individual, site-specific servers. To publish a new page, developers pass their HTML, CSS, and JavaScript files to Veil's compiler; the compiler transforms the URLs in the content so that, when the page loads on a user's browser, URLs are derived from a secret user key. The blinding service and the Veil-enabled page exchange encrypted data that is also protected by the user's key. The result is that Veil pages can safely store encrypted content in the browser cache; furthermore, the URLs exposed to system interfaces like the DNS cache are unintelligible to attackers who do not possess the user's key. To protect against post-session inspection of swap file artifacts, Veil uses heap walking (which minimizes the likelihood that secret data is paged out), content mutation (which garbles in-memory artifacts if they do get swapped out), and DOM hiding (which prevents the browser from learning site-specific HTML, CSS, and JavaScript content in the first place). Veil-enabled pages load on unmodified commodity browsers, allowing developers to provide stronger semantics for private browsing without forcing users to install or reconfigure their machines. Veil provides these guarantees even if the user does not visit a page using a browser's native privacy mode.

1.2.2 Splinter: Practical, Private Web Application Queries

Many online services let users and businesses query datasets such as maps, flight prices, patents, and medical information. The datasets themselves do not contain sensitive information, but unfortunately, queries on these datasets can reveal sensitive information. This dissertation presents Splinter, a system that protects queries and scales to realistic applications. A user splits her query into multiple parts and sends each part to a different provider that holds a copy of the data. As long as any one of the providers does not collude with the others, the providers cannot determine the query. Splinter uses and extends a new cryptographic primitive called Function Secret Sharing (FSS) that makes it more efficient than prior systems based on other cryptographic techniques such as Private Information Retrieval and garbled circuits. We develop protocols extending FSS to new types of queries, such as MAX and TOPK queries. We also provide an optimized implementation of FSS using AES-NI instructions and multicores. Splinter achieves end-to-end latencies below 1.6 seconds for realistic workloads including a Yelp clone, flight search, and map routing.

Two

Veil: Private Browsing Semantics without Browser-side Assistance

2.1 Motivation

Web browsers are the client-side execution platform for a variety of online services. Many of these services handle sensitive personal data like emails and financial transactions. Since a user's machine may be shared with other people, she may wish to establish a *private session* with a web site, such that the session leaves no persistent client-side state that can later be examined by a third party. Even if a site does not handle personally identifiable information, users may not want to leave evidence that a site was even visited. Thus, all popular browsers implement a private browsing mode which tries to remove artifacts like entries in the browser's "recently visited" URL list.

Unfortunately, implementations of private browsing mode still allow sensitive information to leak into persistent storage [3, 52, 65, 83]. Browsers use the file system or a SQLite database to temporarily store information associated with private sessions; this data is often incompletely deleted and zeroed-out when a private session terminates, allowing attackers to extract images and URLs from the session. During a private session, web page state can also be reflected from RAM into swap files and hibernation files; this state is in cleartext, and therefore easily analyzed by curious individuals who control a user's machine after her private browsing session has ended. Simple greps for keywords are often sufficient to reveal sensitive data [3, 52].

Web browsers are complicated platforms that are continually adding new features (and thus new ways for private information to leak). As a result, it is difficult to implement even seemingly straightforward approaches for strengthening a browser's implementation of incognito modes. For example, to prevent secrets in RAM from paging to disk, the browser could use OS interfaces like `mlock()` to pin memory pages. However, pinning may interfere in subtle ways with other memory-related functionality like garbage collecting or tab discarding [92]. Furthermore, the browser would have to use `mlock()` indiscriminately, on *all* of the RAM state belonging to a private session, because the

browser would have no way to determine which state in the session is actually sensitive, and which state can be safely exposed to the swap device.

In this dissertation, we introduce Veil, a system that allows web developers to implement private browsing semantics for their own pages. For example, the developers of a whisteblowing site can use Veil to reduce the likelihood that employers can find evidence of visits to the site on workplace machines. Veil's privacy-preserving mechanisms are enforced *without assistance from the browser*—even if users visit pages using a browser's built-in privacy mode, Veil provides stronger assurances that can only emerge from an intentional composition of HTML, CSS, and JavaScript. Veil leverages five techniques to protect privacy: URL blinding, content mutation, heap walking, DOM hiding, and state encryption.

- Developers pass their HTML and CSS files through Veil's compiler. The compiler locates cleartext URLs in the content, and transforms those raw URLs into *blinded references* that are derived from a user's secret key and are cryptographically unlinkable to the original URLs. The compiler also injects a runtime library into each page; this library interposes on dynamic content fetches (e.g., via `XMLHttpRequests`), and forces those requests to also use blinded references.

- The compiler uploads the objects in a web page to Veil's *blinding servers*. A user's browser downloads content from those blinding servers, and the servers collaborate with a page's JavaScript code to implement the blinded URL protocol. To protect the client-side memory artifacts belonging to a page, the blinding servers also *dynamically mutate* the HTML, CSS, and JavaScript in a page. Whenever a user fetches a page, the blinding servers create syntactically different (but semantically equivalent) versions of the page's content. This ensures that two different users of a page will each receive unique client-side representations of that page.

- Ideally, sensitive memory artifacts would never swap out in the first place. Veil allows developers to mark JavaScript state and renderer state as sensitive. Veil's compiler injects *heap walking code* to keep that state from swapping out. The code uses JavaScript reflection and forced DOM relayouts to periodically touch the memory pages that contain secret data. This coerces the OS's least-recently-used algorithm to keep the sensitive RAM pages in memory.

- Veil sites which desire the highest level of privacy can opt to use Veil's *DOM hiding* mode. In this mode, the client browser essentially acts as a dumb graphical terminal. Pages are rendered on a content provider's machine, with the browser sending user inputs to the machine via the blinding servers; the content provider's machine responds with new bitmaps that represent the updated view of the page.

Browsing mode	Persistent, per-site client-side storage	Information leaks through client-side, name-based interfaces	Per-site browser RAM artifacts	GUI interactions
Regular browsing	Yes (cleartext by default)	Yes	Yes	Locally processed
Regular incognito mode	No	Yes	Yes	Locally processed
Veil with encrypted client-side storage, mutated DOM content, heap walking	Yes (always encrypted)	No (blinding servers)	Yes (but mutated and heap-walked)	Locally processed
Veil with DOM hiding	No	No (blinding servers)	No	Remotely processed

Table 2-1: A comparison between Veil's two browsing modes, regular incognito browsing, and regular browsing that does not use incognito mode.

In DOM hiding mode, the page's unique HTML, CSS, and JavaScript content is never transmitted to the client browser.

- Veil also lets a page store private, persistent state by *encrypting* that state and by naming it with a blinded reference that only the user can generate.

By using blinded references for all content names (including those of top-level web pages), Veil avoids information leakage via client-side, name-centric interfaces like the DNS cache [35], the browser cache, and the browser's address bar. Encryption allows a Veil page [1] to safely leverage the browser cache to reduce page load times, or store user data across different sessions of the private web page. A page that desires the highest level of security will eschew even the encrypted cache, and use DOM hiding; in concert with URL blinding, the hiding of DOM content means that the page will generate *no greppable state in RAM or persistent storage* that could later be used to identify the page. Table 2-1 summarizes the different properties of Veil's two modes for private browsing.

In summary, **Veil is the first web framework that allows developers to implement privacy-preserving browsing semantics for their own pages.** These semantics are stronger than those provided by native in-browser incognito modes; however, Veil pages load on commodity browsers, and do not require users to reconfigure their systems or run their browsers within a special virtual machine [32]. Veil can translate legacy pages to more secure versions automatically, or with minimal developer assistance (§2.5), easing the barrier to deploying privacy-preserving sites. Experiments show that Veil's overheads are moderate: 1.25x–3.25x for Veil with encrypted client-side storage, mutated DOM content, and heap walking; and 1.2x–2.1x for Veil in DOM hiding mode.

2.2 Deployment Model

Veil uses an opt-in model, and is intended for web sites that want to actively protect client-side user privacy. For example, a whistleblowing site like SecureDrop [132] is incentivized to hide client-side evidence that the SecureDrop website has been visited;

[1] We use the term *Veil page* to refer to a Veil-enabled page in this dissertation.

strong private browsing protections give people confidence that visiting SecureDrop on a work machine will not lead to incriminating aftereffects. As another example of a site that is well-suited for Veil, consider a web page that allows teenagers to find mental health services. Teenagers who browse the web on their parents' machines will desire strong guarantees that the machines store no persistent records of private browsing activity.

Participating Veil sites must explicitly recompile their content using the Veil compiler. This requirement is not unduly burdensome, since all non-trivial frameworks for web development impose a developer-side workflow discipline. For example, Aurelia [18], CoffeeScript [25], and Meteor [70] typically require a compilation pass before content can go live. To handle dynamic content that results from personalization on a webpage, blinding servers can also help with the compilation process. We discuss this in more detail in Section 2.4.7.

Participating Veil sites must also explicitly serve their content from Veil blinding servers. Like Tor servers [29], Veil's blinding servers can be run by volunteers, although content providers can also contribute physical machines or VMs to the blinding pool (§2.4.2).

Today, many sites are indifferent towards the privacy implications of web browsing; other sites are interested in protecting privacy, but lack the technical skill to do so; and others are actively invested in using technology to hide sensitive user data. Veil targets the latter two groups of site operators. Those groups are currently in the minority, but they are growing. An increasing number of web services define their value in terms of privacy protections [31, 33, 98, 99], and recent events have increased popular awareness of privacy issues [91]. Thus, we believe that frameworks like Veil will become more prevalent as users demand more privacy, and site operators demand more tools to build privacy-respecting systems.

2.3 Threat Model

As described in Section 2.2, Veil assumes that a web service is actively interested in preserving its users' client-side privacy. Thus, Veil trusts web developers and the blinding servers. Veil's goal is to defend the user against local attackers who take control of a user's machine *after* a private session terminates. If an attacker has access to the machine *during* a private session, the attacker can directly extract sensitive data, e.g., via keystroke logging or by causing the browser to core dump; such exploits are out-of-scope for this dissertation.

Veil models the post-session attacker as a skilled system administrator who knows the location and purpose of the swap file, the browser cache, and files like `/var/log/*` that record network activity like DNS resolution requests. Such an attacker can use tools like

`grep` or `find` to look for hostnames, file types, or page content that was accessed during a Veil session. The attacker may also possess off-the-shelf forensics tools like Mandiant Redline [67] that look for traces of private browsing activity. However, the attacker lacks the skills to perform a customized, low-level forensics investigation that, e.g., tries to manually extract C++ data structures from browser memory pages that Veil could not prevent from swapping out.

Given this attacker model, Veil's security goals are weaker than strict forensic deniability [32]. However, Veil's weaker type of forensic resistance is both practically useful and, in many cases, the strongest guarantee that can be provided without forcing users to run browsers within special OSes or virtual machines. Veil's goal is to load pages within *unmodified* browsers that run atop *unmodified* operating systems. Thus, Veil is forced to implement privacy-preserving features using browser and OS interfaces that are unaware of Veil's privacy goals. These constraints make it impossible for Veil to provide strict forensic deniability. However, most post-session attackers (e.g., friends, or system administrators at work, Internet cafes, or libraries) will lack the technical expertise to launch FBI-style forensic investigations.

Using blinded URLs, Veil tries to prevent data leaks through system interfaces that use network names. Examples of name-based interfaces are the browser's "visited pages" history, the browser cache, cookies, and the DNS cache (which leaks the hostnames of the web servers that a browser contacts [3]). It is acceptable for the attacker to learn that a user has contacted Veil's blinding servers—those servers form a large pool whose hostnames are generic (e.g., `veil.io`) and do not reveal any information about particular Veil sites (§2.4.2).

Veil assumes that web developers only include trusted content that has gone through the Veil compiler. A page may embed third party content like a JavaScript library, but the Veil compiler analyzes both first party and third party content during compilation (§2.4.1). Veil also assumes that blinding servers do not maliciously modify content uploaded by the web developers.

Heap walking (§2.4.5) allows Veil to prevent sensitive RAM artifacts from swapping to disk. Veil does not try to stop information leaks from GPU RAM [58], but GPU RAM is never swapped to persistent storage. Poorly-written or malicious browser extensions that leak sensitive page data [59] are also outside the scope of this dissertation.

2.4 Design

As shown in Figure 2-2, the Veil framework consists of three components. The *compiler* transforms a normal web page into a new version that implements static and dynamic privacy protections. Web developers upload the compiler's output to *blinding servers*.

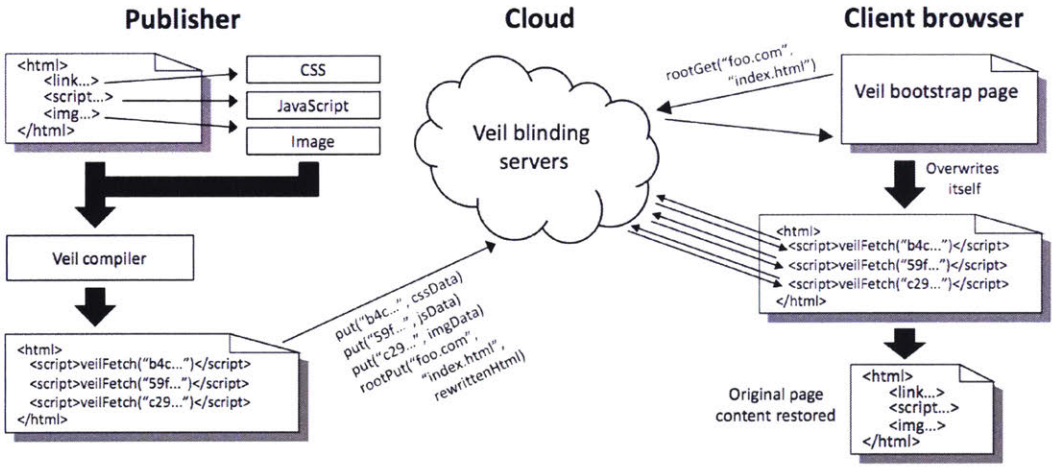


Figure 2-2: The Veil architecture (cryptographic operations omitted for clarity).

These servers act as intermediaries between content publishers and content users, encrypting content. To load the Veil page, a user first loads a small *bootstrap page*. The bootstrap asks for a per-user key and the URL of the Veil page to load; the bootstrap then downloads the appropriate objects from the blinding servers and dynamically overwrites itself with the privacy-preserving content in the target page.

In the remainder of this section, we describe Veil's architecture in more detail. Our initial discussion involves a simple, static web page that consists of an HTML file, a CSS file, a JavaScript file, and an image. We iteratively refine Veil's design to protect against various kinds of privacy leakage. Then, we describe how Veil handles more complex pages that dynamically fetch and generate new content.

2.4.1 The Veil Compiler and veilFetch()

The compiler processes the HTML in our example page (Figure 2-2), and finds references to three external objects (i.e., the CSS file, the JavaScript file, and the image). The compiler computes a hash value for each object, and then replaces the associated HTML tags with dynamic JavaScript loaders for the objects. For example, if the original image tag looked like this:

```
<img src="http://foo.com/img.jpg"/>
```

the compiler would replace that tag with the following:

```
<script>veilFetch("b6a0d...");</script>
```

where the argument to `veilFetch()` is the hash name of the image. At page load time, when `veilFetch()` runs, it uses an `XMLHttpRequest` request to download the appropriate object from the blinding service. In our example, the URL in the `XMLHttpRequest` might be `http://veil.io/b6a0d...`.

Such a URL resides in the domain of the blinding servers, not the domain of the original content publisher. Furthermore, the URL identifies the underlying object by hash, so the URL itself does not leak information about the original publisher or the data contained within the object. So, even though the execution of `veilFetch()` may pollute name-based interfaces like the DNS cache, a post-session attacker which inspects those registries cannot learn anything about the content that was fetched. However, a network-observing attacker who sees a `veilFetch()` URL can simply ask the blinding server for the associated content, and then directly inspect the data that the user accessed during the private session!

To defend against such an attack, Veil associates each user with a symmetric key k_{user} (we describe how this key is generated and stored in Section 2.4.4). Veil also associates the blinding service with a public/private keypair. When `veilFetch(hashName)` executes, it does not ask the blinding service for `hashName`—instead, it asks for <`hashName`>$_{k_{user}}$. In the HTTP header for the request, `veilFetch()` includes $< k_{user} >_{PubKeyBServ}$, i.e., the user's symmetric key encrypted by the blinding service's public key. When the blinding service receives the request, it uses its private key to decrypt $< k_{user} >_{PubKeyBServ}$. Then, it uses $< k_{user} >$ to extract the hash name of the requested object. The blinding service locates the object, encrypts it with k_{user}, and then sends the HTTP response back to the client. Figure 2-3 depicts the full protocol.[2] In practice, the blinding service's public/private keypair can be the service's TLS keypair, as used by HTTPS connections to the service. Thus, the encryption of k_{user} can be encrypted by the standard TLS mechanisms used by an HTTPS connection.

Once `veilFetch()` receives the response, it decrypts the data and then dynamically reconstructs the appropriate object, replacing the script tag that contained `veilFetch()` with the reconstructed object. The compiler represents each serialized object using JSON [26]; Figure 2-4 shows an example of a serialized image. To reinflate the image, `veilFetch()` extracts metadata like the image's width and height, and dynamically injects an image tag into the page which has the appropriate attributes. Then, `veilFetch()` extracts the Base64-encoded image data from the JSON, and sets the `src` attribute of the image tag to a data URL [68] which directly embeds the Base64 image data. This causes the browser to load the image. `veilFetch()` uses similar techniques to reinflate other content types.

This client-server protocol has several nice properties. First, it solves the replay problem—if an attacker wants to replay old fetches, or guess visited URLs (as in a CSS-

[2] A stateful blinding service can cache decrypted user keys and eliminate the public key operation from all but the user's first request.

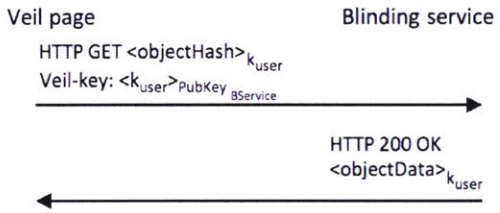


Figure 2-3: The `veilFetch()` protocol.

```
{"img_type": "jpeg",
"dataURI": "ab52f...",
"tag_attrs": {"width": "20px",
"height": "50px"}}
```

Figure 2-4: A serialized <`img`> tag.

based history attack [53, 126]), the attacker will not be able to decrypt the responses unless she has the user's key. Also, since the blinding service returns encrypted content, that encrypted content is what would reside in the browser cache. Thus, Veil pages can now persist data in the browser cache such that only the user can decrypt and inspect that content. Of course, a page does not have to use the browser cache—when a publisher uploads an object to the blinding service, the publisher indicates the caching headers that the service should return to clients.

In addition to uploading data objects like images to the blinding service, the compiler also uploads "root" objects. Root objects are simply top-level HTML files like `foo.com/index.html`. Root objects are signed with the publisher's private key, and are stored in a separate namespace from data objects using a 2-tuple key that consists of the publisher name (`foo.com`) and the HTML name (`index.html`). Unlike data objects, which are named by hash (and thus self-verifying), root objects change over time as the associated HTML evolves. Thus, root objects are signed by the publisher to guarantee authenticity and allow the blinding service to reject fraudulent updates.

2.4.2 The Blinding Service

In the previous section, we described the high-level operation of the blinding service. It exports a key/value interface to content publishers, and an HTTP interface to browsers. The HTTP code path does content encryption as described above. As described in Section 2.4.6, the blinding service also performs *content mutation* to protect RAM artifacts that spill to disk; mutation does not provide cryptographically strong protections, but it does significantly raise the difficulty of post-session forensics. The blinding servers also implement the DOM hiding protocol (§2.4.8), which Veil sites can use to prevent exposing *any* site-specific HTML, CSS, or JavaScript to client browsers.

The blinding service can be implemented in multiple ways, e.g., as a peer-to-peer distributed hash table [108, 115], a centralized service that is run by a trusted authority like the EFF, or even a single cloud VM that is paid for and operated by a single privacy-conscious user. In practice, we expect a blinding service to be run by an altruistic organization like the EFF, or by altruistic individuals (as in Tor [29]), or by a large set of privacy-preserving sites who will collaboratively pay for the cloud VMs that run the blinding servers. Throughout the dissertation, we refer to a single blinding service `veil.io` for convenience. However, independent entities can simultaneously run independent blinding services.

Veil's publisher-side protocol is compatible with accounting, since the blinding service knows which publisher uploaded each object, and how many times that object has been downloaded by clients. Thus, it is simple for a cloud-based blinding service to implement proportional VM billing, or cost-per-download billing. In contrast, an altruistic blinding service (e.g., implemented atop a peer-to-peer DHT [108, 115]) could host anonymous object submissions for free.

2.4.3 The Same-origin Policy

A single web page can aggregate content from a variety of different origins. As currently described, Veil maps all of these objects to a single origin: at compile time, Veil downloads the objects from their respective domains, and at page load time, Veil serves all of the objects from `https://veil.io`.

The browser uses the same-origin policy [109] to constrain the interactions between content from different origins. Mapping all content to a single origin would effectively disable same-origin security checks. Thus, Veil's static rewriter injects the `sandbox` attribute [94] into all `<iframe>` tags. Using this attribute, the rewriter forces the browser to give each frame a unique origin with respect to the same-origin policy. This means that, even though all frames are served from the `veil.io` domain, they cannot tamper with each other's JavaScript state. In our current implementation of the compiler, developers are responsible for ensuring that dynamically-generated frames are also tagged with the `sandbox` attribute; however, using DOM virtualization [51, 72], the compiler could inject DOM interpositioning code that automatically injects `sandbox` attributes into dynamically-generated frames.

DOM storage [124] exposes the local disk to JavaScript code using a key/value interface. DOM storage is partitioned by origin, i.e., a frame can only access the DOM storage of its own domain. By assigning an ephemeral, unique origin to each frame, Veil seemingly prevents an origin from reliably persisting data across multiple user sessions of a Veil page. To solve this problem, Veil uses indirection. When a frame wants to access DOM storage, it first creates a child frame which has the special URL `https://veil.io/domStorage`. The child frame provides Veil-mediated access to DOM storage, accepting read and write

requests from the parent frame via `postMessage()`. Veil associates a private storage area with a site's public key, and engages in a challenge/response protocol with a frame's content provider before agreeing to handle the frame's IO requests; the challenge/response traffic goes through the blinding servers (§2.4.7). The Veil frame that manages DOM storage employs the user's key to encrypt and integrity-protect data before writing it, ensuring that post-session attackers cannot extract useful information from DOM storage disk artifacts.

Since Veil assigns random, ephemeral origins to frames, cookies do not work in the standard way. To simulate persistent cookies, an origin must read or write values in DOM storage. Sending a cookie to a server also requires explicit action. For example, a Veil page which contains personalized content might use an initial piece of non-personalized JavaScript to find the local cookie and then generate a request for dynamic content (§2.4.7).

2.4.4 The Bootstrap Page

Before the user can visit any Veil sites, she must perform a one-time initialization step with the Veil bootstrap page (e.g., `https://veil.io`). The bootstrap page generates a private symmetric key for the user and places it in local DOM storage, protecting it with a user-chosen password. Veil protects the in-memory versions of the password and symmetric key with heap walking (§2.4.5) to prevent these cleartext secrets from paging to disk.

Later, the user determines the URL (e.g., `foo.com/index.html`) of a Veil site to load. The user should discover this URL via an already-known Veil page like a directory site, or via out-of-band mechanisms like a traditional web search on a different machine than the one needing protection against post-session attackers; looking for Veil sites using a traditional search engine on the target machine would pollute client-side state with greppable content. Once the user possesses the desired URL, she returns to the bootstrap page. The bootstrap prompts the user for her password, extracts her key from local storage, and decrypts it with the password. The bootstrap then prompts the user for the URL of the Veil page to visit. The bootstrap fetches the root object for the page. Then, the bootstrap overwrites itself with the HTML in the root object. Remember that this HTML is the output of the Veil compiler; thus, as the browser loads the HTML, the page will use `veilFetch()` to dynamically fetch and reinflate encrypted objects.

Once the bootstrap page overwrites itself, the user will see the target page. However, no navigation will have occurred, i.e., the browser's address bar will still say `https://veil.io`. Thus, the browser's history of visited pages will never include the URL of a particular Veil page, only the URL of the generic Veil bootstrap. The compiler rewrites links within a page so that, if the user clicks a link, the page will fetch the

relevant content via a blinded URL, and then deserialize and evaluate that content as described above.

2.4.5 Protecting RAM Artifacts

As a Veil page creates new JavaScript objects, the browser transparently allocates physical memory pages on behalf of the site. Later, the OS may swap those pages to disk if memory pressure is high and those pages are infrequently used. JavaScript is a high-level, garbage-collected language that does not expose raw memory addresses. Thus, browsers do not define JavaScript interfaces for pinning memory, and Veil has no explicit way to prevent the OS from swapping sensitive data to disk.

By frequently accessing sensitive JavaScript objects, Veil *can* ensure that the underlying memory pages are less likely to be selected by the OS's LRU replacement algorithm. Veil's JavaScript runtime defines a `markAsSensitive(obj)` method; using this method, an application indicates that Veil should try to prevent `obj` from paging to disk. Internally, Veil maintains a list of all objects passed to `markAsSensitive()`. A periodic timer walks this list, accessing every property of each object using JavaScript reflection interfaces. Optionally, `markAsSensitive()` can recurse on each object property, and touch every value in the object tree rooted by `obj`. Such recursive traversals make it easier for developers to mark large sets of objects at once. JavaScript defines a special `window` object that is an alias for the global namespace, so if an application marks `window` as recursively sensitive, Veil will periodically traverse the entire heap graph that is reachable from global variables. Using standard techniques from garbage collection algorithms, Veil can detect cycles in the graph and avoid infinite loops.

`markAsSensitive()` maintains references to all of the sensitive objects that it has ever visited. This prevents the browser from garbage collecting the memory and possibly reusing it without applying secure deallocation [24]. At page unload time, Veil walks the sensitive list a final time, deleting all object properties. Since JavaScript does not expose raw memory, Veil cannot `memset()` the objects to zero, but deleting the properties does make it more difficult for a post-session attacker to reconstruct object graphs.

Sensitive data can reside in the JavaScript heap, but it can also reside in the memory that belongs to the renderer. The renderer is the browser component that parses HTML, calculates the screen layout, and repaints the visual display. For example, if a page contains an HTML tag like `<b>Secret</b>`, the cleartext string `Secret` may page out from the renderer's memory. As another example, a rendered page's image content may be sensitive.

The renderer is a C++ component that is separate from the JavaScript engine; JavaScript code has no way to directly access renderer state. However, JavaScript can indirectly touch renderer memory through preexisting renderer interfaces. For example, if the application creates an empty, invisible `<img>` tag, and injects the tag into the page's

HTML, the browser invalidates the page's layout. If the application then reads the size of the image tag's parent, the browser is forced to recalculate the layout of the parent tag. Recalculating the layout touches renderer memory that is associated with the parent tag (and possibly other tags). Thus, Veil can walk the renderer memory by periodically injecting invisible tags throughout the HTML tree (forcing a relayout) and then removing those tags, restoring the original state of the application.

The browser's network stack contains memory buffers with potentially sensitive content from the page. However, Veil only transmits encrypted data over the network, so network buffers reveal nothing to an attacker if they page out to disk and are subsequently recovered. Importantly, Veil performs heap walking on the user's password and symmetric key. This prevents those secrets from paging out and allowing an attacker to decrypt swapped out network buffers.

2.4.6 Mutation Techniques

Veil's main protection mechanism for RAM artifacts is heap walking, and we show in Section 2.7.3 that heap walking is an effective defense during expected rates of swapping. However, Veil provides a second line of defense via content mutation. Mutation ensures that, each time a client loads a page, the page will return different HTML, CSS, and JavaScript, even if the baseline version of the page has not changed. Mutation makes grep-based attacks more difficult, since the attacker cannot simply navigate to a non-Veil version of a page, extract identifying strings from the page, and then grep local system state for those strings. Content mutation is performed by the blinding servers (§2.4.2); below, we briefly sketch some mutation techniques that the blinding servers can employ.

Note that blinding servers can mutate content in the background, *before* the associated pages are requested by a client. For example, blinding servers can store a pool of mutated versions for a single object, such that, when a client fetches HTML that refers to the object, the blinding server can late-bind the mutated version that the page references. Using this approach, mutation costs need not be synchronous overheads that are paid when a client requests a page. In addition, when a user requests a Veil page, the blinding servers update the corresponding hashes for the mutated objects in the root object before sending it to the user to preserve the self-verification property of Veil objects described in Section 2.4.1.

JavaScript: To mutate JavaScript files, the blinding service uses techniques that are adapted from metamorphic viruses [127]. Metamorphic viruses attempt to elude malware scanners by ensuring that each instantiation of the virus has syntactically different code that preserves the behavior of the base implementation. For example, functions can be defined in different places, and implemented using different sequences of assembler instructions that result in the same output.

Our prototype blinding service mutates JavaScript code using straightforward analogues of the transformations described above. JavaScript code also has a powerful advantage that assembly code lacks—the `eval()` statement provides a JavaScript program with the ability to emit new mutated code at runtime. Such "`eval()`-folding" is difficult to analyze [27], particularly if the attacker can only recover a partial set of RAM artifacts for a page.[3]

However, note that if a faulty blinding server forgets to mutate invocations of `veilFetch(hashName)`, then unscrambled object hash names may be paged out to disk in JavaScript source code! If an attacker recovered such artifacts, he could directly replay the object fetches that were made by the private session. Thus, JavaScript mutation is a core responsibility for the blinding service.

HTML and CSS: The grammars for HTML and CSS are extremely complex and expressive. Thus, there are many ways to represent a canonical piece of HTML or CSS [47]. For example, HTML allows a character to be encoded as a raw binary symbol in a character encoding like `UTF-8` or `Unicode-16`. HTML also allows characters to be expressed as escape sequences known as HTML entities. An HTML entity consists of the token "&#" followed by the Unicode code point for a character and then a semicolon. For instance, the HTML entity for "a" is "a". The HTML specification allows an HTML entity to have leading zeroes which the browser ignores; the specification also allows for code points to be expressed in hexadecimal. Thus, to defeat simple exact-match greps of HTML artifacts, the blinding service can randomly replace native characters with random HTML entity equivalents.

There are a variety of more sophisticated techniques to obfuscate HTML and CSS. For a fuller exploration of these topics, we defer the reader to other work [47]. Our blinding service prototype uses random HTML entity mutation. It also obscures the HTML structure of the page using randomly inserted tags which do not affect the user-perceived visual layout of the page.

Images: The blinding service can automatically mutate images in several ways. For example, the blinding service can select one of several formats for a returned image (e.g., JPEG, PNG, GIF, etc.). Each instantiation of the image can have a different resolution, as well as different filters that are applied to different parts of the visual spectrum. Web developers can also use application-specific knowledge to generate more aggressive mutations, such as splitting a single base image into two semi-transparent images that are stacked atop each other by client-side JavaScript. As explained in our threat model (§2.3), Veil does not protect against leaks of the raw display bitmap that resides in GPU

[3] Some .NET viruses already leverage access to the runtime's reflection interface to dynamically emit code [118].

memory; thus, the mutation techniques from above are sufficient to thwart grep-based forensics on memory artifacts from the DOM tree. For a more thorough discussion of image mutation techniques that thwart classification algorithms, we defer to literature from the computer vision community [16].

2.4.7 Dynamic Content

At first glance, Veil's compile-time binding of URLs to objects seems to prevent a publisher from dynamically generating personalized user content. However, Veil can support dynamic content generation by using the blinding service as a proxy that sits between the end-user and the publisher. More specifically, a Veil page can issue an HTTP request with a `msg-type` of "forward". The body of the request contains two things: user information like a site-specific Veil cookie (§2.4.3), and a publisher name (e.g., `foo.com`). The page gives the request a random hash name, since the page will not cache the response. When the blinding service receives the request, it forwards the message to the publisher's dynamic content server. The publisher generates the dynamic content from the provided user information, and then sends the content to the blinding service, who forwards it to the client as the HTTP response to the client's "forward" request. The client and the publisher can encrypt the user information and the personalized content if the blinding service is not trusted with user-specific data; in this scenario, the content provider's web server is responsible for mutating objects before returning them to the client. Regardless, the content provider must compile dynamically-generated content (§2.4.1 and §2.5).

Another option is to start with the same forwarding protocol as above, but instead of having the publisher compile and mutate the content, the publisher just sends the unmodified user-specific content back to the blinding servers. Then, the blinding servers compile and mutate the content before returning it to the user.

The question is which of the two options is better. More specifically, should the blinding servers or the publishers perform compilation and mutation? Ideally, the end host would manipulate the dynamic content as it might contain sensitive user information, which can be encrypted on host and thus hidden from the blinding servers. However, the downside is that all end hosts have to adopt Veil. Having the proxy perform the manipulation solves this problem, but this scenario would require the proxy to handle a heavier computation workload. The networking community has examined these tradeoffs in a similar context, so we refer the reader to that specific research for a more in-depth discussion [2, 80]. The performance overhead is minimal because only the dynamic portions of the site have to be compiled during the page load, and more detailed numbers are in Section 2.7.2.

2.4.8 DOM Hiding

Heap walking reduces the likelihood that in-memory browser state will swap to disk. Content mutation ensures that, if state does swap out, then the state will not contain greppable artifacts from a canonical version of the associated page. However, some Veil sites will be uncomfortable with sending *any* site-specific HTML, CSS, or JavaScript to a client, even if that content is mutated. For example, a site might be concerned that a determined sysadmin can inspect swapped-out fragments of mutated HTML, and try to reverse-engineer the mutation by hand.

To support these kinds of sites, Veil provides a mode of operation called DOM hiding. In DOM hiding mode, the user's browser essentially acts as a thin client, with the full version of the page loaded on a remote server that belongs to the content provider. The user's browser employs a generic, page-agnostic JavaScript library to forward GUI events to the content provider through the blinding service; the content provider's machine applies each GUI event to the server-side page, and then returns an image that represents the new state of the page.

The advantage of DOM hiding is that site-specific HTML, CSS, and JavaScript is never pushed to the user's browser. The disadvantage is that each GUI interaction now suffers from a synchronous wide-area latency. For some Veil sites, this trade-off will be acceptable. We characterize the additional interactive latency in Section 2.7.4.

Figure 2-5 provides more details about how Veil implements DOM hiding. The Veil bootstrap page receives the URL to load from the user, as described in Section 2.4.4. The bootstrap page then issues an initial HTTP request through the blinding servers to the content provider. The content provider returns a page-agnostic remoting stub; this stub merely implements the client-side of the remote GUI architecture. As the content provider returns the stub to the user, the provider also launches a headless browser[4] like PhantomJS [1] to load the normal (i.e., non-rewritten) version of the page. The content provider associates the headless browser with a Veil GUI proxy. The proxy uses native functionality in the headless browser to take an initial screenshot of the page. The GUI proxy then sends the initial screenshot via the blinding servers to the user's remoting stub. The stub renders the image, and uses page-agnostic JavaScript event handlers to detect GUI interactions like mouse clicks and keyboard presses. The stub forwards those events to the GUI proxy. The proxy replays those events in the headless browser, and ships the resulting screen images back to the client. Note that a page which uses DOM hiding will not use encrypted client-side browser caching (§2.4.1) or DOM storage (§2.4.3)—there will be no page-specific client-side state to store.

[4] A headless browser is one that does not have a GUI. However, a headless browser *does* maintain the rest of the browser state; for example, DOM state can be queried using normal DOM methods, and modified through the generation of synthetic DOM events like mouse clicks.

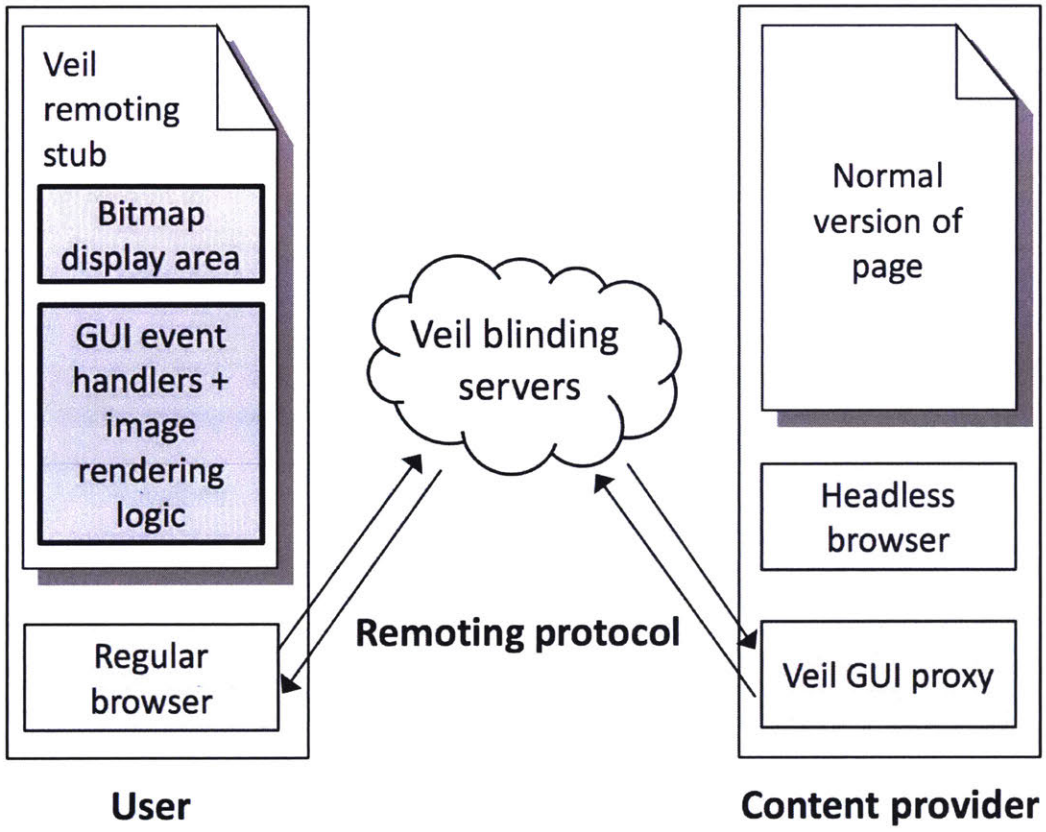


Figure 2-5: With DOM hiding, the client-side remoting stub sends GUI events to the content provider, and receives bitmaps representing new page states. The page's raw HTML, CSS, and JavaScript are never exposed to the client.

2.4.9 Discussion

Veil tries to eliminate cleartext client-side evidence of browsing activity. However, Veil does not prevent the server-side of a web page from tracking user information. Thus, Veil is compatible with preexisting workflows for ad generation and accounting (although advertising infrastructure must be modified to use blinded URLs and "forward" messages).

If a Veil page wants to use the browser cache, Veil employs encryption to prevent attackers from inspecting or modifying cache objects. However, an attacker may be able to fingerprint the site by observing the size and number of its cached objects. Sun et al. [116] provide a survey of techniques which prevent such fingerprinting attacks; their discussion is in the context of protecting HTTPS sessions, but their defensive techniques are equally applicable to Veil. The strongest defense is to reduce the number of objects in a page. Veil's compiler can easily do this by inlining objects into HTML [71]; for example, the compiler can directly embed CSS content that the original HTML incorporated via a link to an external file. The blinding service can also inject noise into the distribution

of object sizes and counts. For example, when the service returns objects to clients, it can pad data sizes to fixed offsets, e.g., 2KB boundaries or power-of-2 boundaries. Alternatively, the blinding service can map object sizes for page X to the distribution for object sizes in a different page Y [128]. All of these defensive approaches hurt performance in some way—inlining and merging reduce object cacheability, and padding increases the amount of data which must be encrypted and transmitted over the network. Note that publishers must explicitly enable client-side caching, so paranoid sites can simply disable this feature.

2.5 Porting Legacy Applications

In this section, we describe how Veil helps developers to port legacy web pages to the Veil framework. In particular, we provide case studies which demonstrate how Veil's compiler and runtime library can identify unblinded fetches and, in some cases, automatically transform those fetches into blinded ones.

Raw XMLHttpRequests: Veil's compiler traverses a statically defined HTML tree, converting raw URLs into Veil hash pointers. However, a page's JavaScript code can use `XMLHttpRequests` to dynamically fetch new content. Veil's static HTML compiler does not interpose on such fetches, so they will generate unblinded transfers that pollute the client's DNS cache and browser cache.

In debugging mode, Veil's client library shims the JavaScript runtime [72] and interposes on the `XMLHttpRequest` interface. This allows Veil to inspect the URLs in `XMLHttpRequests` before the associated HTTP fetches are sent over the network. Veil drops unblinded requests and writes the associated URLs to a log. A web developer can then examine this log and determine how to port the URLs.

For static content, one porting solution is to leverage Veil's *AJAX maps*. Once the debugging client library has identified a page's raw `XMLHttpRequest` URLs, the library sends those URLs to Veil's HTML compiler. The compiler automatically fetches the associated objects and uploads them to the object servers. Additionally, when the compiler rewrites the HTML, it injects JavaScript code at the beginning of the HTML which maps the raw `XMLHttpRequest` URLs to the hash names of the associated objects. Later, when the page is executed by real users, Veil's shimmed `XMLHttpRequests` use the AJAX map to convert raw URLs to blinded references. Veil will drop requests that are not mentioned in the translation map. This approach is complete from the security perspective, since all unblinded `XMLHttpRequests` will be dropped. However, for this approach to please users (who do not want *any* requests to drop), Veil developers should use testing tools with good coverage [74, 82, 110] to ensure that all of a page's `XMLHttpRequest` URLs are mapped.

AJAX maps are unnecessary for native Veil pages which always generate blinded `XMLHttpRequests`. However, URL validation via `XMLHttpRequest` shimming is useful when developers must deal with complex legacy libraries.

Dynamic tag generation: A legacy page can generate unblinded fetches by dynamically creating new DOM nodes that contain raw URLs in `src` attributes. For example, using `document.createElement()`, a page can inject a new <img> tag into its HTML. A page can also write to the `innerHTML` property of a preexisting DOM node, creating a new HTML subtree that is attached to the preexisting node. Neither type of tag creation will be captured by `XMLHttpRequest` shimming.

`XMLHttpRequest` shimming is a specific example of a more general technique called DOM virtualization. If desired, the entire DOM interface can be virtualized [4, 51, 73], allowing Veil to interpose on all mechanisms for dynamic tag creation. However, full DOM virtualization adds non-trivial performance overhead—the native DOM implementation is provided by the browser in fast C++ code, but a virtualized DOM is implemented by the application in comparatively slow JavaScript code. Furthermore, the full DOM interface is much more complex than the narrow `XMLHttpRequest` interface.

Our current implementation of Veil supports `XMLHttpRequest` shimming, but not full DOM virtualization. We leave the integration of Veil with a full virtualization system [50] as future work.

Unblinded links in CSS: CSS files can directly reference image objects using the `url()` statement, e.g., `body{background: url('x.jpg')}`. After the Veil compiler processes HTML files, it examines the associated CSS files and replaces raw image links with inline data URLs. Thus, when the Veil page loads a post-processed CSS file, the image data will be contained within the CSS itself, and will not require network fetches.

Angular.js: Angular [7] is a popular JavaScript framework that provides model-view-controller semantics for web applications. Angular uses a declarative model to express data bindings. For example, the `{{}}` operator is used to embed live views of the controller into HTML. The HTML snippet `<img src={{controller.x}}/>` instructs Angular to dynamically update the content of the <img> whenever the JavaScript value `controller.x` changes. Many other popular frameworks define a similar templating mechanism [9, 100, 122].

The `{{}}` operator is not part of the official HTML grammar. To implement `{{}}` and other kinds of data binding, Angular uses a dynamic DOM node compiler. This compiler is a JavaScript file that runs at the end of the page load, when the initial DOM tree has been assembled. The compiler locates special Angular directives like `{{}}`, and replaces them with new JavaScript code and DOM nodes that implement the data binding protocol.

Angular allows URLs to contain embedded {{}} expressions. Since these URLs are not resolved until runtime, Veil's static compiler cannot directly replace those URLs with blinded ones. However, Veil can rewrite Angular directives in a way that passes control to Veil code whenever a data binding changes. In the previous <img> example, Veil rewrites the tag as follows:

```
<img src="0" alt={{controller.x}}/>
```

The src attribute of the image is set to a network path which is known to be nonexistent (but whose URL does not leak private information). When the page tries to load the image, the load failure will invoke a custom onerror handler that Veil has attached to the window object. That handler will read the value of the alt attribute, which will contain the dynamic value of controller.x. Veil will then issue a blinded fetch for the associated image. In parallel, Veil also sets an Angular $watch() statement to detect future changes in {{controller.x}}; when a change occurs, Veil reads the new value, and then blindly fetches and updates the image as before. This basic approach is compatible with the template semantics of other popular JavaScript frameworks [9, 100, 122].

If dynamic Angular URLs can be drawn from an arbitrarily large set, Veil uses the "forward" message type from Section 2.4.9 to bind the raw URL to a blinded one. If the URL is drawn from a finite set, the compiler can upload the associated objects to the blinding service, and then inject the page with a blinding map that translates resolved Angular URLs to the associated hash names. The blinding service mutates that table in the same way that it mutates the hash names passed to veilFetch().

2.6 Implementation

Our Veil prototype consists of a compiler, a blinding server, a GUI proxy, a bootstrap page, and a client-side JavaScript library that implements veilFetch() and other parts of the Veil runtime.

We implemented the compiler and the blinding server in Python. The compiler uses BeautifulSoup [104] to parse and mutate HTML; the compiler also uses the Esprima/Escodegen tool chain [48, 117] to transform JavaScript code into ASTs, and to transform the mutated ASTs back into JavaScript. To implement cryptography, we use the PyCrypto library [62] in the blinding server, and the native Chrome WebCrypto API [125] in the Veil JavaScript library. We use OpenCV [87] to perform image mutation on the blinding server.

To implement DOM hiding, we used Chrome running in headless mode as the browser used by the content provider's GUI proxy. The GUI proxy was written in Python, and used Selenium [111] to take screenshots and generate synthetic GUI events within the headless browser.

Operation	Speed
Generate an AES key and encrypt it with RSA public key (2048 bit)	0.75 ms
Encrypt 64 character hash (blinded reference)	0.16 ms
Throughput for decryption using AES-CTR	520 MB/s
Throughput for verifying SHA256 hash of file	220 MB/s

Figure 2-6: Overhead for client-side JavaScript cryptography using the WebCrypto API [125].

2.7 Evaluation

In this section, we evaluate Veil's raw performance, and its ability to safeguard user privacy. Using forensic tools and manual analysis, we find that blinded references and encrypted objects are sufficient to prevent information leakage through the browser cache and name-based interfaces like the DNS cache. We show that Veil's heap walking techniques are effective at preventing secrets from paging out unless system-wide memory pressure is very high. We also demonstrate that the performance of our Veil's prototype is acceptable, with page load slowdowns of 1.2x–3.25x.

All performance tests ran on a machine with a 2 GHz Intel Core i7 CPU with 8GB of RAM. Unless otherwise specified, those tests ran in the Chrome browser, and we ran each experiment 100 times and measured the average. We configured Veil to use 2048-bit RSA and 128-bit AES in CTR mode. The phrase "standard Veil mode" corresponds to non-DOM hiding mode.

2.7.1 Performance Microbenchmarks

Veil uses cryptography to implement blind references and protect the data that it places in client-side storage. Figure 2-6 depicts the costs for those operations. Before a user can load a Veil page, she must generate an AES key and encrypt it with the blinding service's RSA key. This one time cost is 0.75 ms. The remaining three rows in Figure 2-6 depict cryptographic overheads that Veil incurs during a page load.

- For `veilFetch()` to generate a blinded reference, it must encrypt a hash value with the user's AES key. This operation took 0.16 ms.
- When `veilFetch()` receives a response, it must decrypt that response with the AES key. That operation proceeds at 520 MB/s. For example, decrypting a 300 KB image would require 0.6 ms.
- `veilFetch()` also validates the hash of the downloaded object. This proceeds at 220 MB/s, requiring 1.3 ms for a 300 KB image.

Operation	Speed
Decrypt AES key (2048 bit RSA)	3.1 ms
Decrypt 64 char hash (blinded reference)	0.04 ms
Throughput for encryption using AES-CTR	62 MB/s

Figure 2-7: Overhead for server-side operations using PyCrypto [62].

Figure 2-7 depicts the cryptography overheads on the server-side of the protocol. End-to-end, fetching a 300 KB object incurs roughly 10 ms of cryptographic overhead.

2.7.2 Performance Macrobenchmarks: Standard Veil Mode

To measure the increase in page load time that Veil imposes, we ported six sites to the Veil framework. **Washington Post** is the biggest site that we ported, and contains large amounts of text, images, and JavaScript files. **Imgur** is a popular image-sharing site; compared to the other test sites, it has many images but less text. **Woot!** is an e-commerce site that has a large amount of text and images, but comparatively few scripts. **Piechopper** is a highly dynamic site that uses Angular (§2.5). Piechopper is script-and-text heavy, but has few images. **University** represents a university's website. This site is the smallest one that we tested, although it uses CSS with raw URLs that Veil must blind (§2.5). **Google** represents the results page for the search term "javascript." Most of that page's JavaScript and CSS objects are inlined into the HTML, meaning that they do not require network fetches.

To port a preexisting site to Veil, we had the compiler download the top-level HTML file and extract the URLs which referenced external objects like images. The compiler downloaded those objects from the relevant servers. After calculating hashes for those objects (and converting raw URLs into blinded ones), the compiler uploaded the objects to the blinding server. Since preexisting sites were not designed with Veil in mind, they occasionally fetched content dynamically, e.g., via unblinded `<img>` tags generated by JavaScript at runtime. For sites like this, we observed which objects were dynamically fetched, and then manually handed them to the compiler for processing; we also manually rewrote the object fetch code to refer to the compiler-generated object names. Native Veil pages would invoke the Veil runtime library to dynamically fetch such content, avoiding the need for manual rewriting.

Page load time: Figure 2-8 depicts the load times for three versions of each site: the regular version of the site, a Veil port that does not perform cryptography, and a Veil port with cryptography enabled. The regular versions of a page were loaded from a localhost

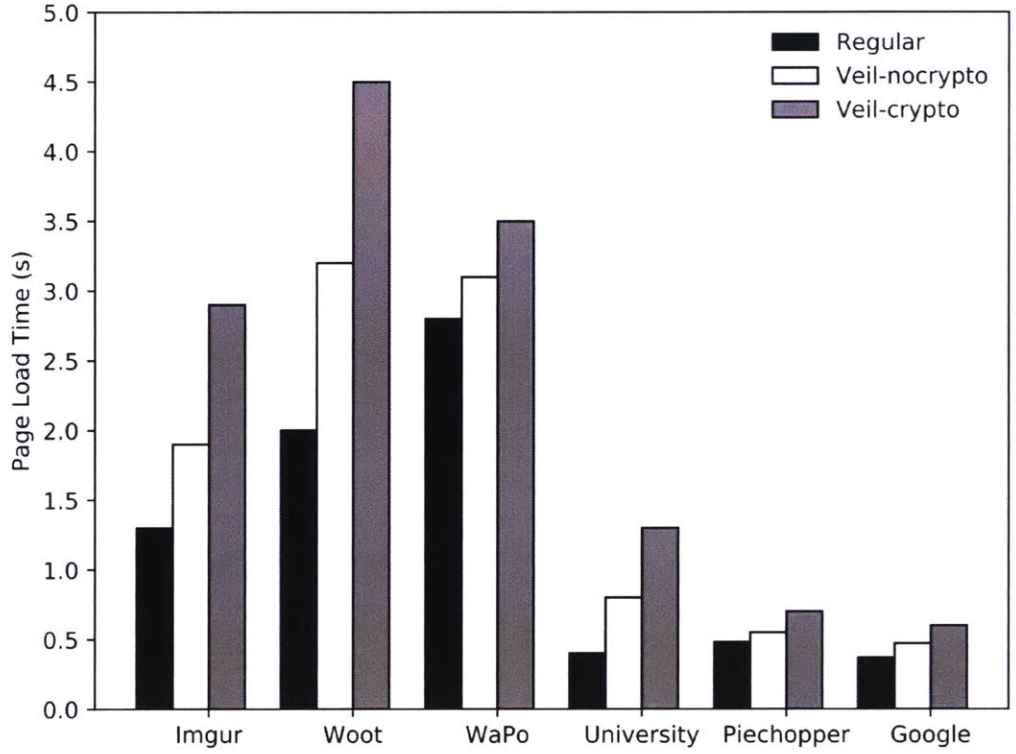


Figure 2-8: Page load times for each website: regular; with Veil (but no cryptography); with Veil (and using cryptography).

webserver, whereas the Veil pages were loaded from a localhost blinding server. This setup isolated the overhead of cryptography and content mutation.

As shown in Figure 2-8, page loads using Veil with no cryptography were 1.25x–2x slower. This is mostly due to extra computational overhead on the client. For example, parsing overheads increased because, as we quantify below, mutated objects were larger than the baseline objects; for images, the browser also had to Base64-decode the bitmaps before displaying them. Veil with cryptography added another slowdown factor of 1.1x–1.63x, with higher penalties for pages with many objects (regardless of their type). The end-to-end slowdown for the full Veil system was 1.25x–3.25x. Note that these slowdowns were for browsers with cold caches; Veil's overhead would decrease with caching, since server-side cryptography could be avoided. Also note that the University site was a challenging case for Veil, because the site was small in absolute size, but has many small images. Thus, Veil's per-blinded-reference cryptographic overheads (see Figures 2-6 and 2-7) were paid more frequently. A Veil-optimized version of the site would use image spriting [42] to combine multiple small images into a single, larger one.

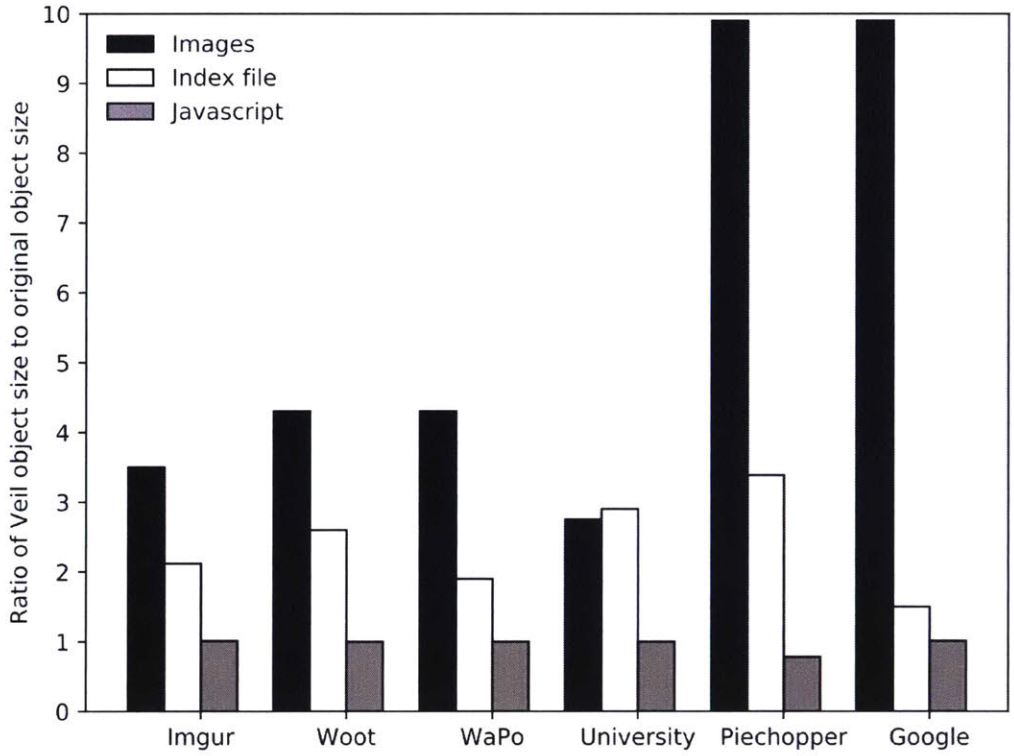


Figure 2-9: Size increases for Veil's mutated objects.

Dynamic content overhead: As described in Section 2.4.7, dynamic content has some overhead because it has to be compiled during the page load. Fortunately, the compilation cost for a single dynamic object is typically small. For example, compiling a 100 KB image requires Base64-encoding it and generating a few metadata fields, taking roughly 75 ms. Content providers or blinding servers can compile multiple dynamic objects in parallel.

Object growth: Figure 2-9 shows how object sizes grew after post-processing by Veil. Images experienced two sources of size expansion: mutation and Base64 encoding. Base64 encoding resulted in a 1.33x size increase. Our Veil prototype implements mutation via the addition of Gaussian noise, with the resulting size increases dependent on the image format. PNG is lossless, so the addition of noise generated a 10x size increase. In contrast, JPG is a lossy format, so noise injection resulted in less than a 2x size increase. The Piechopper and Google pages contained many PNGs, and thus suffered from worse image expansion than the other test pages.

As shown in Figure 2-9, mutated JavaScript files typically remained the same size, or became somewhat smaller—mutation adds source code, but Veil passes the mutated

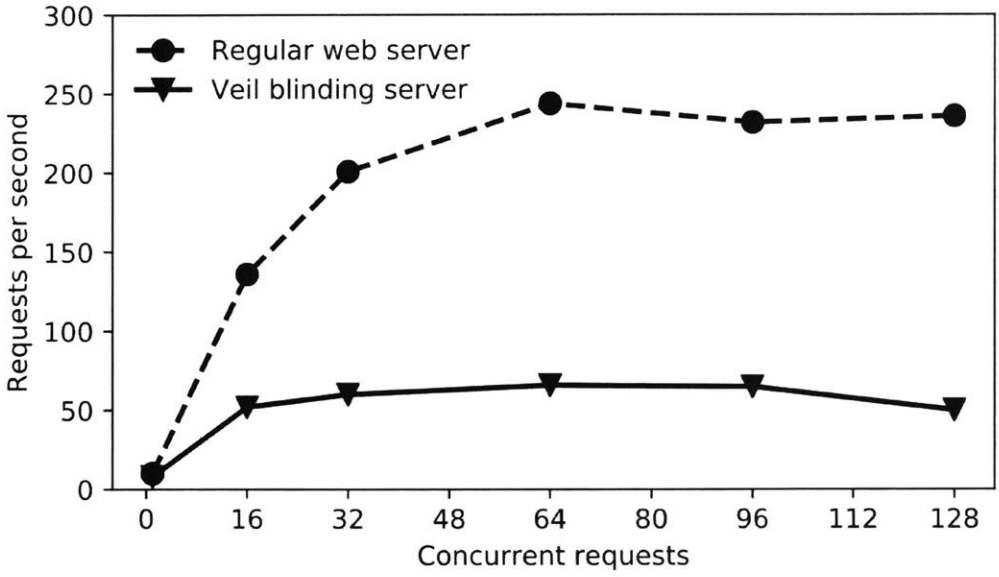


Figure 2-10: Scalability comparison between a blinding server and a regular web server.

code through a minifier which removes extraneous whitespace and rewrites variable names to be shorter. HTML suffered from larger size increases, because mutation tricks like random HTML entity encoding strictly increase the number of characters in the HTML.

Server-side scalability: Figure 2-10 shows the HTTP-level request throughput of a Veil blinding server, compared to the baseline performance of a blinding server that performed none of Veil's added functionality (and thus acted as a normal web server). HTTP requests were generated using `ab`, the Apache benchmarking tool [121].

As shown in Figure 2-10, Veil reduces web server throughput by roughly 70% due to the additional cryptographic operations that Veil must perform. By quantifying Veil's scalability penalty for a fixed client load compared to a regular web server, blinding server hosts can know the additional servers needed to handle a specific load on a Veil page. Remember that when Veil operates in regular (i.e., non-DOM hiding mode), Veil blinding servers mutate content in the background, out of the critical path for an HTTP response; thus, the slowdowns in Figure 2-10 are solely caused by synchronous cryptographic operations.

2.7.3 Preventing Information Leakage

Name-based interfaces: To determine how well Veil protects user privacy, we created a

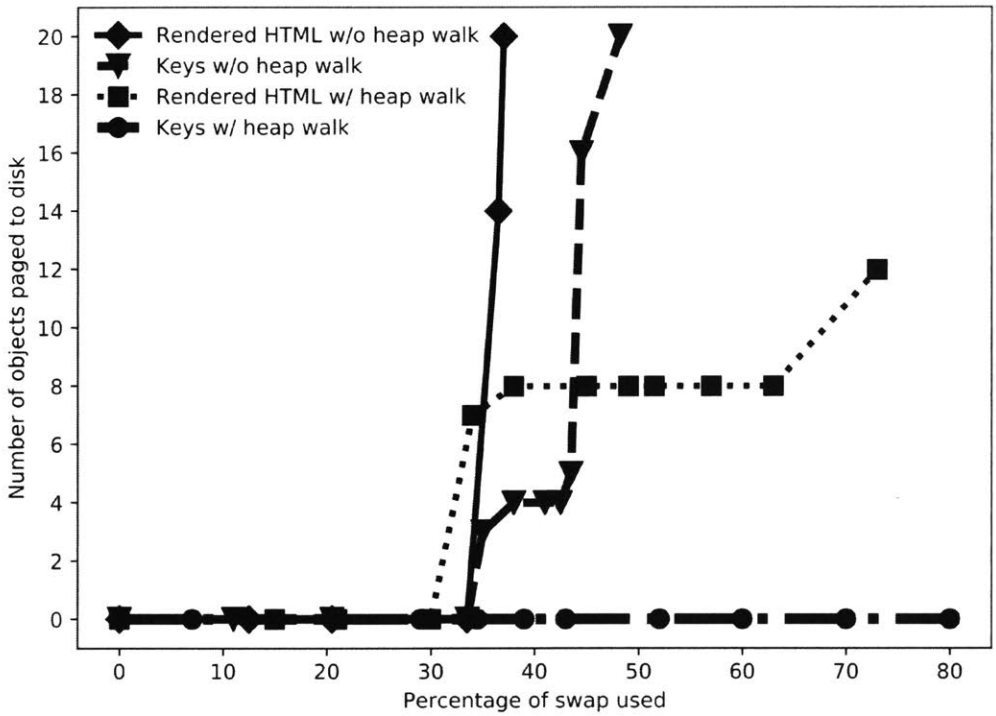


Figure 2-11: The effectiveness of heap walking to prevent secrets from paging out.

baseline VM image which ran Lubuntu 13.10 and had two different browsers (Firefox and Chrome). In the baseline image, the browsers were installed, but they had not been used to visit any web pages. We then ran a series of experiments in which we loaded the baseline image, opened a browser, and then visited a single site. We took a snapshot of the browser's memory image using `gcore`, and we also examined disk state such as the browser cache and the log entries for DNS resolution requests. We did this for the regular and Veil-enabled versions of each page described in Section 2.7.2.

In all tests, the Veil pages were configured to store data in the browser cache, and in all tests, the cache only contained encrypted data at the end of the private session. Greps through the memory snapshots and DNS records did not reveal cleartext URLs or hostnames. Unsurprisingly, the regular versions of the web pages left unencrypted data in the browser cache, and various cleartext URLs in name-based data stores. To cross-validate these results, we repeated these experiments on Windows, and used the Mandiant Redline forensics tool [67] to search for post-session artifacts in persistent storage. Redline confirmed that the only cleartext URL in the browser history was the URL for the Veil bootstrap page, and that all other URLs were blinded.

Protecting RAM artifacts: To determine whether heap walking can prevent secrets from paging out, we wrote a C program which gradually increases its memory pressure. The program allocates memory without deallocating any, and periodically, it reads the first byte in every allocated page to ensure that the OS considers the page to be hot. We ran the program inside of a QEMU VM with 1 GB of swap space and 1 GB of RAM. We also ran a browser inside of the VM. The browser had 20 open tabs. Each tab had a Uint8Array representing a tab-specific AES key, and a tab-specific set of strings in its HTML. The control experiments did not do heap walking. The test experiments used Veil's heap walking code to touch the AES key and the renderer state.

The VM used the `pwritev` system call to write memory pages to the swap file. To determine whether secrets paged out as memory pressure increased, we used strace to log the `pwritev` calls. Since each tab contained a set of unique byte patterns, we could grep through our `pwritev` logs to determine whether secret RAM artifacts hit the swap file. We ran experiments for increasing levels of memory pressure until the VM became unresponsive, at roughly 75% in-use swap space.

Figure 2-11 shows the results. The x-axis varies the memory pressure, and the y-axis depicts the number of tabs which suffered data leakage, as determined by greps through the `pwritev` log. Heap walking successfully kept all of the secret keys from paging out, up to the maximum 75% of in-use swap space. Without heap walking, keys begin to page out at 35% swap utilization; by 50%, all keys had swapped out. Note that the data points do not perfectly align on the x-axis due to nondeterminism in when the VM decides to swap data out.

Heap walking was less effective for renderer memory pages. Those pages swapped out earlier and immediately in the control case, around 35% swap utilization. With Veil, renderer state also began to leak at 35% utilization, but Veil still managed to safeguard 12 out of 20 tabs up to 63% swap utilization.

2.7.4 DOM Hiding

When Veil runs in DOM hiding mode, the client-side page contains no site-specific, greppable content. Thus, Veil does not need to perform heap walking (although Veil does use blinding servers to eliminate information leakage through name-based system interfaces). We loaded our test pages in DOM hiding mode, and confirmed the absence of site-specific content by grepping through VM images as we did in Section 2.7.3.

Figure 2-12 evaluates the impact of DOM hiding on a page's initial load. The client, the blinding server, and the content server ran on the same machine, to focus on computational overheads. Figure 2-12 demonstrates that DOM hiding imposed moderate overheads, with page load times increasing by 1.2x–2.1x. When Veil runs in DOM hiding

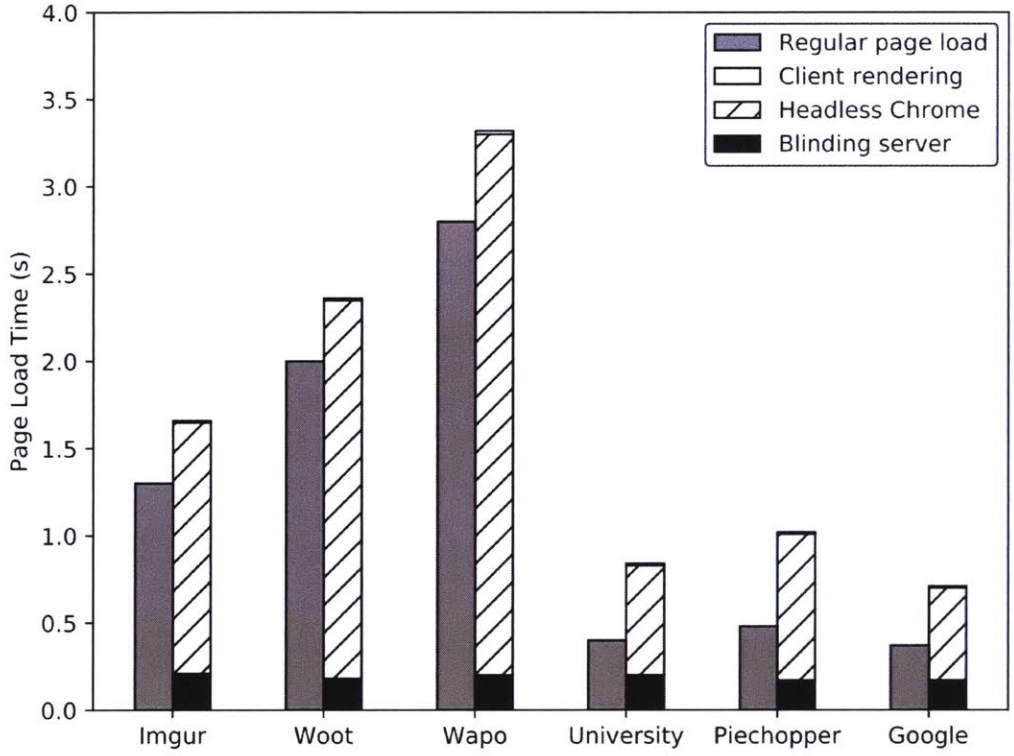


Figure 2-12: DOM hiding's impact on page load times.

mode, image mutation has to be performed synchronously, for each screenshot that is returned to a client; screenshotting requires 150ms–180ms, whereas image mutation requires 170ms–200ms.

Figure 2-13 shows the time that a DOM-hiding page needed to respond to a mouse click. Responding to such a GUI event required the browser to forward the event to the content provider, and then receive and display the new screenshot. Once again, the bulk of the end-to-end time was consumed by the screenshot capture and the image mutation at the content provider.

Privacy-sensitive users and web sites are often willing to trade some performance for better security. For example, fetching an HTTP object through Tor results in HTTP-level RTTs of more than a second [123]. Thus, we believe that the performance of Veil's DOM hiding mode is adequate for many sites. However, Veil's performance may be too slow for sites that are highly interactive, or require content servers to frequently and proactively push new images (e.g., due to animations in a page). Our next version of the Veil GUI proxy will grab screenshots directly from the content server's framebuffer [20] instead of via the comparatively-slow rendering API that browsers expose [76]; this implementation change will greatly reduce screenshotting overhead.

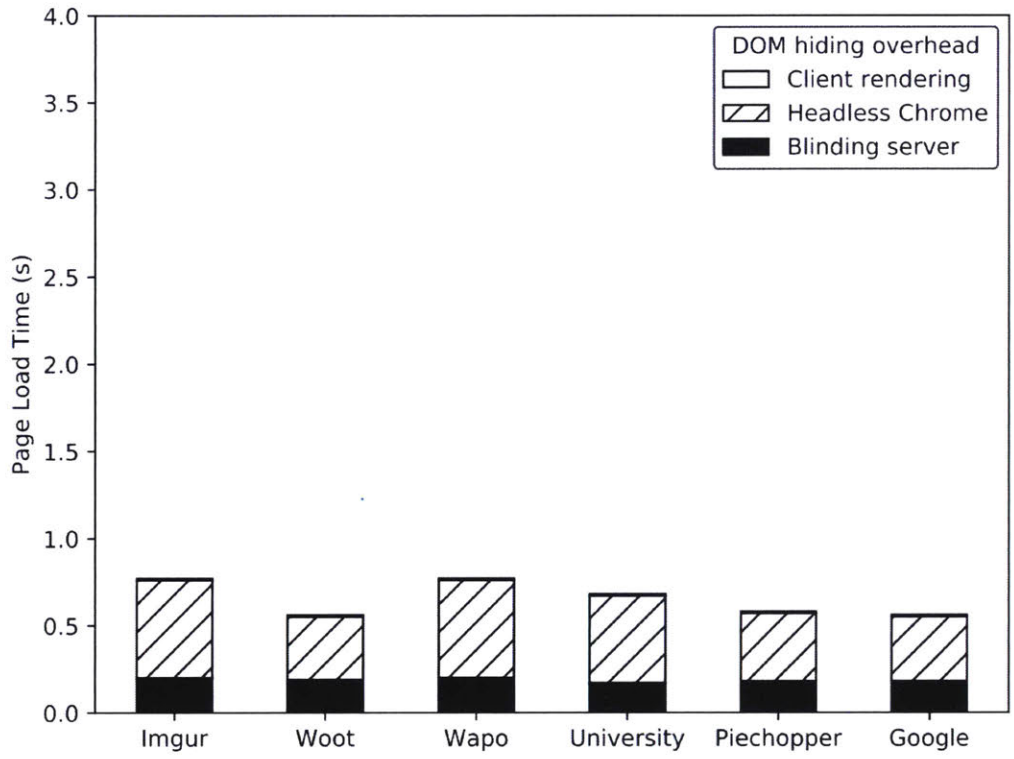


Figure 2-13: The time that a DOM-hiding page needs to respond to a mouse click event.

2.7.5 Network Latency

Figure 2-14 uses Chrome's built-in network emulation framework [43] to compare load times for three versions of the Imgur page: a normal version; a Veil version which used content mutation, heap walking, and encrypted storage; and a Veil version which used DOM hiding. The DOM hiding variant was largely insensitive to increased network latency, since loading a page only required two HTTP-level round trips (one to fetch the bootstrap page, and another to fetch the initial screenshot). The other variant of Veil was more sensitive to network latency. The reason is that, in this version of the page, the bootstrap code had to fetch multiple objects, all of which were served from the same blinding server origin (`https://veil.io`). Browsers cap the number of simultaneous connections that a client can make to a single origin, so the Veil page could not leverage domain sharding [56] to circumvent the cap. This limitation is not fundamental to Veil's design, since content providers can shard across multiple blinding server domains (e.g., `https://a.veil.io` and `https://b.veil.io`). However (and importantly), if a content provider wishes to use sharding, the provider must be careful to avoid bias in the mapping of objects to domains—otherwise, per-site fingerprints may arise in a

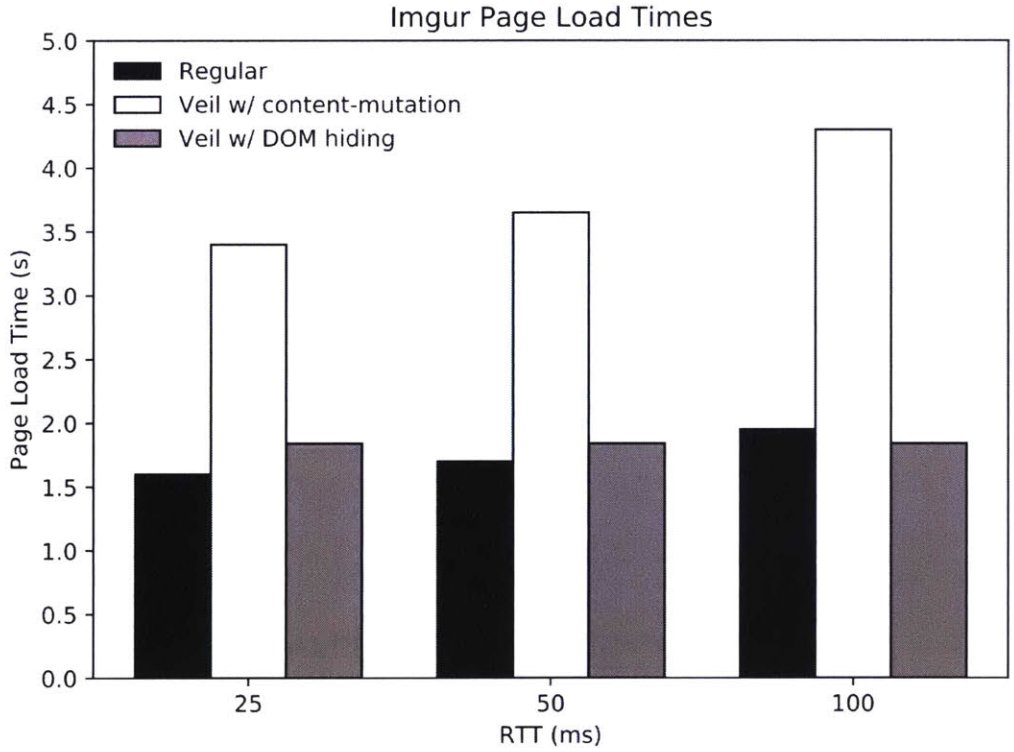


Figure 2-14: The impact of emulated network latency on page load times. In all cases, the download bandwidth cap was 30 Mbps, and the upload bandwidth cap was 10 Mbps, emulating a broadband connection. Bandwidth was not varied because page load times are largely governed by network latency, not bandwidth [37].

page's access patterns to various domains. Thus, for some content providers, domain sharding may not be worth the potential loss in security.

Domain sharding is also relevant to Content Security Policies (CSPs) [75]. A CSP allows a page to restrict the origins which can provide specific types of content. For example, a CSP might state that a page can only load JavaScript from `https://a.com`, and CSS from `https://b.com`. A CSP is expressed as a server-provided HTTP response header; the CSP is enforced by the browser. CSPs are useful for preventing cross-site scripting attacks, but require a page to be able to explicitly shard content across domains. As discussed in the last paragraph, Veil can enable sharding at the cost of reduced security.

2.8 Related Work

To minimize information leakage via RAM artifacts, applications can use best practices like pinning sensitive memory pages, and avoiding excessive copying of secret data [46].

Operating systems and language runtimes can also scrub deallocated memory as quickly as possible [24]. Web browsers do not expose low-level OS interfaces to JavaScript code, so privacy-preserving sites cannot directly access raw memory for the purposes of secure deallocation or pinning. Determining the best way to expose raw memory to JavaScript is an open research problem, given the baroque nature of the same-origin policy, and the fact that the browser itself may contend with JavaScript code for exclusive access to a memory page (e.g., to implement garbage collection or tab discarding [92]).

An OS can protect RAM artifacts by encrypting the swap space or the entire file system [17, 101, 133]. Veil's content mutation and DOM hiding allow Veil to protect RAM artifacts even when a browser does not run atop an encrypted storage layer. Content mutation obviously does not provide a cryptographically strong defense, but DOM hiding allows a Veil site to avoid sending any site-specific, greppable content to a client browser.

CleanOS [119] is a smartphone OS that protects sensitive data when mobile devices are lost or stolen. CleanOS defines sensitive data objects (SDOs) as Java objects and files that contain private user data. CleanOS observes which SDOs are not actively being used by an application, and encrypts them; the key is then sent to the cloud, deleted from the smartphone, and only retrieved when the SDOs become active again. SDOs could potentially be used as a building block for private browsing. However, SDOs are insufficient for implementing blinded references unless the SDO abstraction is spread beyond the managed runtime to the entire OS.

Lacuna [32] implements private sessions by running applications inside of VMs. Those VMs execute atop the Lacuna hypervisor and a modified Linux host kernel. The hypervisor and the host kernel collectively implement "ephemeral" IO channels. These encrypted channels allow VMs to communicate with hardware or small pieces of trusted code, but only the endpoints can access raw data—user-mode host processes and the majority of the host kernel can only see encrypted data. Lacuna also encrypts swap memory. Upon VM termination, Lacuna zeros the VM's RAM space and discards the ephemeral session keys. PrivExec [86] is similar to Lacuna, but is implemented as an OS service instead of a hypervisor. Lacuna and PrivExec provide stronger forensic deniability than Veil. However, these systems force layperson end-users to install and configure a special runtime; furthermore, private applications cannot persist data across sessions because keys are ephemeral.

UCognito [130] exposes a sandboxed file system to a private browsing session. The sandboxed file system resides atop the normal one, absorbing writes made during private browsing. When the browsing session terminates, UCognito discards the writes. Like PrivExec and Lacuna, UCognito requires a modified client-side software stack. UCognito also does not protect against information leakage via the non-sandboxed parts of the host OS. For example, unmodified RAM artifacts may page to the native swap file; DNS requests are exposed to the host's name resolution subsystem.

Amazon Silk [5] is a browser used on Amazon Kindles and uses a technique called remote dependency resolution (also known as split browsing) [81, 113]. When the Silk client issues an HTTP request for a web page, the request actually goes to an Amazon-maintained proxy that runs in the cloud. The proxy then uses a headless browser to load the requested page. Since the proxy lives in the core of the Internet, the proxy can fetch objects over low-latency network paths. As the proxy fetches these objects, they are streamed back to the user. This technique allows Silk to avoid high last-mile latencies afflicting the path between the client and Internet core. However, the client-side Silk browser still loads regular DOM objects, like HTML, Javascript, CSS, etc., thus not implementing DOM hiding that exists in Veil. It also does not protect RAM artifacts or provide content mutation.

Collaborative browsing frameworks [64, 95] allow multiple users with different browsers to simultaneously interact with a shared view of a web page. Like these frameworks, Veil's DOM hiding mode has to synchronize the GUI inputs and rendering activity that belong to a canonical version of a page. However, Veil only needs to support one remote viewer. More importantly, Veil's DOM hiding mode only exposes the client browser to generic JavaScript event handlers, as well as a bitmap display; in contrast, prior collaborative browsing frameworks replicate a site-specific, canonical DOM tree on each client browser. Prior frameworks also do not use blinding servers to hide information from client-side, name-centric interfaces like the DNS cache.

Silo [71] and the framework of Jiang et al [54] use client-side bootstrap pages which dynamically overwrite themselves with new content. Silo uses this technique to layer a delta-encoding protocol atop HTTP; Jiang's system uses dynamic assembly as a crude copy-protection mechanism, so that users who right click and "Save as" a page will only store the initial bootstrap HTML and not the dynamically assembled content. By itself, dynamic assembly cannot provide strong privacy guarantees. For example, blinded URLs are needed to prevent information leakage through the DNS cache and the browser cache.

2.9 Conclusions

Veil is the first web framework that allows developers to implement private-session semantics for their pages. Using the Veil compiler, developers rewrite pages so that all page content is hosted by blinding servers. The blinding servers provide name indirection, preventing sensitive information from leaking to client-side, name-based system interfaces. The blinding servers mutate content, making object fingerprinting more difficult; rewritten pages also automatically encrypt client-side persistent storage, and actively walk the heap to reduce the likelihood that in-memory RAM artifacts will swap to disk in cleartext form. In the extreme, Veil transforms a page into a thin client which does not

include any page-specific, greppable RAM artifacts. Veil automates much of the effort that is needed to port a page to Veil, making it easier for web developers to improve the privacy protections of their applications.

THREE

Splinter: Practical, Private Web Application Queries

3.1 Motivation

Web services are collecting increasing amounts of data, and this data contains information of interest to both users and businesses. For example, users can access crowdsourced information, such as the most up-to-date traffic data to determine the fastest route. Similarly, businesses can also leverage this crowdsourced data to extract cross-user trends that would be difficult or impossible to detect without this data. Many of these applications that crowdsource data currently allow users to query their datasets. For example, users might search WebMD for some information on their medical condition. They might also search Yelp to find a restaurant for dinner. Since this data can be valuable, an increasing number of web services with crowdsourced data are also allowing businesses and researchers to query their dataset. Google, for instance, has an API that allows organizations to query its map data to improve business decisions. However, the problem is that these queries can reveal sensitive information, such as medical conditions, user behavior, and business strategy [77, 78].

To solve this problem, we introduce Splinter, a practical system that allows servers to properly respond to queries without servers learning the sensitive information present in the queries. In Splinter, each *provider* hosts a copy of the dataset (Figure 3-1). Then, the user[1] divides each query into shares and sends them to these providers. As long as any one of the providers is honest (does not collude with the others), the providers cannot discover sensitive information in the query. However, given responses from all the providers, the user can compute the answer to her query.

Previous private query systems have generally not achieved practical performance because they use expensive cryptographic primitives and protocols. For example, systems

[1] In this chapter of the dissertation, we use the term "user" broadly to refer to a business, a researcher, and end-user of an application, i.e. any client of Splinter.

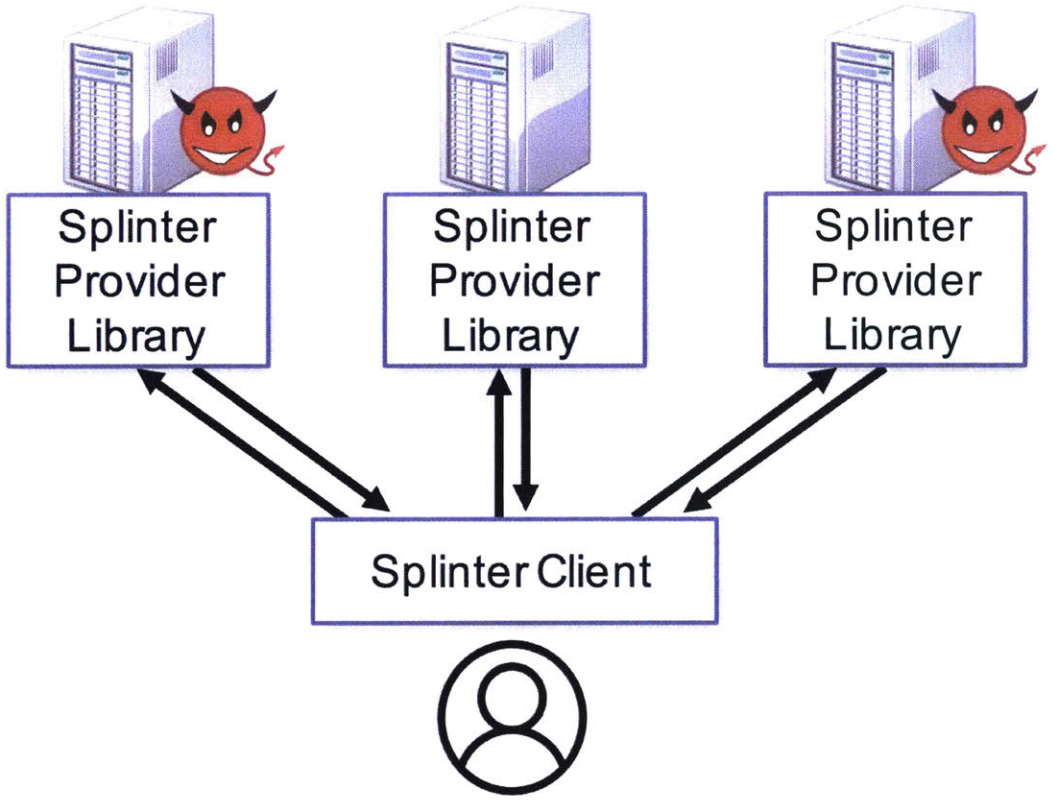


Figure 3-1: Splinter architecture. The Splinter client splits each user query into shares and sends them to multiple providers. It then combines their results to obtain the final answer. The user's query remains private as long as any one provider does not collude with the others.

based on techniques such as Private Information Retrieval (PIR) [22, 84, 103] require many round trips and high bandwidth for complex queries, while systems based on garbled circuits [15, 57, 129] have a high computational cost. These approaches are especially costly for mobile clients on high-latency networks.

To make private queries efficient, Splinter extends a recent cryptographic primitive called Function Secret Sharing (FSS) [19, 39] for private queries. FSS allows the client to split functions into shares that keep parameters of the function hidden unless all the providers collude. With judicious use of FSS, many queries can be answered in only a single network round trip with low CPU and bandwidth costs.

Splinter extends previous work on FSS in two important ways. First, prior work has only demonstrated efficient FSS protocols for point and interval functions with additive aggregates such as SUMs [19]. We present efficient protocols that support a more complex set of non-additive aggregates such as MAX/MIN and TOPK. These protocols let Splinter support a subset of SQL that can capture many popular online applications.

Second, we develop an optimized implementation of FSS that leverages AES-NI [107] instructions and multicore CPUs. For example, we use one-way compression functions, a cryptographic technique that utilizes modern AES instruction sets. As a result, our implementation is 2.5× faster per core than a naïve implementation of FSS. Together, these optimizations let Splinter query datasets with millions of records at sub-second latency.

We evaluate Splinter by implementing three applications atop it: a restaurant review site similar to Yelp, an airline ticket search, and a map routing service. For all of our applications, Splinter can execute queries in less than 1.6 seconds, at a cost of less than 0.05 cents in server resources on Amazon EC2.

3.2 Splinter Architecture

In this section, we describe Splinter's principals and security goals. Then, we discuss what services are amenable to Splinter and conclude with the threat model.

3.2.1 Splinter Principals

There are three main principals in Splinter: the *data owners*, the *providers*, and the *user*.

Data owners, such as Yelp and Google, collect non-sensitive data. By non-sensitive, we mean the data is not sensitive to the users that provide. Although the data itself might not be sensitive, data owners might restrict user access to this data because it is valuable to the data owner. For example, Google Maps traffic data might not be sensitive, but Google probably does not want to release this data publicly because it has business value.

Providers host a copy of the data. They can retrieve this data from a public repository or mirror site, or license it from data owners. In both scenarios, the providers store the data in cleartext.

Users issue queries to the provider. For a given user query, all the providers have to execute it on the same view of the data. Maintaining data consistency from mirror sites is beyond the scope of this dissertation, but standard techniques can be used [21, 120].

3.2.2 Security Goals

The goal of Splinter is to hide sensitive parameters in a user's query. Specifically, Splinter lets users run *parametrized queries*, where both the parameters and query results are hidden from providers. For example, consider the following query, which finds the 10 cheapest flights between a source and destination:

```
SELECT TOP 10 flightid FROM flights
WHERE source = ? AND dest = ?
ORDER BY price
```

Splinter hides the information represented by the questions marks, i.e., the source and destination in this example. The column names being selected and filtered are not hidden. The number of conditions in the WHERE clause is also not hidden. Finally, Splinter also hides the query's results from the providers—otherwise, the providers can use the results to infer the source and destination. Splinter supports a subset of the SQL language, which we describe in Section 3.4.

The easiest way to achieve these properties would be for users to download the whole database and run the queries locally. However, in Section 3.2.3, we explain why doing this might not be feasible.

3.2.3 Splinter-amenable Web Services

Although Splinter can handle complex queries, it is not meant as a private query system for all SQL-like databases. Splinter's use cases are similar to those of PIR. More specifically, the queries contain sensitive user information and need to be protected, but the database itself does not contain sensitive user information. For example, users might not want to reveal where they are traveling to Google when searching for directions. Similarly, data analysts might want to hide their query parameters because they might leak trade secrets for their algorithms.

Splinter works well for applications with large databases and regular updates because downloading the whole database and receiving updates would be more expensive in terms of bandwidth than querying the Splinter service. Services like flight price lookups, map navigation, and domain name availability searches are good fits for Splinter. In Section 3.8.2, we discuss and quantify the "break even" point for our case studies.

Even if it is more efficient for the user to download the whole database and updates, Splinter can still be useful. Many applications might enforce rate limiting or query restrictions to prevent users from accessing the whole database because the data might contain proprietary information. For example, Yelp might allow only limited querying for data scientists through an API but not give complete access to their dataset. In this scenario, attempting a full database download would be too expensive in comparison to employing the normal client-server query interface.

3.2.4 Threat Model

Splinter keeps the parameters in the user's query hidden as long as at least one of the user-chosen providers does not collude (share information or communicate) with the others. Splinter also assumes these providers are *passive adversaries*: a provider can observe the interactions between itself and the client, but Splinter does not protect against providers returning incorrect results or maliciously modifying the dataset.

We assume the data on the providers is stored in cleartext and that the user communicates with each provider through a secure channel (e.g., using SSL), and that the user's Splinter client is uncompromised. Our cryptographic assumptions are standard.

3.3 Function Secret Sharing

In this section, we give an overview of Function Secret Sharing (FSS), the main primitive used in Splinter, and show how to use it in simple queries. Sections 3.4 and 3.5 then describe Splinter's full query model and our new techniques for more complex queries.

3.3.1 Overview of Function Secret Sharing

Function Secret Sharing [19] lets a client divide a function f into *function shares* $f_1, f_2, \ldots, f_k$ so that k parties can help evaluate f without learning certain parameters. These shares have the following properties:

- They are close in size to a description of f.
- They can be evaluated quickly (similar in time to f).
- They sum to the original function f. That is, for any input x, $\sum_{i=1}^{k} f_i(x) = f(x)$. We assume that all computations are done over $\mathbb{Z}_{2^m}$, where m is the number of bits in the output range.
- Given any $k-1$ shares f_i, an adversary cannot recover the parameters of f.

Although it is possible to perform FSS for arbitrary functions [30], practical FSS protocols only exist for *point* and *interval* functions. These take the following forms:

- Point functions f_a are defined as $f_a(x) = 1$ if $x = a$ or 0 otherwise.
- Interval functions are defined as $f_{a,b}(x) = 1$ if $a \leq x \leq b$ or 0 otherwise.

In both cases, FSS keeps the parameters a and b private: an adversary can tell that it was given a share of a point or interval function, but cannot find a and b. In Splinter, we use the FSS scheme of Boyle et al. [19]. Under this scheme, the shares f_i for both functions require $O(\lambda\ell)$ bits to describe and $O(\ell)$ bit operations to evaluate for a security parameter λ (the size of cryptographic keys), and ℓ is the number of bits in the input domain.

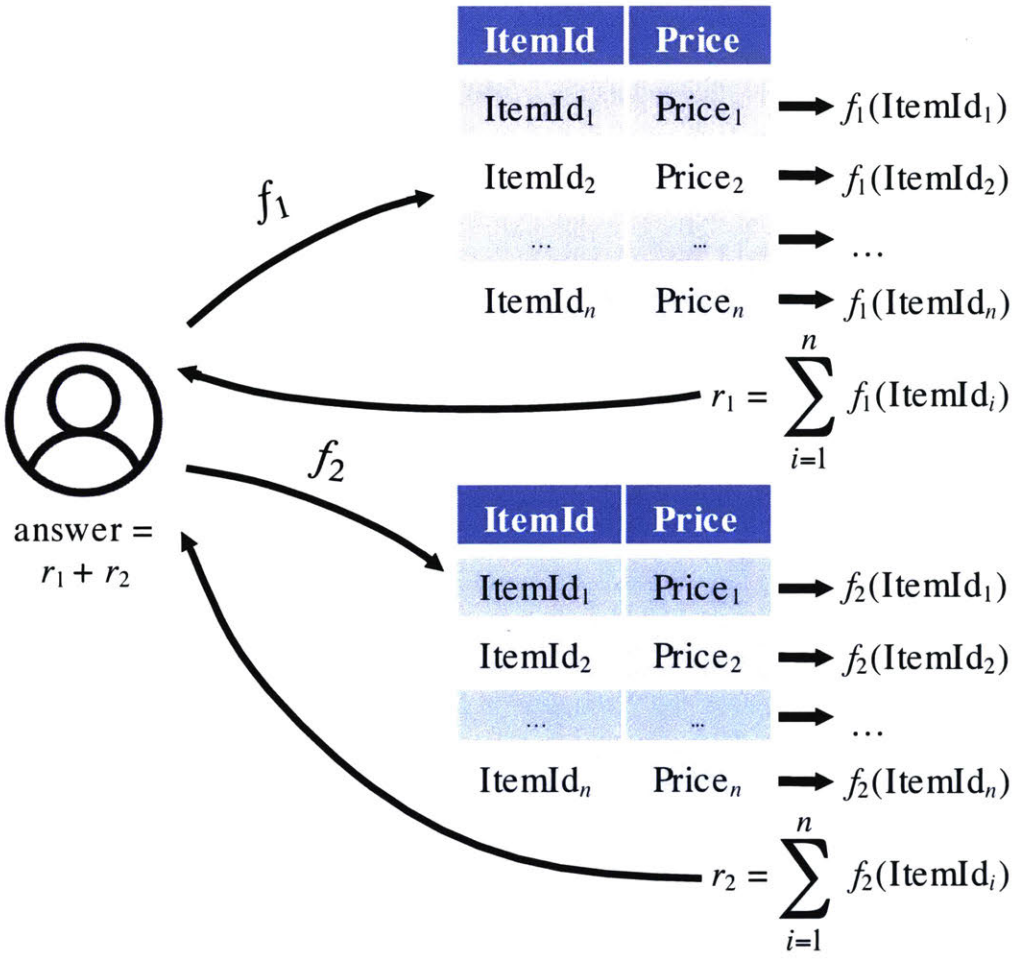


Figure 3-2: Overview of how FSS can be applied to database records on two providers to perform a COUNT query.

3.3.2 Using FSS for Database Queries

We can use the additive nature of FSS shares to run private queries over an entire table in addition to a single data record. We illustrate here with two examples.

Example: COUNT query. Suppose that the user wants to run the following query on a table served by Splinter:

```
SELECT COUNT(*) FROM items WHERE ItemId = ?
```

Here, '?' denotes a parameter that the user would like to keep private; for example, suppose the user is searching for `ItemId = 5`, but does not want to reveal this value.

To run this query, the Splinter client defines a point function $f(x) = 1$ if $x = 5$ or 0 otherwise. It then divides this function into function shares $f_1, \ldots, f_k$ and distributes

ItemId	Price	f_1(ItemId)	f_2(ItemId)
5	8	10	-9
1	8	3	-3
5	9	10	-9

Figure 3-3: Simple example table with outputs for the FSS function shares f_1, f_2 applied to the ItemId column. The function is a point function that returns 1 if the input is 5, and 0 otherwise. All outputs are integers modulo 2^m for some m.

them to the k providers, as shown in Figure 3-2. For simplicity, suppose that there are two providers, who receive shares f_1 and f_2. Because these shares are additive, we know that $f_1(x) + f_2(x) = f(x)$ for every input x. Thus, each provider p can compute $f_p(\text{ItemId})$ for every ItemId in the database table, and send back $r_p = \sum_{i=1}^{n} f_p(\text{ItemId}_i)$ to the client where n is the number of database records. The client then computes $r_1 + r_2$, which is equal to $\sum_{i=1}^{n} f(\text{ItemId}_i)$, that is, the count of all matching records in the table.

To make this more concrete, Figure 3-3 shows an example table and some sample outputs of the function shares, f_1 and f_2, applied to the ItemId column. There are a few important observations. First, to each provider, the outputs of their function share seem random. Consequently, the provider does not learn the original function f and the parameter "5". Second, because f evaluates to 1 on inputs of 5, $f_1(\text{ItemId}) + f_2(\text{ItemId}) = 1$ for rows 1 and 3. Similarly, $f_1(\text{ItemId}) + f_2(\text{ItemId}) = 0$ for row 2. Therefore, when summed across the providers, each row contributes 1 (if it matches) or 0 (if it does not match) to the final result. Finally, each provider aggregates the outputs of their shares by summing them. In the example, one provider returns 23 to the client, and the other returns -21. The sum of these is the correct query output, 2.

This additivity of FSS enables Splinter to have *low communication costs* for aggregate queries, by aggregating data locally on each provider.

Example: SUM query. Suppose that instead of a COUNT, we wanted to run the following SUM query:

```
SELECT SUM(Price) FROM items WHERE ItemId=?
```

This query can be executed privately with a small extension to the COUNT scheme. As in COUNT, we define a point function f for our secret predicate, e.g., $f(x) = 1$ if $x = 5$ and 0 otherwise. We divide this function into shares f_1 and f_2. However, instead of computing $r_p = \sum_{i=1}^{n} f_p(\text{ItemId}_i)$, each provider p computes

$$r_p = \sum_{i=1}^{n} f_p(\text{ItemId}_i) \cdot \text{Price}_i$$

Query format:

SELECT $aggregate_1$, $aggregate_2$, ...
FROM *table*
WHERE *condition*
[GROUP BY $expr_1$, $expr_2$, ...]

aggregate:

- COUNT | SUM | AVG | STDEV (*expr*)
- MAX | MIN (*expr*)
- TOPK (*expr*, *k*, *sort_expr*)
- HISTOGRAM (*expr*, *bins*)

condition:

- $expr = secret$
- $secret_1 \leq expr \leq secret_2$
- AND of '=' conditions and up to one interval
- OR of multiple disjoint conditions
  (e.g., `country="UK" OR country="USA"`)

expr: any public function of the fields in a table row
(e.g., `ItemId + 1` or `Price * Tax`)

Figure 3-4: Splinter query format. The TOPK aggregate returns the top k values of *expr* for matching rows in the query, sorting them by *sort_expr*. In conditions, the parameters labeled *secret* are hidden from the providers.

As before, $r_1 + r_2$ is the correct answer of the query, that is, $\sum_{i=1}^{n} f(\text{ItemId}_i) \cdot \text{Price}_i$. We add in each row's price, Price_i, 0 times if the ItemId is equal to 5, and 1 time if it does not equal 5.

3.4 Splinter Query Model

Beyond the simple SUM and COUNT queries in the previous section, we have developed protocols to execute a large class of queries using FSS, including non-additive aggregates such as MAX and MIN, and queries that return multiple individual records instead of an aggregate. For all these queries, our protocols are efficient in both computation and communication. On a database of n records, all queries can be executed in $O(n \log n)$ time and $O(\log n)$ communication rounds, and most only require 1 or 2 communication rounds (Figure 3-6 on page 59).

Figure 3-4 describes Splinter's supported queries using SQL syntax. Most operators are

self-explanatory. The only exception is TOPK, which is used to return up to k individual records matching a predicate, sorting them by some expression *sort_expr*. This operator can be used to implement `SELECT...LIMIT` queries, but we show it as a single "aggregate" to simplify our exposition. To keep the number of matching records hidden from providers, the protocol always pads its result to exactly k records.

Although Splinter does not support all of SQL, we found it expressive enough to support many real-world query services over public data. We examined various websites, including Yelp, Hotels.com, and Kayak, and found we can support most of their search features as shown in Section 3.8.1.

Finally, Splinter only "natively" supports fixed-width integer data types. However, such integers can also be used to encode strings and fixed-precision floating point numbers (e.g., SQL DECIMALs). For strings in predicates, we can also encode them using hashes. We use them to represent other types of data in our sample applications.

3.5 Executing Splinter Queries

Given a query in Splinter's query format (Figure 3-4), the system executes it using the following steps:

1. The Splinter client builds function shares for the condition in the query, as we shall describe in Section 3.5.1.

2. The client sends the query with all the secret parameters removed to each provider, along with that provider's share of the condition function.

3. If the query has a GROUP BY, each provider divides its data into groups using the grouping expressions; otherwise, it treats the whole table as one group.

4. For each group and each aggregate in the query, the provider runs an evaluation protocol that depends on the aggregate function and on properties of the condition. We describe these protocols in Section 3.5.2. Some of the protocols require further communication with the client, in which case the provider batches its communication for all grouping keys together.

The main challenge in developing Splinter is designing efficient execution protocols for Splinter's complex conditions and aggregates (Step 4). Our contribution is multiple protocols that can execute non-additive aggregates with low computation and communication costs.

One key insight that pervades our design is that *the best strategy to compute each aggregate depends on properties of the condition function*. For example, if we know that the condition can only match one value of the expression it takes as input, we can simply

compute the aggregate's result for *all* distinct values of the expression in the data, and then use a point function to return just one of these results to the client. On the other hand, if the condition can match multiple values, we need a different strategy that can combine results across the matching values. To reason about these properties, we define three *condition classes* that we then use in aggregate evaluation.

3.5.1 Condition Types and Classes

For any condition c, the Splinter client defines a function f_c that evaluates to 1 on rows where c is true and 0 otherwise, and divides f_c into shares for each provider. Given a condition c, let $E_c = (e_1, \ldots, e_t)$ be the list of expressions referenced in c (the *expr* parameters in its clauses). Because the best strategy for evaluating aggregates depends on c, we divide conditions into three classes:

- *Single-value conditions.* These are conditions that can only be true on one combination of the values of $(e_1, \ldots, e_t)$. For example, conditions consisting of an AND of '=' clauses are single-value.
- *Interval conditions.* These are conditions where the input expressions $e_1, \ldots, e_t$ can be ordered such that c is true on an interval of the range of values $e_1||e_2||\ldots||e_t$ (where || denotes string concatenation).
- *Disjoint conditions,* i.e., all other conditions.

The condition types described in our query model (Figure 3-4) can all be converted into sharable functions, and categorized into these classes, as follows:

Equality-only conditions. Conditions of the form $e_1 = secret_1$ AND ... AND $e_t = secret_t$ can be executed as a single point function on the binary string $e_1||\ldots||e_t$. This is simply a point function that can be shared using existing FSS schemes [19]. These conditions are also single-value.

Interval and equality. Conditions of the form $e_1 = secret_1$ AND ... AND $e_{t-1} = secret_{t-1}$ AND $secret_t \leq e_t \leq secret_{t+1}$ can be executed as a single interval function on the binary string $e_1||\ldots||e_t$. This is again supported by existing FSS schemes [19], and is an interval condition.

Disjoint OR. Suppose that $c_1, \ldots, c_t$ are *disjoint* conditions that can be represented using functions $f_{c_1}, \ldots, f_{c_t}$. Then $c = c_1$ OR... OR c_t is captured by $f_c = f_{c_1} + \ldots + f_{c_t}$. We share this function across providers by simply giving them shares of the underlying functions f_{c_i}. In the general case, however, c is a disjoint condition where we cannot say much about which inputs give 0 or 1.

3.5.2 Aggregate Evaluation

Sum-Based Aggregates

To evaluate SUM, COUNT, AVG, STDEV and HISTOGRAM, Splinter sums one or more values for each row regardless of the condition function class. For SUM and COUNT, each provider sums the expression being aggregated or a 1 for each row and multiplies it by $f_i(\text{row})$, its share of the condition function, as in Section 3.3.2. Computing AVG(x) for an expression x, requires finding SUM(x) and COUNT(x), while computing STDEV(x) requires finding these values and SUM(x^2). Finally, computing a HISTOGRAM into bin boundaries provided by the user simply requires tracking one count per bin, and adding each row's result to the count for its bin. Note that the binning expression is not private—only information about which rows pass the query's condition function.

MAX and MIN

Suppose we are given a query to find MAX(e_0) WHERE $c(e_1, \ldots, e_t)$, for expressions $e_0, \ldots, e_t$. The best evaluation strategy depends on the class of the condition c.

Single-value conditions. If c is only true for one combination of the values $e_1, \ldots, e_t$, each provider starts by evaluating the query

`SELECT MAX(`e_0`) FROM data GROUP BY` $e_1, \ldots, e_t$

This query gives an *intermediate table* with the tuples $(e_1, \ldots, e_t)$ as keys and MAX(e_0) as values. Next, each provider computes $\sum \text{MAX}(e_0) \cdot f_i(e_1, \ldots, e_t)$ across the rows of the intermediate table, where f_i is its share of the condition function. This sum will add a 0 for each non-matching row and MAX(e_0) for the matching row, thus returning the right value. Note that if the original table had n rows, the intermediate table can be built in $O(n)$ time and space using a hash table.

Interval conditions. Suppose that c is true if and only if $e_1 || \ldots || e_t$ is in an interval $[a, b]$, where a and b are secret parameters. As in the single-value case, the providers can build a data structure that helps them evaluate the query without knowing a and b.

In this case, each provider builds an array A of entries (k, v), where the keys are all values of $e_1 || \ldots || e_t$ in lexicographic order, and the values are MAX(e_0) for each key. It then computes MAX($A[i..j]$) for all *power-of-2 aligned* intervals of the array A (Figure 3-5). This data structure is similar to a Fenwick tree [36].

Query evaluation then proceeds in two rounds. First, Splinter counts how many keys in A are less than a and how many are less than b: the client sends the providers shares of the interval functions $k \in [0, a-1]$ and $k \in [0, b-1]$, and the providers apply these

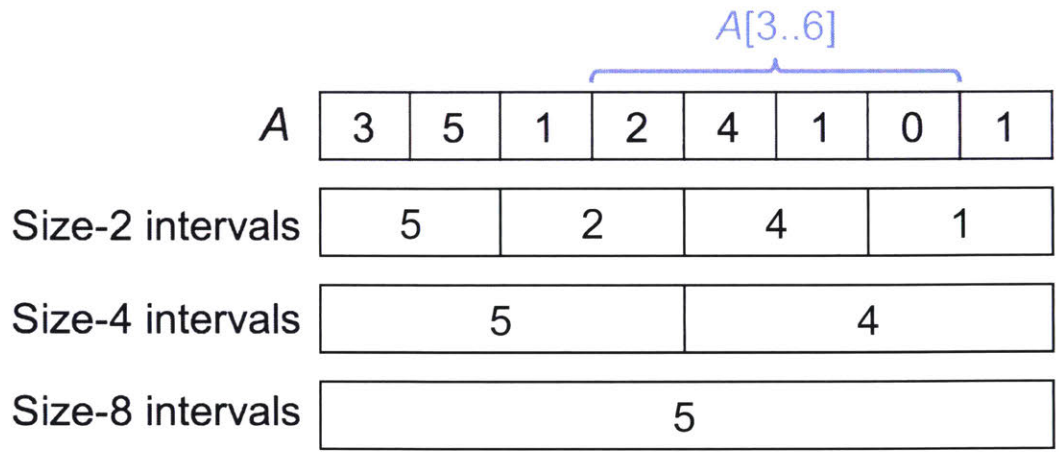


Figure 3-5: Data structure for querying MAX on intervals. We find the MAX on each power-of-2 aligned interval in the array, of which there are $O(n)$ total. Then, any interval query requires retrieving $O(\log n)$ of these values. For example, to find $MAX(A[3..6])$, we need two size-1 intervals and one size-2.

to all keys k and return their results. This lets the client find indices i and j in A such that all the keys $k \in [a, b]$ are in $A[i..j]$.

Second, the client sends each provider shares of new point functions that select up to two intervals of size 1, up to two intervals of size 2, etc out of the power-of-2 sized intervals that the providers computed MAXes on, so as to cover exactly $A[i..j]$. Note that any integer interval can be covered using at most 2 intervals of each power of 2. The providers evaluate these functions to return the MAXes for the selected intervals, and the client combines these $O(\log n)$ MAXes to find the overall MAX on $A[i..j]$.[2]

For a table of size n, this protocol requires $O(n \log n)$ time at each provider (to sort the data to build A, and then to answer $O(\log n)$ point function queries). It also only requires two communication rounds, and $O(\log n)$ communication bandwidth. The same protocol can be used for other associative aggregates, such as products.

Disjoint conditions. If we must find MAX(e_0) WHERE $c(e_1, \ldots, e_t)$ but know nothing about c, Splinter builds an array A of all rows in the dataset sorted by e_0. Finding MAX(e_0) WHERE c is then equivalent to finding the largest index i in A such that $c(A[i])$ is true. To do this, Splinter uses binary search. The client repeatedly sends private queries of the form

```
SELECT COUNT(*) FROM A
WHERE c(e_1,...,e_t) AND index ∈ [secret_1, secret_2],
```

[2] To hide which sizes of intervals were actually required, the client should always request 2 intervals of each size and ignore unneeded ones.

where *index* represents the index of each row in A and the interval for it is kept private. By searching for secret intervals in decreasing power-of-2 sizes, the client can find the largest index i such that $c(A[i])$ is true. For example, if we had an array A of size 8 with largest matching element at $i = 5$, the client would probe $A[0..3]$, $A[4..7]$, $A[4..5]$, $A[6..7]$ and finally $A[4]$ to find that 5 is the largest matching index.

Normally, ANDing the new condition $index \in [secret_1, secret_2]$ with c would cause problems, because the resulting conditions might no longer be in Splinter's supported condition format (ANDs with at most one interval and ORs of disjoint clauses). Fortunately, because the intervals in our condition are always power-of-2 aligned, it can also be written as an equality on the first k bits of *index*. For example, supposing that *index* is a 3-bit value, the condition $index \in [4, 5]$ can be written as $index_{0,1} =$ "10", where $index_{0,1}$ is the first two bits of *index*. This lets us AND the condition into all clauses of c.

Once the client has found the largest matching index i, it runs one more query with a point function to select the row with $index = i$. The whole protocol requires $O(\log n)$ communication rounds and $O(n \log n)$ computation and works well if c has many conditions.

However, if c has a small number of OR clauses, an optimization is to run one query for each clause in parallel. The user then resolves the responses locally to find the answer to the original query. Although doing this optimization requires more bandwidth because the returned result size is larger, it avoids the $O(\log n)$ communication rounds and the $O(n \log n)$ computation.

TOPK

Our protocols for evaluating TOPK are similar to those for MAX and MIN. Suppose we are given a query to find TOPK(e, k, e_{sort}) WHERE $c(e_1, \ldots, e_t)$. The evaluation strategy depends on the class of the condition c.

Single-value conditions. If c is only true for one combination of $e_1, \ldots, e_t$, each provider starts by evaluating

```
SELECT TOPK(e, k, e_sort) FROM data
GROUP BY e_1,...,e_t
```

This gives an intermediate table with the tuples $(e_1, \ldots, e_t)$ as keys and TOPK($\cdot$) for each group as values, from which we can select the single row matching c as in MAX.

Interval conditions. Here, the providers build the same auxiliary array A as in MAX, storing the TOPK for each key instead. They then compute the TOPKs for power-of-2 aligned intervals in this array. The client finds the interval $A[i..j]$ it needs to query,

extracts the top k values for power-of-2 intervals covering it, and finds the overall top k. As in MAX, this protocol requires 2 rounds and $O(\log n)$ communication bandwidth.

Disjoint conditions. Finding TOPK for disjoint conditions is different from MAX because we need to return multiple records instead of just the largest record in the table that matches c. This protocol proceeds as follows:

1. The providers sort the whole table by e_{sort} to create an auxiliary array A.
2. The client uses binary search to find indices i and j in A such that the top k items matching c are in $A[i..j]$. This is done the same way as in MAX, but searching for the largest indices where the count of later items matching c is 0 and k.
3. The client uses a sampling technique (Section 3.5.3) to extract the k records from $A[i..j]$ that match c. Intuitively, although we do not know which rows these are, we build a result table of $> k$ values initialized to 0, and add the FSS share for each row of the data to one row in the result table, chosen by a hash. This scheme extracts all matching records with high probability.

This protocol needs $O(\log n)$ communication rounds and $O(n \log n)$ computation if there are many clauses, but like the protocol for MAX, if the number of clauses in c is small, the user can issue parallel queries for each clause to reduce the communication rounds and computation.

3.5.3 Extracting Disjoint Records with FSS

Here, we describe our sampling-based technique for returning multiple records using FSS, used in TOPK queries with disjoint conditions (Section 3.5.2). Given a table T of records and a condition c that matches up to k records, we wish to return those records to the client with high probability without revealing c.

To solve this problem, the providers each create a result table R of size $l > k$, containing (value, count) columns all initialized to 0. They then iterate through the records and choose a result row to update for each record based on a hash function h of its index i. For each record r, each provider adds $1 \cdot f_c(r)$ to $R[h(i)]$.count and $r \cdot f_c(r)$ to $R[h(i)]$.value, where f_c is its share of the condition c. The client then adds up the R tables from all the providers to build up a single table, which contains a value and count for all indices that a record matching c hashed into.

Given this information, the client can tell how many records hashed into each index: entries with count=1 have only one record, which can be read from the entry's value. Unfortunately, entries with higher counts hold multiple records that were added together in the value field. To recover these entries, the client can run the same process multiple times in parallel with different hash functions h.

Aggregate	Condition	Time	Rounds	Bandwidth
Sum-based	any	$O(n)$	1	$O(1)$
MAX/MIN	1-value	$O(n)$	1	$O(1)$
MAX/MIN	interval	$O(n \log n)$	2	$O(\log n)$
MAX/MIN	disjoint	$O(n \log n)$	$O(\log n)$	$O(\log n)$
TOPK	1-value	$O(n)$	1	$O(1)$
TOPK	interval	$O(n \log n)$	2	$O(\log n)$
TOPK	disjoint	$O(n \log n)$	$O(\log n)$	$O(\log n)$

Figure 3-6: Complexity of Splinter's query evaluation protocols for a database of size n. For bandwidth, we report the multiplier over the query's normal result size.

In general, for any given value of r and k, the probability of a given record colliding with another under each hash function is a constant (e.g., it is less than $1/3$ for $r = 3k$). Repeating this process with more hash functions causes the probability to fall exponentially. Thus, for any k, we can return all the distinct results with high probability using only $O(\log k)$ hash functions and hence only $O(\log k)$ extra communication bandwidth.

3.5.4 Complexity

Figure 3-6 summarizes the complexity of Splinter's query evaluation protocols based on the aggregates and condition classes used. We note that in all cases, the computation time is $O(n \log n)$ and the communication costs are smaller than the size of the database. This makes Splinter practical even for databases with millions of records, which covers many common web application datasets, as shown in Section 3.8. Finally, the main operations used to evaluate Splinter queries at providers, namely sorting and sums, are highly parallelizable.

3.6 Optimized FSS Implementation

Apart from introducing new protocols to evaluate complex queries using FSS, Splinter includes an FSS implementation optimized for modern hardware.

The two-party FSS protocol [19] is efficient because of its use of one-way functions. A common class of one-way functions is pseudorandom generators (PRGs) [60], and in practice, AES is the most commonly used PRG because of hardware accelerations, i.e. the AES-NI [107] instruction. Generally, using AES as a PRG is straightforward (use AES in counter mode). However, the use of PRGs in FSS is not only atypical, but it also represents a large portion of the computation cost in the protocol. The FSS protocol requires many instantiations of a PRG with different initial seed values, especially in

the two-party protocol [19]. Initializing multiple PRGs with different seed values is very computationally expensive because AES cipher initialization is *much slower* than performing an AES evaluation on an input. Therefore, the challenge in Splinter is to find an efficient PRG for FSS.

Our solution is to use *one-way compression functions*. One way compression functions are commonly used as a primitive in hash functions, like SHA, and are built using a block cipher like AES. In particular, Splinter uses the Matyas-Meyer-Oseas one-way compression function [69] because this function utilizes a *fixed key* cipher. As a result, the Splinter protocol initializes the cipher only once per query.

More precisely, the Matyas-Meyer-Oseas one-way compression function is defined as:

$$F(x) = E_k(x) \oplus x$$

where x is the input, i.e. PRG seed value, and E is a block cipher with a fixed key k.

The output of a one-way compression function is a fixed number of bits, but we can use multiple one-way compression functions with different keys and concatenate the outputs to obtain more bits. Security is preserved because a function that is a concatenation of one-way functions is still a one-way function.

With this one-way compression function, Splinter initializes the cipher, E_k, at the beginning of the query and reuses it for the rest of the query, avoiding expensive AES initialization operations in the FSS protocol. For each record, the Splinter protocol needs to perform only n XORs and n AES evaluations using the AES-NI instruction, where n is the input domain size of the record. In Section 3.8.5, we show that Splinter's use of one-way compression functions results in a 2.5× speedup over using AES directly as a PRG.

3.7 Implementation

We implemented Splinter in C++, using OpenSSL 1.0.2e [89] and the AES-NI hardware instructions for AES encryption. We used GMP [38] for large integers and OpenMP [88] for multithreading. Our optimized FSS library is about 2000 lines of code, and the applications on top of it are about 2000 lines of code. There is around 1500 lines of test code to issue the queries. Our FSS library implementation can be found at https://github.com/frankw2/libfss.

Dataset	Query Desc.	FSS Scheme	Input Bits	Round Trips	Query Size	Response Size	Response Time
Restaurant	COUNT of Thai restaurants (Q1)	Two-party Multi-party	11	1	~2.75 KB ~10 KB	~0.03 KB ~18 KB	57 ms 52 ms
Restaurant	Top 10 Mexican restaurants near user (Q2)	Two-party Multi-party	22	1	~16.5 KB ~1.9 MB	~7 KB ~0.21 KB	150 ms 542 ms
Restaurant	Best rated restaurant in category subset (Q3)	Two-party Multi-party	11	11	~244 KB ~880 KB	~0.7 KB ~396 KB	1.3 s 1.6 s
Flights	AVG monthly price for a certain flight route (Q1)	Two-party Multi-party	17	1	~8.5 KB ~160 KB	~0.06 KB ~300 KB	1.0 s 1.2 s
Flights	Top 10 cheapest flights for a route (Q2)	Two-party Multi-party	13	1	~3.25 KB ~20 KB	~0.3 KB ~0.13 KB	30 ms 39 ms
Maps	Routing query on NYC map	Two-party Multi-party	Grid: 14 Transit Node: 22	2	~12.5 KB ~720 KB	~31 KB ~1.1 KB	1.2 s 1.0 s

Figure 3-7: Performance of various queries in our case study applications on Splinter. Response times include 14 ms network latency per network round trip. All subqueries are issued in parallel unless they depend on a previous subquery. Query and response sizes are measured per provider. For the multi-party FSS scheme, we run 3 parties. Input bits represent the number of bits in the input domain for FSS, i.e., the maximum size of a column value.

3.8 Evaluation

We built and evaluated clones of three applications on Splinter: Yelp clone, flight price lookup, and map routing, using real datasets. We also compared Splinter to previous private systems, and estimate hosting costs. Our providers ran on 64-core Amazon EC2 `x1` servers with Intel Xeon E5-2666 Haswell processors and 1.9 TB of RAM. The client was a 2 GHz Intel Core i7 machine with 8 GB of RAM. Our client's network latency to the providers was 14 ms.

Overall, our experiments show the following:

- Splinter can support realistic applications including the search features of Yelp and flight search sites, and data structures required for map routing.
- Splinter achieves end-to-end latencies below 1.6 seconds for queries in these applications on realistic data.
- In most cases, Splinter's protocols are more efficient than those of the most recent practical private query system by Olumofin et al. [84].

3.8.1 Case Studies

Here, we discuss the three application clones we built on Splinter. Figure 3-7 summarizes our results, and Figure 3-8 describes the sizes and characteristics of our three datasets.

Dataset	# of rows	Size (MB)	Cardinality
Yelp [131]	225,000	23	900 categories
Flights [33]	6,100,000	225	5000 flights
NYC Map [28]	260,000 nodes 733,000 edges	300	1333 transit nodes

Figure 3-8: Datasets used in the evaluation. The cardinality of queried columns affects the input bit size in our FSS queries.

Finally, we also review the search features available in real websites to study how many Splinter supports.

Restaurant review site: We implement a restaurant review site using the Yelp academic dataset [131]. The original dataset contains information for local businesses in 10 cities, but we duplicate the dataset 4 times so that it would approximately represent local businesses in 40 cities. We use the following columns in the data to perform many of the queries expressible on Yelp: name, stars, review count, category, neighborhood and location.

For location-based queries, e.g., restaurants within 5 miles of a user's current location, multiple interval conditions on the longitude and latitude would typically be used. To run these queries faster, we quantize the locations of each restaurant into overlapping hexagons of different radii (e.g., 1, 2 and 5 miles), following the scheme from [79]. We precompute which hexagons each restaurant is in and expose these as additional columns in the data (e.g., `hex1mi` and `hex2mi`). This allows the location queries to use '=' predicates instead of intervals.

For this dataset, we present results for the following three queries:

```
Q1: SELECT COUNT(*) WHERE category="Thai"

Q2: SELECT TOP 10 restaurant
WHERE category="Mexican" AND (hex2mi=1 OR hex2mi=2 OR hex2mi=3)
ORDER BY stars

Q3: SELECT restaurant, MAX(stars)
WHERE category="Mexican" OR category="Chinese" OR category="Indian"
OR category="Greek" OR category="Thai" OR category="Japanese"
GROUP BY category
```

Q1 is a count on the number of Thai restaurants. Q2 returns the top 10 Mexican restaurants within a 2 mile radius of a user-specified location by querying three hexagons.

We assume that the provider caches the intermediate table for the Top 10 query as described in Section 3.5.2 because it is a common query. Finally, Q3 returns the best rated restaurant from a subset of categories. This requires more communication than other queries because it performs a MAX with many disjoint conditions, as described in Section 3.5.2. Although most queries will probably not have this many disjoint conditions, we test this query to show that Splinter's protocol for this case is also practical.

Note that for Q2 and Q3, the communication costs will be higher compared to Q1 because in Q2 and Q3, we are returning ASCII-encoded strings of the restaurant names rather than just an integer in Q1.

Flight search: We implement a flight search service similar to Kayak [55], using a public flight dataset [33]. The columns are flight number, origin, destination, month, delay, and price. To find a flight, we search by origin-destination pairs. We present results for two queries:

```
Q1: SELECT AVG(price) WHERE month=3
AND origin=1 AND dest=2

Q2: SELECT TOP 10 flight_no
WHERE origin=1 and dest=2 ORDER BY price
```

Q1 shows the average price for a flight during a certain month. Q2 returns the top 10 cheapest flights for a given source and destination, which we encode as integers. Since this is a common query, the results in Figure 3-7 assume a cached Top 10 intermediate table.

Map routing: We implement a private map routing service, using real traffic map data from DIMACS [28] for New York City. However, implementing map routing in Splinter is difficult because the providers can perform only a restricted set of operations. The challenge is to find a shortest path algorithm compatible with Splinter. Fortunately, extensive work has been done to optimize map routing [10]. One algorithm compatible with Splinter is transit node routing (TNR) [8, 12], which has been shown to work well in practice [11]. In TNR, the provider divides up a map into grids, which contain at least one transit node, i.e. a transit node that is part of a "fast" path. There is also a separate table that has the shortest paths between all pairs of transit nodes, which represent a smaller subset of the map. To execute a shortest path query for a given source and destination, the user can use FSS to download the paths in her source and destination grid. She locally finds the shortest path to the source transit node and destination transit node. Finally, she queries the provider for the shortest path between the two transit nodes.

FSS scheme	Grid	Transit Node	Total
Two Party	0.35 s	0.85 s	1.2 s
Multi-party	0.15 s	0.85 s	1.0 s

Figure 3-9: Grid, transit node, and total query times for NYC map. A user issues 2 grid queries and one transit node query. The two grid queries are issued together in one message, so there are a total of 2 network round trips.

We used the source code from Arz et al. [8] and identified the 1333 transit nodes. We divided the map into 5000 grids, and calculated the shortest path for all transit node pairs. The grid table has 5000 rows representing the edges and nodes in a grid, and the transit node table has about 800,000 rows representing the number of shortest paths for all transit node pairs.

Figure 3-7 shows the total response time for a routing query between a source and destination in NYC. Figure 3-9 shows the breakdown of time spent on querying the grid and transit node table. One observation is that the multi-party version is slightly faster than the two party version because it is faster at processing the grid query as shown in Figure 3-9. The two-party version of FSS requires using GMP operations, which is slower than integer operations used in the multi-party version, but the two-party version requires less bandwidth.

Splinter has response times of 50 ms to 1.6 seconds. Although these response times are much higher compared to a system without FSS and Splinter, privacy-sensitive users are often willing to trade some performance for better security. For example, fetching a website on Tor takes 3-4 seconds [123]. Therefore, we believe that our performance is acceptable.

3.8.2 Communication Costs

Figure 3-7 shows the total bandwidth of a query request and response for the various case study queries. The sum of those two values represents total bandwidth between the providers and user.

There are two main observations. First, both the query and response sizes are *much smaller* than the size of the database in most cases. Second, for non-aggregate queries, the multi-party protocol has a smaller response size compared to the two-party protocol but the query size is much larger than the two-party protocol, leading to higher overall communication. For aggregate queries, the multi-party FSS scheme is only xor homomorphic, so it outputs all the matches for a specific predicate/condition. The user has to perform the aggregation locally, leading to a larger response size than the two-party protocol. Overall, the multi-party protocols have higher total bandwidth compared to

the two-party protocols despite some differences in response size. However, FSS is a relatively new cryptographic primitive, especially compared to PIR and garbled circuits, so we believe that improvements in the FSS protocol could lower these communication costs in the future.

As stated in Section 3.2.3, querying with Splinter and PIR systems might be more efficient than downloading the whole database, assuming there is no rate limiting or query restrictions as described in Section 3.2.3. Query restrictions imposed by data owners will probably lead to more round trips and communication costs compared to downloading the database under normal network conditions. Thus, depending on the specific restrictions, using Splinter might be more efficient than attempting to download the whole database under restricted network conditions.

To better quantify the "break even" point, i.e. where the communication costs are equal to the database size, we look at our case study datasets. For the Yelp clone, we assume that the user downloads only her city (not all 40). For two-party Restaurant Q1, it will take about 250 of these types of queries before reaching that point. For multi-party Restaurant Q1 and two-party Restaurant Q2, it would take about 25 queries. For multi-party Restaurant Q2 and Restaurant Q3, it would take about 1 query to reach that point. However, users tend to issue different kinds of queries and updates might happen, it is not obvious whether downloading the whole database or using Splinter would be more efficient for this case study. Moreover, the purpose of this case study is to compare Splinter's performance on smaller datasets to prior systems and to larger datasets. For flights, it would take about 550 queries for multi-party Flights Q1 and 50,000 queries for the other flight queries. Finally, for maps, it would take 25,000 queries for the two-party version and 2500 for the multi-party version. However, these two databases are larger than Yelp and change more frequently, so it might not make sense to download the database. We discuss Splinter-amenable web services in more detail in Section 3.2.3.

3.8.3 Coverage of Supported Queries

We also manually characterized the applicability of Splinter to several widely used online services by studying how many of the search fields on these services' interfaces Splinter can support. Figure 3-10 shows the results. Most services use equality and range predicates: for example, the Hotels.com user interface includes checkboxes for selecting categories, neighborhoods, stars, etc, a range fields for price, and one free-text search field that Splinter does not support. In general, all features except free-text search could be supported by Splinter. For free-text search, simple keywords that map to a category (e.g., "grocery store") could also be supported.

Website	Search Feature	Splinter Primitive
Yelp	Booking Method, Cities, Distance	Equality
	Price	Range
	Best Match, Top Rated, Most Reviews	Sorting
	Free text search	—
Hotels.com	Destination, Room type, Amenities	Equality
	Check in/out, Price, Ratings	Range
	Stars, Distance, Ratings, Price	Sorting
	Name contains	—
Kayak	From/To, Cabin, Passengers, Stops	Equality
	Date, Flight time, Layover time, Price	Range
Google Maps	From/To, Transit type, Route options	Equality

Figure 3-10: Example website search features and their equivalent Splinter query class.

Splinter Query	RTs in [84]	RTs in Splinter
Restaurant Q1	6	1
Restaurant Q2	6	1
Restaurant Q3	6	11
Flights Q1	13	1
Flights Q2	8	1
Map Routing	19	2

Figure 3-11: Round trips required in Olumofin et al. [84] and Splinter.[3]

3.8.4 Comparison to Other Private Query Systems

To the best of our knowledge, the most recent private query system that can perform a similar class of queries as Splinter is that of Olumofin et al. [84], which uses multi-party PIR. In PIR, a user can query for an index i without revealing the index or the result to the servers, making it a more restrictive querying model compared to FSS, but Olumofin et al. develops protocols to extend PIR beyond just index querying. However, FSS can perform many of the complex queries in Olumofin et al. without additional protocols,

[3] The number of round trips in Restaurant Q3 is $O(\log n)$ in both Splinter and Olumofin et al., but the absolute number is higher in Splinter because we use a binary search whereas Olumofin et al. use a 4-ary tree. Splinter could also use a 4-ary search to achieve the same number of round trips, but we have not yet implemented this.

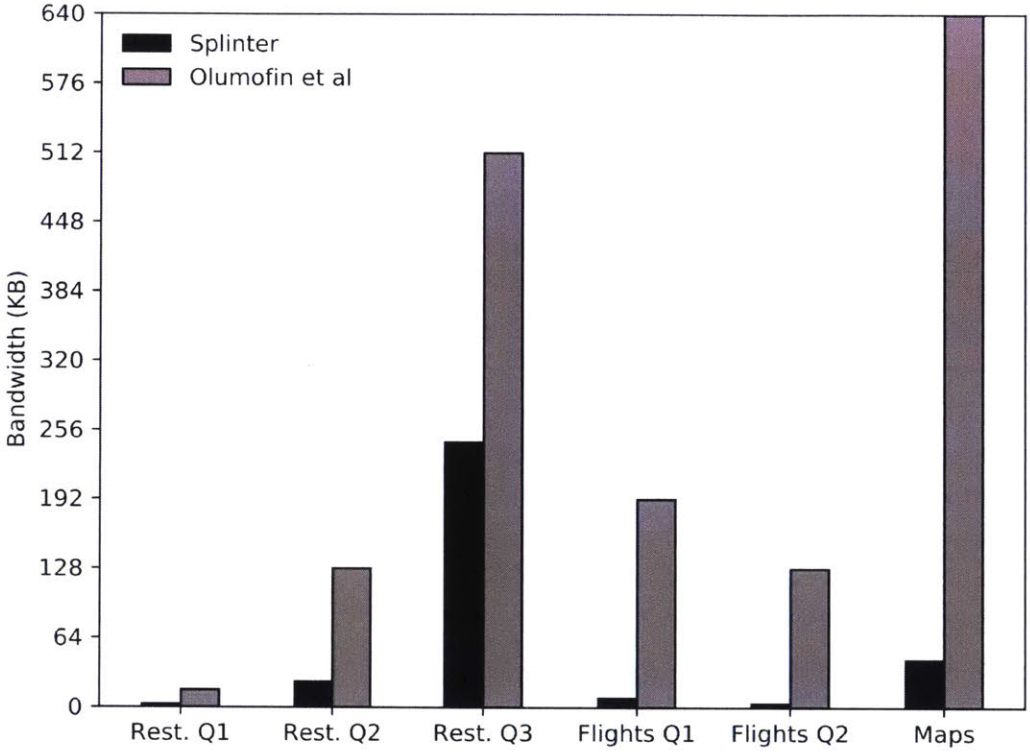


Figure 3-12: Total bandwidth for Splinter and Olumofin et al. [84]

Splinter Query	**Time in [84]**	**Time in Splinter**
Restaurant Q1	80 ms	40 ms
Restaurant Q2	245 ms	130 ms
Restaurant Q3	1.2 s	1.1 s
Flights Q1	10.9 s	0.97 s
Flights Q2	150 ms	15 ms
Map Routing	10.6 s	1.1 s

Figure 3-13: Server-side computation costs for Olumofin et al. [84] and Splinter.

such as COUNT and SUM with non-index predicates.

We implemented the private query protocol in Olumofin et al., ported our case queries, and ran them on the same Amazon AWS setup as Splinter (described at the beginning of this section). We compare the two-party version of Splinter with Olumofin et al. because the system of Olumofin et al. assumes only two parties and does not describe how to extend it to more servers. [4] In particular, we compare Olumofin et al. and Splinter on the following three metrics: number of round trips, bandwidth, and server-side computation. We find that across all of our queries, Splinter is almost always more efficient than Olumofin et al., often by an order of magnitude or more.

Figure 3-11 shows the round trips required in Olumofin et al.'s system and in Splinter for the queries in our case studies. Olumofin et al. creates an m-ary ($m = 4$) B+ index tree for the dataset and uses PIR to extract the results. Consequently, their queries require $O(\log_m n)$ round trips, where n is the number of records. In Splinter, the number of rounds trips does not depend on the size of the database for most queries. As shown in Section 3.5.2, the exception is for MIN/MAX and TOPK queries with many disjoint conditions where Splinter's communication is similar; if there are a small number of disjoint conditions, Splinter will be faster than previous systems because the user can issue parallel queries.

Figure 3-12 shows the total bandwidth required in Olumofin et al.'s system and in Splinter. Note that Olumofin et al. does not have a direct way to support queries with disjoint OR conditions used in Restaurant Q3, so we assumed that they issue a separate query for each OR condition. Splinter has much lower overall communication costs, especially for the queries on the larger flights and maps databases. The main reason for this is that the bandwidth in PIR depends on both the number of database records (specifically a square root factor) and record size whereas in FSS, the bandwidth is independent of the number of records and depends just on the record size. Therefore, the disparity in bandwidth will increase as the database size increases. This larger bandwidth is problematic on mobile networks where data is more expensive.

Figure 3-13 shows the server-side computation costs for both systems. As expected, the difference is minimal on the smaller restaurant database but greater on the larger databases. Although the PIR scheme used in Olumofin et al. has similar performance to FSS, their protocols require more PIR operations per record.

Compared to Splinter, Olumofin et al. also has more round trips for the smaller database, which increases the overall response times. For example, in our experimental setup with 14 ms network latency, Olumofin et al. would incur an additional 70 ms delay versus Splinter for Restaurant Q1 and Restaurant Q2. This delay increases as we move

[4] From our understanding, it is possible for Olumofin et al. to support more than two parties, but server-side computation and bandwidth would increase, most likely eliminating effects of the optimizations described in their paper.

to mobile networks. If we replace the client with a mobile device on a 4G network with latency of approximately 100 ms [90], the restaurant queries would incur an additional 500 ms delay in Olumofin et al. compared to Splinter. For bigger databases, the number of round trips increases, so the total amount of latency incurred will also increase. For instance, for maps, the additional latency on Olumofin et al. would be about 1.7 seconds.

3.8.5 FSS Microbenchmarks

Cryptographic operations are the main cost in Splinter. We present microbenchmarks to show these costs of various parts of the FSS protocol, tradeoffs between various FSS protocols, and the throughput of FSS. The microbenchmarks also show why the response times in Figure 3-7 are different between the two-party and multi-party FSS cases. All of these experiments are done on one core to show the per-core throughput of the FSS protocol.

Two-party FSS: For two-party FSS, generating a function share takes less than 1 ms. The speed of FSS evaluation is proportional to the size of the input domain, i.e. number of bits per record. We can perform around 700,000 FSS evaluations per second on 24-bit records, i.e. process around 700,000 distinct 24-bit records, using one-way compression functions. Figure 3-14 shows the per-core throughput of our implementation for different FSS schemes, i.e. number of unique database records that can be processed per second. It also shows that using one-way compression functions as described in Section 3.6, we obtain a 2.5× speedup over using AES as a PRG.

Multi-party FSS: As shown in Figure 3-14, for the multi-party FSS scheme from [19], the time to generate the function share and evaluate it is proportional to $2^{n/2}$ where n is the number of bits in the input domain. The size of the share scales with $2^{n/2}$ rather than just n in the two-party case. An important observation is that using one-way compression functions instead of AES does not make a significant difference for multi-party FSS because the PRG is called less often compared to two-party FSS. For small input domains (< 20 bits), the multi-party version of FSS is faster than the 2-party version, but a provider cannot aggregate locally for SUM and COUNT queries in the multi-party version.

3.8.6 Hosting Costs

We estimate Splinter's server-side computation cost on Amazon AWS, where the cost of a CPU-second using Amazon Lambda is about 0.005 cents. The cost of storage and running a web server can be amortized over requests. We found that most of our queries cost less than 0.005 cents. Map queries are a bit more costly, about 0.05 cents to run

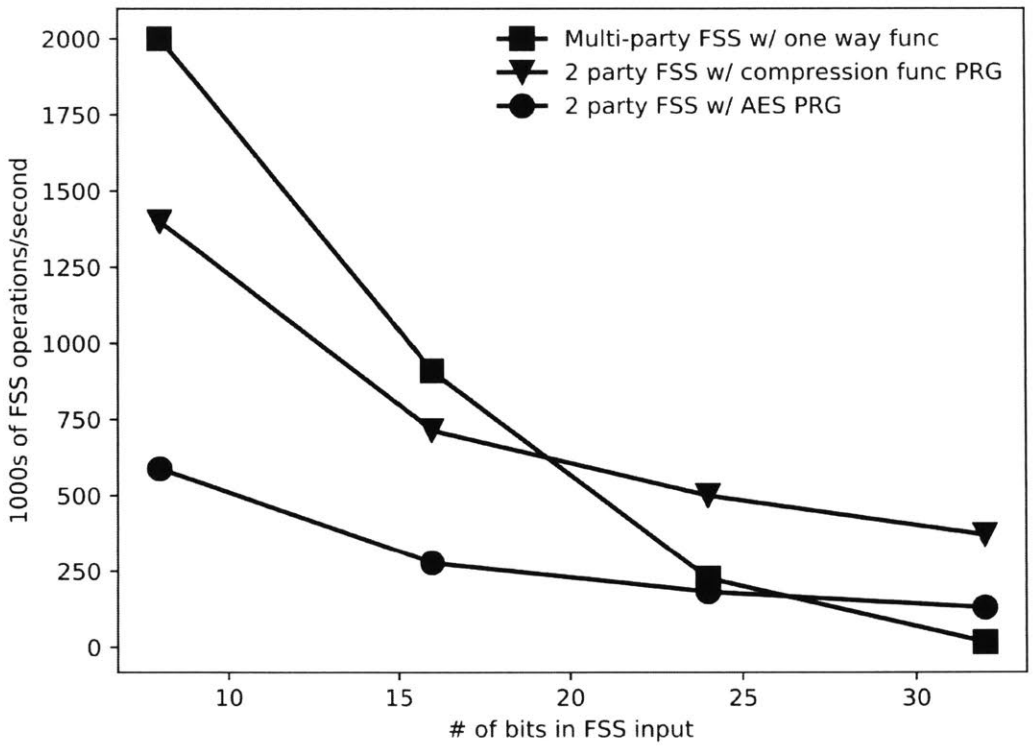


Figure 3-14: Per-core throughput of various FSS protocols. The graph shows the number of FSS operations that can be performed, i.e. database records processed, per second for various input sizes, on one core.

a shortest path query for NYC, because the amount of computation required is higher. With the decreasing cost of cloud computing resources [6], we expect even lower costs in the future. Although there are other costs associated with running a web service, our results show that Splinter's server-side computation costs are very reasonable.

3.9 Discussion and Limitations

Economic feasibility: Although it is hard to predict real-world deployment, we believe that Splinter's low cost makes it economically feasible for several types of applications. Here are some possible methods for monetization. For example, despite many current data owners, such as Yelp and Google Maps, generating revenue primarily by showing ads and mining user data, they can license their data to Splinter providers and have these providers manage a Splinter deployment. The providers can then charge a subscription fee, e.g. $1 a month, for usage of the server. Similarly, these providers can collectively issue a utility token that can be used to pay for the queries. Splinter's trust model, where

only one provider needs to be honest, also makes it easy for new providers to join the market, increasing users' privacy.

This business model seems reasonable as studies have shown that many consumers are willing to pay for services that protect their privacy [49, 106]. In fact, users might not use certain services because of privacy concerns [102, 105]. Similarly, more users are using sites like DuckDuckGo and technologies like Tor because they are unwilling to have sites track their query behavior, which shows a growing consumer market for privacy-preserving technologies. However, whether such a business model would work or be feasible in practice is beyond the scope of this dissertation.

Unsupported queries: As shown in Section 3.4, Splinter supports only a subset of SQL. Splinter does not support partial text matching or image matching, which are common in types of applications that might use Splinter. Moreover, Splinter cannot support private joins, i.e. Splinter can only support joining with another table if the join condition is public, which encompasses a large majority of join operations. Despite these limitations, our study in Section 3.8.3 shows Splinter can support many application search interfaces.

Number of providers: One limitation of Splinter is that a Splinter-based service has to be deployed on at least two providers. However, previous practical PIR systems described in Section 3.10 also require at least two providers.

Full table scans: FSS, like PIR, requires scanning the whole input dataset on every Splinter query, to prevent providers from figuring out which records have been accessed. Despite this limitation, we have shown that Splinter is practical on large real-world datasets, such as maps.

Splinter needs to scan the whole table only for conditions that contain sensitive parameters. For example, consider the query:

```
SELECT flight from table WHERE src=SFO
AND dst=LGA AND delay < 20
```

If the user does not consider the delay of 20 in this query to be private, Splinter could send it in the clear. The providers can then create an intermediate table with only flights where the delay < 20 and apply the private conditions only to records in this table. In a similar manner, users querying geographic data may be willing to reveal their location at the country or state level but would like to keep their location inside the state or country private.

3.10 Related Work

Splinter is related to work in Private Information Retrieval (PIR), garbled circuit systems, encrypted data systems, and Oblivious RAM (ORAM) systems. Splinter achieves higher performance than these systems through its mapping of database queries to the Function Secret Sharing (FSS) primitive.

PIR systems: Splinter is most closely related to systems that use Private Information Retrieval (PIR) [23] to query a database privately. In PIR, a user queries for the i^{th} record in the database, and the database does not learn the queried index i or the result. Much work has been done on improving PIR protocols [85, 93]. Work has also been done to extend PIR to return multiple records [44], but it is computationally expensive. Our work is most closely related to the system in [84], which implements a parametrized SQL-like query model similar to Splinter using PIR, but requires more computation than Splinter.

Popcorn [45] is a media delivery service that uses PIR to hide user consumption habits from the provider and content distributor. However, Popcorn is optimized for streaming media databases, like Netflix, which have a small number (about 8000) of large records, so Popcorn serves a different purpose than Splinter.

Note that both systems above are designed and optimized, assuming two servers, and it is not obvious that these optimizations hold beyond two servers. Splinter can efficiently support two and three servers because it extends Function Secret Sharing (FSS) [19, 39], which enables executions of complex operations such as SUMs in one round trip.

Garbled circuits: Systems such as Embark [57], BlindBox [112], and private shortest path computation systems [129] use garbled circuits [14, 40] to perform private computation on a single untrusted server. Even with improvements in practicality [13], these techniques still have high computation and bandwidth costs for queries on large datasets because a new garbled circuit has to be generated for each query. (Reusable garbled circuits [41] are not yet practical.)

Encrypted data systems: Systems that compute on encrypted data, like CryptDB [96], Mylar [97], SPORC [34], Depot [66], and SUNDR [61], all try to protect private data against a server compromise, which is a different problem than what Splinter tries to solve. CryptDB is most similar to Splinter because it allows for SQL-like queries over encrypted data. However, all these systems protect against a single, potentially compromised server where the user is storing data privately, but they do not hide data access patterns. In contrast, Splinter hides data access patterns and a user's query parameters but is only designed to operate on a cleartext datasets that is hosted at multiple providers.

ORAM systems: Splinter is also related to systems that use Oblivious RAM [63, 114]. ORAM allows a user to read and write data on an untrusted server without revealing her data access patterns to the server. However, ORAM cannot be easily applied into the Splinter setting. One main requirement of ORAM is that the user can only read data that she has written. In Splinter, the provider hosts a cleartext dataset, not created by any specific user, and many users need to access the same dataset.

3.11 Conclusions

Splinter is a new private query system that protects sensitive parameters in SQL-like queries while scaling to realistic applications. Splinter uses and extends a recent cryptography primitive, Function Secret Sharing (FSS), allowing it to achieve much better performance compared to previous private query systems. We develop protocols to execute complex queries with low computation and bandwidth. As a proof of concept, we have evaluated Splinter with three sample applications—a Yelp clone, map routing, and flight search—and showed that Splinter has low response times from 50 ms to 1.6 seconds with low hosting costs.

FOUR

Conclusion and Future Work

In this dissertation, we presented two systems, Veil and Splinter, to minimize data leakage when a user accesses a web service. These systems have raised interesting questions regarding the practicality of privacy-preserving systems.

Veil is the first platform to allow developers to provide stronger private browsing semantics directly to users. A few key questions remain. How do we handle more complex content like videos? In current version of Veil, we assume that developers create a pool of blinding servers. However, content delivery networks and proxies are becoming more prevalent. How do we leverage this existing infrastructure to make Veil more usable? Is it easy to turn these proxies into blinding servers? What specifically needs to change to allow for this?

Splinter leveraged function secret sharing (FSS) to reduce the overhead associated with private queries compared to previous work. However, open research problems still remain. For example, can private queries scale to billions or trillions of records? Furthermore, can private queries support more expressive operators like JOINs or NOT conditions? What are the limitations on the types of FSS can support practically?

Secure multi-party computation (MPC) allows participants to evaluate a common function without revealing their respective inputs. As hospitals, governments, and corporations increasingly transition from paper records to electronic ones, MPC-style computations represent a natural way to securely enable cross-organization data sharing. MPC is a well-studied cryptographic solution to this problem, but its impracticality has prevented widespread adoption. However, FSS and MPC are closely related, and the creation of FSS has shown promise for more practical protocols. In particular, are there ways to perform MPC practically on more complex computations, such as graph queries?

With the increased number of data and privacy breaches, users are becoming more aware of the "cost" of using web services, i.e. providing these services with their data. Moreover, regulations like GDPR are levying heavy penalties on organizations that do not build secure mechanisms that protect user data. As a result, we will see an increase both in users and web services that want more data protections. In addition, users are willing to trade some performance for privacy and security as long as it does not affect their

experience and workflow. The increased use of DuckDuckGo and Tor support this trend. Therefore, as the need for secure systems grows, it is important to focus on performance and practicality. We hope that the systems in this dissertation serve as a good foundation for thinking about practical, secure mechanisms in various web application contexts.

Bibliography

[1] A. Hidayat. PhantomJS: Full web stack—No browser required, 2017. http://phantomjs.org/.

[2] Victor Agababov, Michael Buettner, Victor Chudnovsky, Mark Cogan, Ben Greenstein, Shane McDaniel, Michael Piatek, Colin Scott, Matt Welsh, and Bolian Yin. Flywheel: Google's data compression proxy for the mobile web. In *Proceedings of the 12th Symposium on Networked Systems Design and Implementation (NSDI)*, volume 15, pages 367–380, Oakland, CA, May 2015.

[3] G. Aggarwal, E. Burzstein, C. Jackson, and D. Boneh. An Analysis of Private Browsing Modes in Modern Browsers. In *Proceedings of the 19th Usenix Security Symposium*, Washington, DC, August 2010.

[4] D. Akhawe, P. Saxena, and D. Song. Privilege Separation in HTML5 Applications. In *Proceedings of the 21st Usenix Security Symposium*, Bellevue, WA, August 2012.

[5] Amazon. https://docs.aws.amazon.com/silk/latest/developerguide/split-arch.html.

[6] Amazon. https://aws.amazon.com/blogs/aws/category/price-reduction/.

[7] Angular.js. Angular: A Superheroic JavaScript MVW Framework. https://angularjs.org/, 2014.

[8] Julian Arz, Dennis Luxen, and Peter Sanders. Transit node routing reconsidered. In *Experimental Algorithms*, pages 55–66, 2013.

[9] Backbone. Backbone.js. http://backbonejs.org/, 2017.

[10] Hannah Bast, Daniel Delling, Andrew Goldberg, Matthias Müller-Hannemann, Thomas Pajor, Peter Sanders, Dorothea Wagner, and Renato F Werneck. Route planning in transportation networks. *arXiv preprint arXiv:1504.05140*, 2015.

[11] Holger Bast, Stefan Funke, and Domagoj Matijevic. Ultrafast shortest-path queries via transit nodes. *The Shortest Path Problem: Ninth DIMACS Implementation Challenge*, 74:175–192, 2009.

[12] Holger Bast, Stefan Funke, Peter Sanders, and Dominik Schultes. Fast routing in road networks with transit nodes. *Science*, 316(5824):566–566, 2007.

[13] Mihir Bellare, Viet Tung Hoang, Sriram Keelveedhi, and Phillip Rogaway. Efficient garbling from a fixed-key blockcipher. In *Proceedings of the 34th IEEE Symposium on Security and Privacy*, pages 478–492, San Francisco, CA, May 2013.

[14] Mihir Bellare, Viet Tung Hoang, and Phillip Rogaway. Foundations of garbled circuits. In *Proceedings of the 19th ACM Conference on Computer and Communications Security (CCS)*, pages 784–796, Raleigh, NC, October 2012.

[15] Assaf Ben-David, Noam Nisan, and Benny Pinkas. FairplayMP: A system for secure multi-party computation. In *Proceedings of the 15th ACM Conference on Computer and Communications Security (CCS)*, pages 257–266, Alexandria, VA, October 2008.

[16] B. Biggio, G. Fumera, I. Pillai, and F. Roli. A Survey and Experimental Evaluation of Image Spam Filtering Techniques. *Pattern Recognition Letters*, 32(10), July 2011.

[17] M. Blaze. A Cryptographic File System for Unix. In *Proceedings of the 1st ACM Conference on Computer and Communications Security (CCS)*, Fairfax, VA, November 1993.

[18] Blue Spire Inc. Aurelia, 2017. http://aurelia.io/.

[19] Elette Boyle, Niv Gilboa, and Yuval Ishai. Function secret sharing. In *Proceedings of the 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT)*, pages 337–367, Sofia, Bulgaria, April 2015.

[20] A. Buell. Linux Framebuffer HOWTO, August 5, 2010. http://www.tldp.org/HOWTO/html_single/Framebuffer-HOWTO/#AEN134.

[21] Chi-Hung Chi, Choon-Keng Chua, and Weihong Song. A novel ownership scheme to maintain web content consistency. In *International Conference on Grid and Pervasive Computing*, pages 352–363. Springer, 2008.

[22] Benny Chor, Niv Gilboa, and Moni Naor. *Private information retrieval by keywords*. Citeseer, 1997.

[23] Benny Chor, Eyal Kushilevitz, Oded Goldreich, and Madhu Sudan. Private information retrieval. *Journal of the ACM (JACM)*, 45(6):965–981, 1998.

[24] J. Chow, B. Pfaff, Tal Garfinkel, and M. Rosenblum. Shredding Your Garbage: Reducing Data Lifetime Through Secure Deallocation. In *Proceedings of the 14th Usenix Security Symposium*, Baltimore, MD, August 2005.

[25] CoffeeScript. CoffeeScript: A Little Language that Compiles to JavaScript, October 26, 2017. http://coffeescript.org/.

[26] D. Crockford. The application/json Media Type for JavaScript Object Notation (JSON). RFC 4627 (Draft Standard), July 2006.

[27] C. Curtsinger, B. Livshits, B. Zorn, and C. Seifert. Zozzle: Fast and Precise In-Browser JavaScript Malware Detection. In *Proceedings of the 20th Usenix Security Symposium*, San Francisco, CA, August 2011.

[28] DIMACS. 9th DIMACS Implementation Challenge - Shortest Paths. http://www.dis.uniroma1.it/challenge9/download.shtml.

[29] R. Dingledine, N. Mathewson, and P. Syverson. Tor: The Second-Generation Onion Router. In *Proceedings of the 13th Usenix Security Symposium*, San Diego, CA, August 2004.

[30] Yevgeniy Dodis, Shai Halevi, Ron Rothblum, and Daniel Wichs. Spooky encryption and its applications. In *Proceedings of the 36th Annual International Cryptology Conference (CRYPTO)*, pages 93–122, Santa Barbara, CA, August 2016.

[31] DuckDuckGo. Take back your privacy! Switch to the search engine that doesn't track you., 2017. https://duckduckgo.com/about.

[32] A. Dunn, M. Lee, S. Jana, S. Kim, M. Silberstein, Y. Xu, V. Shmatikov, and E. Witchel. Eternal Sunshine of the Spotless Machine: Protecting Privacy with Ephemeral Channels. In *Proceedings of the 9th Symposium on Operating Systems Design and Implementation (OSDI)*, Vancouver, Canada, October 2010.

[33] Enigma. Arrival Data for Non-Stop Domestic Flights by Major Air Carriers for 2012. https://app.enigma.io/table/us.gov.dot.rita.trans-stats.on-time-performance.2012.

[34] Ariel J. Feldman, William P. Zeller, Michael J. Freedman, and Edward W. Felten. SPORC: Group collaboration using untrusted cloud resources. In *Proceedings of the 9th Symposium on Operating Systems Design and Implementation (OSDI)*, Vancouver, Canada, October 2010.

[35] E. Felten and M. Schneider. Timing Attacks on Web Privacy. In *Proceedings of the 7th ACM Conference on Computer and Communications Security (CCS)*, Athens, Greece, November 2000.

[36] Peter M. Fenwick. A new data structure for cumulative frequency tables. *Software – Practice and Experience*, 24(3):327–336, March 1994.

[37] T. Flach, N. Dukkipati, A. Terzis, B. Raghavan, N. Cardwell, Y. Cheng, A. Jain, S. Hao, E. Katz-Bassett, and R. Govindan. Reducing Web Latency: The Virtue of Gentle Aggression. In *Proceedings of the 2013 ACM SIGCOMM*, Hong Kong, China, August 2013.

[38] Free Software Foundation. GNU Multi Precision Arithmetic Library. https://gmplib.org/.

[39] Niv Gilboa and Yuval Ishai. Distributed point functions and their applications. In *Proceedings of the 33rd Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT)*, pages 640–658, Copenhagen, Denmark, May 2014.

[40] Shafi Goldwasser. Multi party computations: past and present. In *Proceedings of the 16th Annual ACM Symposium on Principles of Distributed Computing (PDC)*, pages 1–6, 1997.

[41] Shafi Goldwasser, Yael Kalai, Raluca Ada Popa, Vinod Vaikuntanathan, and Nickolai Zeldovich. Reusable garbled circuits and succinct functional encryption. In *Proceedings of the 45th Annual ACM Symposium on Theory of Computing (STOC)*, pages 555–564, Palo Alto, CA, June 2013.

[42] Google. PageSpeed Module Documentation: Sprite Images, 2014. https://developers.google.com/speed/pagespeed/module/filter-image-sprite.

[43] Google. Network Analysis Reference, 2017. https://developers.google.com/web/tools/chrome-devtools/network-performance/reference.

[44] Jens Groth, Aggelos Kiayias, and Helger Lipmaa. Multi-query computationally-private information retrieval with constant communication rate. In *International Workshop on Public Key Cryptography*, pages 107–123. Springer, 2010.

[45] Trinabh Gupta, Natacha Crooks, Srinath TV Setty, Lorenzo Alvisi, and Michael Walfish. Scalable and private media consumption with Popcorn. In *Proceedings of the 13th Symposium on Networked Systems Design and Implementation (NSDI)*, pages 91–107, Santa Clara, CA, March 2016.

[46] K. Harrison and S. Xu. Protecting Cryptographic Keys From Memory Disclosure Attacks. In *Proceedings of DSN*, Edinburgh, UK, June 2007.

[47] M. Heiderich, E. Nava, G. Heyes, and D. Lindsay. *Web Application Obfuscation*. Syngress, 2010.

[48] A. Hidayat. Esprima: ECMAScript Parsing Infrastructure for Multipurpose Analysis, 2017. https://github.com/ariya/esprima.

[49] Daniel Indiviglio. Most Internet Users Willing to Pay for Privacy, December 22 2010. http://www.theatlantic.com/business/archive/2010/12/most-internet-users-willing-to-pay-for-privacy/68443/.

[50] L. Ingram. TreeHouse, December 2012. https://github.com/lawnsea/TreeHouse.

[51] L. Ingram and M. Walfish. TreeHouse: JavaScript Sandboxes to Help Web Developers Help Themselves. In *Proceedings of the 2012 USENIX Annual Technical Conference*, Boston, MA, June 2012.

[52] D. Isacsson. Microsoft Edge's Incognito Mode Isn't So Incognito, February 1, 2016. Digital Trends. https://www.digitaltrends.com/web/microsoft-edge-security-flaws-in-incognito/.

[53] A. Janc and L. Olejnik. Feasibility and Real-World Implications of Web Browser History Detection. In *Proceedings of the Web 2.0 Security and Privacy Workshop*, Oakland, CA, May 2010.

[54] Z. Jiang and J. Huang. Webpage resource protection via obfuscation and auto-expiry. In *Proceedings of ICIW*, Paris, France, July 2014.

[55] Kayak. Kayak. https://www.kayak.com.

[56] KeyCDN. Domain Sharding, August 19, 2016. https://www.keycdn.com/support/domain-sharding/.

[57] Chang Lan, Justine Sherry, Raluca Ada Popa, Sylvia Ratnasamy, and Zhi Liu. Embark: Securely outsourcing middleboxes to the cloud. In *Proceedings of the 13th Symposium on Networked Systems Design and Implementation (NSDI)*, pages 255–273, Santa Clara, CA, March 2016.

[58] S. Lee, Y. Kim, J. Kim, and J. Kim. Stealing Webpages Rendered on Your Browser by Exploiting GPU Vulnerabilities. In *Proceedings of IEEE Symposium on Security and Privacy*, San Jose, CA, May 2014.

[59] B. Lerner, L. Elberty, N. Poole, and S. Krishnamurthi. Verifying Web Browser Extensions' Compliance with Private-Browsing Mode. In *Proceedings of ESORICS*, Egham, United Kingdom, September 2013.

[60] Leonid A Levin. One way functions and pseudorandom generators. *Combinatorica*, 7(4):357–363, 1987.

[61] Jinyuan Li, Maxwell Krohn, David Mazières, and Dennis Shasha. Secure untrusted data repository (SUNDR). In *Proceedings of the 6th Symposium on Operating Systems Design and Implementation (OSDI)*, pages 91–106, San Francisco, CA, December 2004.

[62] D. Litzenberger. PyCrypto: The Python Cryptography Toolkit, June 23, 2014. https://github.com/dlitz/pycrypto.

[63] Jacob R Lorch, Bryan Parno, James Mickens, Mariana Raykova, and Joshua Schiffman. Shroud: Ensuring private access to large-scale data in the data center. In *Proceedings of the 11th USENIX Conference on File and Storage Technologies (FAST)*, pages 199–213, San Jose, CA, February 2013.

[64] D. Lowet and D. Goergen. Co-Browsing Dynamic Web Pages. In *Proceedings of WWW*, Madrid, Spain, April 2009.

[65] Magnet Forensics. How Does Chrome's "Incognito" Mode Affect Digital Forensics? http://www.magnetforensics.com/how-does-chromes-incognito-mode-affect-digital-forensics/, August 6, 2013.

[66] Prince Mahajan, Srinath Setty, Sangmin Lee, Allen Clement, Lorenzo Alvisi, Mike Dahlin, and Michael Walfish. Depot: Cloud storage with minimal trust. In *Proceedings of the 9th Symposium on Operating Systems Design and Implementation (OSDI)*, Vancouver, Canada, October 2010.

[67] Mandiant. Mandiant Redline Users Guide, 2012. https://dl.mandiant.com/EE/library/Redline1.7_UserGuide.pdf.

[68] L. Masinter. The "data" URL scheme. RFC 2397, Network Working Group, August 1998.

[69] Stephen M Matyas, Carl H Meyer, and Jonathan Oseas. Generating strong one-way functions with cryptographic algorithms. *IBM Technical Disclosure Bulletin*, 27(10A):5658–5659, 1985.

[70] Meteor Development Group. Meteor: The Fastest Way to Build JavaScript Apps, 2017. https://www.meteor.com/.

[71] J. Mickens. Silo: Exploiting JavaScript and DOM Storage for Faster Page Loads. In *Proceedings of USENIX WebApps*, Boston, MA, June 2010.

[72] J. Mickens, J. Elson, and J. Howell. Mugshot: Deterministic Capture and Replay for JavaScript Applications. In *Proceedings of the 7th Symposium on Networked Systems Design and Implementation (NSDI)*, San Jose, CA, April 2010.

[73] J. Mickens and M. Finifter. Jigsaw: Efficient, Low-effort Mashup Isolation. In *Proceedings of USENIX WebApps*, Boston, MA, June 2012.

[74] Monkeys. MonkeyTestJS: Automated Functional Testing for Front-end Web Development, 2017. http://monkeytestjs.io/.

[75] Mozilla. Content Security Policy (CSP), November 20, 2017. Mozilla Developer Network. https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP.

[76] Mozilla. Documentation: tabs.captureVisibleTab(), 2017. https://developer.mozilla.org/en-US/Add-ons/WebExtensions/API/tabs/captureVisibleTab.

[77] Arvind Narayanan and Vitaly Shmatikov. Robust de-anonymization of large sparse datasets. In *Proceedings of the 29th IEEE Symposium on Security and Privacy*, pages 111–125, Oakland, CA, May 2008.

[78] Arvind Narayanan and Vitaly Shmatikov. Myths and fallacies of personally identifiable information. *Communications of the ACM*, 53(6):24–26, 2010.

[79] Arvind Narayanan, Narendran Thiagarajan, Mugdha Lakhani, Michael Hamburg, and Dan Boneh. Location privacy via private proximity testing. In *Proceedings of the 18th Annual Network and Distributed System Security Symposium*, San Diego, CA, February 2011.

[80] Ravi Netravali, Ameesh Goyal, James Mickens, and Hari Balakrishnan. Polaris: Faster page loads using fine-grained dependency tracking. In *Proceedings of the 13th Symposium on Networked Systems Design and Implementation (NSDI)*, Santa Clara, CA, March 2016.

[81] Ravi Netravali and James Mickens. Remote-control caching: Proxy-based url rewriting to decrease mobile browsing bandwidth. In *Proceedings of the 19th International Workshop on Mobile Computing Systems & Applications*, pages 63–68. ACM, 2018.

[82] M. Nielsen. Clickmonkey, 2017. https://www.npmjs.com/package/clickmonkey.

[83] D. Ohana and N. Shashidhar. Do Private and Portable Web Browsers Leave Incriminating Evidence? In *Proceedings of the International Workshop on Cyber Crime*, San Francisco, CA, May 2013.

[84] Femi Olumofin and Ian Goldberg. Privacy-preserving queries over relational databases. In *Proceedings of the 10th Privacy Enhancing Technologies Symposium*, pages 75–92, Berlin, Germany, July 2010.

[85] Femi Olumofin and Ian Goldberg. Revisiting the computational practicality of private information retrieval. In *Financial Cryptography and Data Security*, pages 158–172, 2011.

[86] K. Onarlioglu, C. Mulliner, W. Robertson, and E. Kirda. PrivExec: Private Execution as an Operating System Service. In *Proceedings of the 34th IEEE Symposium on Security and Privacy*, San Francisco, CA, May 2013.

[87] OpenCV. Open Source Computer Vision Library, 2017. https://opencv.org/.

[88] OpenMP. OpenMP. http://www.openmp.org/.

[89] OpenSSL. OpenSSL. https://openssl.org.

[90] O'Reilley. Optimizing for Mobile Networks. https://hpbn.co/optimizing-for-mobile-networks/.

[91] E. Orion. Tor popularity leaps after snooping revelations, August 30, 2013. The Inquirer. http://www.theinquirer.net/inquirer/news/2291758/tor-popularity-leaps-after-snooping-revelations.

[92] A. Osmani. Tab Discarding in Chrome: A Memory-Saving Experiment, September 2015. Google Developer Blog. https://developers.google.com/web/updates/2015/09/tab-discarding.

[93] Rafail Ostrovsky and William E Skeith III. A survey of single-database private information retrieval: Techniques and applications. In *Public Key Cryptography (PKC)*, pages 393–411, 2007.

[94] D. Parys. How to Safeguard Your Site with HTML5 Sandbox. Microsoft Developer Network. http://msdn.microsoft.com/en-us/hh563496.aspx, 2015.

[95] S. Pongelli. Jigsaw: An Infrastructure for Cross-device Mashups. Master's thesis, ETH Zurich, November 6, 2013.

[96] Raluca Ada Popa, Catherine M. S. Redfield, Nickolai Zeldovich, and Hari Balakrishnan. CryptDB: Protecting confidentiality with encrypted query processing. In *Proceedings of the 23rd ACM Symposium on Operating Systems Principles (SOSP)*, pages 85–100, Cascais, Portugal, October 2011.

[97] Raluca Ada Popa, Emily Stark, Jonas Helfer, Steven Valdez, Nickolai Zeldovich, M. Frans Kaashoek, and Hari Balakrishnan. Building web applications on top of encrypted data using Mylar. In *Proceedings of the 11th Symposium on Networked Systems Design and Implementation (NSDI)*, pages 157–172, Seattle, WA, April 2014.

[98] Priv.io. Priv.io homepage, 2015. https://priv.io/.

[99] Priv.ly. Change the Way Your Browser Works: Share Priv(ate).ly, 2017. https://priv.ly/.

[100] Progress Software. Kendo UI for jQuery. https://docs.telerik.com/kendo-ui/, 2017.

[101] N. Provos. Encrypting Virtual Memory. In *Proceedings of the 9th Usenix Security Symposium*, Denver, CO, August 2000.

[102] Ramprasad Ravichandran, Michael Benisch, Patrick Gage Kelley, and Norman M Sadeh. Capturing social networking privacy preferences. In *Proceedings of the 9th Privacy Enhancing Technologies Symposium*, pages 1–18, Seattle, WA, August 2009.

[103] Joel Reardon, Jeffrey Pound, and Ian Goldberg. Relational-complete private information retrieval. *University of Waterloo, Tech. Rep. CACR*, 34:2007, 2007.

[104] L. Richardson. Beautiful Soup: A Python Parser for HTML, 2017. http://www.crummy.com/software/BeautifulSoup/.

[105] Patrick F Riley. The Tolls of Privacy: An underestimated roadblock for electronic toll collection usage. *Computer Law & Security Review*, 24(6):521–528, 2008.

[106] Rebecca J. Rosen. Study: Consumers Will Pay $5 for an App that Respects their Privacy, December 26 2013. http://www.theatlantic.com/technology/archive/2013/12/study-consumers-will-pay-5-for-an-app-that-respects-their-privacy/282663/.

[107] Jeffrey Rott. Intel advanced encryption standard instructions (AES-NI). Technical report, Technical report, Intel, 2010.

[108] Rowstron, Antony and Druschel, Peter. Pastry: Scalable, decentralized object location, and routing for large-scale peer-to-peer systems. In *IFIP/ACM International Conference on Distributed Systems Platforms and Open Distributed Processing*, pages 329–350. Springer, 2001.

[109] J. Ruderman. Same-origin Policy. Mozilla Developer Network. https://developer.mozilla.org/en-US/docs/Web/Security/Same-origin_policy, August 1, 2014.

[110] Sahi. Sahi Pro: The Tester's Automation Tool, 2017. http://sahipro.com/.

[111] SeleniumHQ. Selenium: Browser Automation, 2017. http://www.seleniumhq.org/.

[112] Justine Sherry, Chang Lan, Raluca Ada Popa, and Sylvia Ratnasamy. Blindbox: Deep packet inspection over encrypted traffic. In *Proceedings of the 2015 ACM SIGCOMM*, pages 213–226, London, United Kingdom, August 2015.

[113] Ashiwan Sivakumar, Shankaranarayanan Puzhavakath Narayanan, Vijay Gopalakrishnan, Seungjoon Lee, Sanjay Rao, and Subhabrata Sen. PARCEL: Proxy assisted browsing in cellular networks for energy and latency reduction. In *Proceedings of the 10th ACM International on Conference on emerging Networking Experiments and Technologies*, pages 325–336. ACM, 2014.

[114] Emil Stefanov, Marten van Dijk, Elaine Shi, Christopher Fletcher, Ling Ren, Xiangyao Yu, and Srinivas Devadas. Path ORAM: An extremely simple oblivious RAM protocol. In *Proceedings of the 20th ACM Conference on Computer and Communications Security (CCS)*, Berlin, Germany, November 2013.

[115] Stoica, Ion and Morris, Robert and Karger, David and Kaashoek, M Frans and Balakrishnan, Hari. Chord: A scalable peer-to-peer lookup service for internet applications. *ACM SIGCOMM Computer Communication Review*, 31(4):149–160, 2001.

[116] Q. Sun, D. Simon, Y.M. Wang, W. Russell, V. Padmanabhan, and L. Qiu. Statistical Identification of Encrypted Web Browsing Traffic. In *Proceedings of the 23rd IEEE Symposium on Security and Privacy*, Oakland, CA, May 2002.

[117] Y. Suzuki. Escodegen: ECMAScript Code Generator, 2017. https://github.com/Constellation/escodegen.

[118] P. Szor. Advanced Code Evolution Techniques and Computer Virus Generator Kits. InformIT. http://www.informit.com/articles/article.aspx?p=366890&seqNum=6, March 25, 2006.

[119] Yang Tang, Phillip Ames, Sravan Bhamidipati, Ashish Bijlani, Roxana Geambasu, and Nikhil Sarda. CleanOS: Limiting Mobile Data Exposure with Idle Eviction. In *Proceedings of the 10th Symposium on Operating Systems Design and Implementation (OSDI)*, Hollywood, CA, October 2012.

[120] Renu Tewari, Thirumale Niranjan, and Srikanth Ramamurthy. WCDP: A protocol for web cache consistency. In *Proceedings of the 7th Web Caching Workshop*. Citeseer, 2002.

[121] The Apache Foundation. Apache Benchmark. https://httpd.apache.org/docs/2.4/programs/ab.html.

[122] Tilde Inc. Ember: A Framework for Creating Ambitious Web Applications. https://emberjs.com/, 2017.

[123] Tor Project. Tor Metrics: Performance. https://metrics.torproject.org/torperf.html, November 28, 2017.

[124] W3C Web Apps Working Group. Web Storage: W3C Working Draft. http://www.w3.org/TR/webstorage/, April 19, 2016.

[125] W3C Web Apps Working Group. Web Cryptography: W3C Working Draft, January 26, 2017. http://www.w3.org/TR/WebCryptoAPI/.

[126] Z. Weinberg, E. Chen, P. Jayaraman, and C. Jackson. I Still Know What You Visited Last Summer. In *Proceedings of the 32nd IEEE Symposium on Security and Privacy*, Oakland, CA, May 2011.

[127] W. Wong and M. Stamp. Hunting for metamorphic engines. *Journal in Computer Virology and Hacking*, 2(3), December 2006.

[128] C. Wright, S. Coull, and F. Monrose. Traffic Morphing: An Efficient Defense against Statistical Traffic Analysis. In *Proceedings of the 16th Annual Network and Distributed System Security Symposium*, San Diego, CA, February 2007.

[129] David J Wu, Joe Zimmerman, Jérémy Planul, and John C Mitchell. Privacy-preserving shortest path computation. In *Proceedings of the 2016 Annual Network and Distributed System Security Symposium*, San Diego, CA, February 2016.

[130] M. Xu, Y.Jang, X. Xing, T. Kim, and W. Lee. UCognito: Private Browsing without Tears. In *Proceedings of the 22nd ACM Conference on Computer and Communications Security (CCS)*, Denver, CO, October 2015.

[131] Yelp. Yelp Academic Dataset. https://www.yelp.com/dataset_challenge/dataset.

[132] New Yorker. The New Yorker SecureDrop, 2017. https://projects.newyorker.com/securedrop/.

[133] E. Zadok, I. Badulescu, and A. Shender. Cryptfs: A Stackable Vnode Level Encryption File System. Technical Report CUCS-021-98, University of California at Los Angeles, 1998.