Reverb: Speculative Debugging for Web Applications

Paper #104 (Research Paper)

Abstract

Bugs are common in web pages. Unfortunately, traditional debugging primitives like breakpoints are crude tools for understanding the asynchronous, wide-area data flows that bind client-side JavaScript code and server-side application logic. In this paper, we describe Reverb, a powerful new debugger that makes data flows explicit and queryable. Reverb provides three novel features. First, Reverb tracks *precise value provenance*, allowing a developer to quickly identify the reads and writes to JavaScript state that affected a particular variable's value. Second, Reverb enables *speculative bug fix analysis*. A developer can replay a program to a certain point, change code or data in the program, and then resume the replay; Reverb uses the remaining log of nondeterministic events to influence the post-edit replay, allowing the developer to investigate whether the hypothesized bug fix would have helped the original execution run. Third, Reverb supports *wide-area debugging* for applications whose server-side components use event-driven architectures. By tracking the data flows between clients and servers, Reverb enables speculative replaying of the *distributed* application.

1 Introduction

Debugging the client-side of a web application is hard. The DOM interface [42], which specifies how JavaScript code interacts with the rest of the browser, is sprawling and constantly accumulating new features [30, 37]. Furthermore, the DOM interface is pervasively asynchronous and event-driven, making it challenging for developers to track causality across event handlers [29, 38, 51, 73]. As a result, JavaScript bugs are endemic, even on popular sites that are maintained by professional developers [59, 61].

Commodity browsers include JavaScript debuggers that support breakpoints and watchpoints. However, fixing bugs is still hard. Breakpoints and watchpoints let developers inspect program state at a moment in time; however, in an event-driven program with extensive network and GUI interactions, bug diagnosis often requires complex temporal reasoning to reconstruct a buggy value's *provenance* across multiple asynchronous code paths. This provenance data is not exposed by more advanced tools for replay debugging or program slicing (§2).

In this paper, we introduce Reverb, a new debugger for web applications. Reverb has three features which enable a fundamentally more powerful debugging experience. First, Reverb tracks *precise value provenance*, i.e., the exact set of reads and writes (and the associated source code lines) that produce each program value. Like a traditional replay debugger [16, 38, 64], Reverb records all of the nondeterministic events from a program's execution, allowing Reverb to replay a buggy execution with perfect fidelity. Unlike a traditional replay debugger, Reverb also records the *deterministic* values that are manipulated by reads and writes of page state. Using this extra information at replay time, Reverb enables developers to query fine-grained data flow logs and quickly answer questions like "Did variable `x` influence variable `y`?" or "Was variable `z`'s value affected by a control flow that traversed function `f()`?" Reverb's logging of both nondeterministic and deterministic events is fast enough to run in production: for the median web page in our 300 page test corpus, Reverb increases page load time by only 5.5%, while producing logs that are only 45.4 KB in size.

Reverb's second unique feature is support for *speculative bug fix analysis.* At replay time, Reverb allows a developer to pause the application being debugged, edit the code or data of the application, and then resume the replay. Post-edit, Reverb replays the remaining nondeterministic events in the log, using carefully-defined semantics (§3.3) to determine how those events should be replayed in the context of the edited program execution. Once the altered execution has finished replaying, Reverb identifies the control flows and data flows which differ in the edited and original executions. These analyses help developers to determine whether a hypothesized bug fix would have helped the original program execution. Speculative edit-and-replay is unsound, in the sense that a post-edit program can misbehave in arbitrary ways, e.g., by attempting to read an undefined variable. However, even without Reverb, *the process of testing bug fixes is unsound.* A developer typically lacks a priori knowledge about whether a hypothesized fix will work. The developer implements the hypothesized fix, and then runs tests and tries to determine whether the fix actually worked; even if all of the tests pass, there is no guarantee that the fix is completely correct, since the tests may miss corner cases. However, Reverb provides the developer with an important new weapon: the ability to compare the data flows and the control flows in the original execution and the ostensibly bug-free execution. As we demonstrate through case studies (§5.3), the ability to diff program executions is a powerful debugging tool.

Reverb's third novel feature is to support *wide-area debugging* for applications whose server-side components use single-threaded, event-driven architectures like Node [58], Redis [62], or NGINX [55]. For these components, the event loop interface provides a narrow, semantically-well-defined abstraction layer at which to log and replay the components. Thus, Reverb can use vector clocks and a small assortment of additional tricks (§3.4) to track wide-area causality. Reverb provides two levels of support for server-side components:

- Node components execute JavaScript code. Thus, Reverb can apply its client-side framework to the server-side, and track variable-level data flows and control flows between multiple browsers and multiple server-side Node instances.

- Reverb treats an event-driven (but non-JavaScript) component like Redis as a black box. Reverb logs and replays the component at the level of the component's externally-visible event interface, tracking data flows emanating from, and terminating at, server-side events.

Reverb supports speculative bug fix analysis for data stores and JavaScript state on either side of the wide area. For example, a developer can edit the value that server-side code receives from a Redis database, and then explore how the edited value impacts the remainder of the replaying application's execution.

In summary, our contribution is the first distributed replay debugger that provides fine-grained data flow tracking and speculative bug fix analysis. Supporting this entire set of debugging capabilities was previously intractable, because prior debuggers operated at the wrong semantic level; Reverb's insight is that web services using managed runtimes and event-driven cross-server RPCs *should be analyzed at these levels of abstraction*, instead of at the level of system calls or hardware-level instruction traces. However, to fully leverage this new insight, we must provide new debugging infrastructure that prior work lacks. In particular, we introduce a new logic for reasoning about post-edit replays; this logic describes how editing an application component mid-replay should affect the post-edit replay of that component (§3.3) and remote ones which may see altered output from the mutated component (§3.4). We also introduce new diagnostic techniques for helping developers understand how edited replays diverge from a program's original executions. These techniques, which explain divergences using diffs of data flow graphs and control flow graphs (§3.2), allow Reverb to diagnose complex bugs in real web applications (§5.3). A user study confirms that Reverb is more helpful than traditional in-browser debuggers (§5.6).

2 Background

Having used the debuggers in commodity browsers [21, 24, 41], and having built several state-of-the-art debuggers ourselves [5, 6, 7], we often found ourselves wanting fine-grained data flow tracking and speculative bug fix analysis. In this section, we explain why prior debugging techniques are insufficient to realize the vision of Figure 1.

2.1 Traditional debuggers

Standard debuggers focus on the abstraction of breakpoints [21, 24, 41]. Debuggers like Visual Studio [39] and Eclipse [17] also allow developers to edit some types of program values at a breakpoint, and then resume the program's live execution. Breakpoints are undoubtedly useful, but they force a human developer to guess which source code locations are buggy.

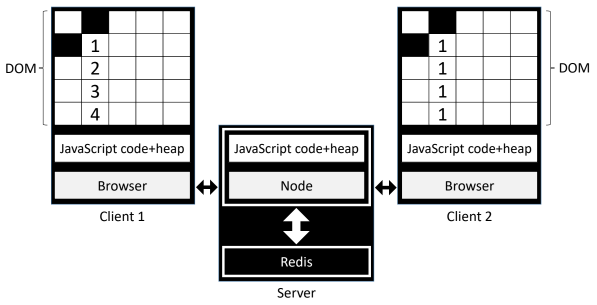


Figure 1: EtherCalc [65] is a web-based, collaborative spreadsheet. Multiple users can simultaneously issue edits to the same spreadsheet, with a Node server broadcasting edits to all users, and storing the spreadsheet data in Redis. Bug #314 in EtherCalc's issue tracker involves a GUI-based edit from client 1 that is not reflected to client 2's DOM. Ideally, a debugging framework could efficiently answer two questions. First, how is the relevant DOM state and JavaScript heap state from client 1 being transmitted through the server-side components to the DOM and JavaScript heap of client 2? Second, given recorded state from a buggy execution run, as well as a hypothesized bug fix that modifies code and/or data on clients or servers, would the hypothesized fix remove the problematic behavior in the recorded execution?

Some debuggers support watchpoints, which pause an application when a specific memory location is read or written. Watchpoints eliminate the need for a developer to guess when and where a particular buggy assignment will occur. However, watchpoints do not capture temporal data flows throughout a program. So, developers still have to manually reconstruct reverse temporal flows to determine how the value in a buggy write was generated. Our case studies (§5.3) demonstrate that automated construction of value provenance eliminates human-driven guess work about how program state is created.

2.2 Deterministic replay

Traditional debuggers pause and inspect the state of live programs. In contrast, replay debuggers [4, 16, 18, 22, 23, 32, 34, 38, 64] first *log* the nondeterministic events in a live execution run, and then *replay* the program in a controlled environment, using the log to carefully recreate the original order and content of nondeterministic events. Replaying the nondeterministic events is sufficient to induce the remaining, deterministic program behavior, so there is no need to log the values that are manipulated by deterministic reads and writes.

The ability to reliably recreate a buggy execution makes it easier to test fault hypotheses. Replay debugging is particularly useful for studying heisenbugs that rarely occur and involve specific event orderings. Some replay debuggers support backwards-stepping [18, 22, 34, 64], such that a developer can set a breakpoint or a watchpoint, and then move execution forwards or backwards in time.

However, even backwards-stepping debuggers force human developers to manually track value provenance. Thus, root cause analysis is still difficult.

2.3 Program slicing

A program slice is a subset of program statements that may have influenced the values that are accessed by a specific line of source code [68]. The tuple `<sourceCodeLine,variablesOfInterest>` is called the slicing criterion. Given a slicing criterion, a static slice is derived purely from analysis of source code [13, 15, 19, 27, 57]; in contrast, a dynamic slice assumes a set of concrete values (e.g., at the slicing criterion) to narrow the set of potentially relevant program statements [1, 2, 26, 33, 68].

Slicing algorithms lack a complete, concrete log of the reads and writes made during a real execution; thus, slicing algorithms are often imprecise, particularly for complex programs. Imprecision hurts the use of slices for bug diagnosis, since developers must consider source code lines that may not be causally related to the bug. Imprecision compounds itself if slices are used to reconstruct wide-area execution behavior. In contrast, Reverb provides *guaranteed-precise, provenance-annotated execution traces* (§3.2). Similar to an instruction trace, a Reverb trace provides a temporal log of the source code statements that a program executed; however, the traces also describe the *values* that the executed statements manipulated, and the *provenance* of those values. For additional discussion of program slicing, the interested reader can peruse Section A.4 in the technical report [8].

2.4 Data Provenance

Provenance-aware file systems [50, 63] allow users to determine which input files were read by a process during the production of output files. Reverb deals with the provenance of application state at the granularity of *individual program variables* that reside on clients and servers. Thus, Reverb tracks how storage data spreads throughout an application, but does so at the level of fine-grained, variable-level flows.

Provenance-aware network platforms let operators discover the route that a packet took [75], or the reason why network switches have certain NDlog rules [71, 72, 74]. Reverb is agnostic about network-level configuration state, but is compatible with systems that track it.

2.5 Speculative edit-and-continue

Dora [69] is a single-machine replay debugger that records the OS-level interactions that belong to a group of processes. Dora allows for limited types of edits to occur during replay. If an edit causes a replay to diverge, Dora explores multiple execution paths that are rooted at this initial divergence. Dora executes each post-divergence path on a live machine, recording the subsequent (and nondeterministic) OS-level interactions. Like Reverb, Dora defines policies for handling new calls to timekeeping functions or socket interfaces. After Dora has explored several potential futures of the divergent replay, Dora identifies the most plausible divergent execution using a metric akin to string edit distance, comparing the system calls of each explored path to those of the original execution.

Dora's speculative power is highly restricted by two factors. First, Dora's vantage point is at the OS layer. In contrast, Reverb's vantage point is within the managed runtime of a JavaScript engine, or at the event loop interface of a single-threaded program like Redis. This difference is fundamental, and represents a key insight of Reverb: *by introspecting on program execution at a higher level of abstraction, Reverb can handle a wider variety of speculative edits*, because the side effects of an edit can be reasoned about with respect to a constrained set of events, instead of the much wider and messier POSIX interface. For example, Dora cannot handle edits which modify thread scheduling, e.g., to cause fewer threads to run, because Dora cannot enumerate and model the ensuing avalanche of side effects upon low-level POSIX state like pthread locks and shared memory pages. In contrast, Reverb can handle a schedule-altering edit that changes the number of client-side frames (the JavaScript equivalent of processes). Reverb can tractably reason about such changes because frames cannot share raw memory, are internally single-threaded, and only communicate via pass-by-value `postMessage` events. Thus, the only way that a newly created frame can impact another frame is via the generation of new `postMessage` events.

Dora's second restriction is that it does not track individual reads and writes to raw memory, because doing so would be too expensive [52]. Thus, Dora cannot provide variable-level value provenance; another consequence is that Dora may incorrectly replay post-edit memory accesses if the edit changes which memory page contains an object. In contrast, Reverb introspects at the JavaScript level, allowing Reverb to efficiently track all reads and writes to *application-visible* state. This difference is fundamental. Logging all reads and writes enables wide-area causality tracking, and is critical for explaining divergences between a logged program run and a speculatively-edited replay (§3.3).

3 Design

Figure 2 provides an overview of Reverb's design. A web application has multiple clients and servers. Clients are assumed to be standard web browsers which execute JavaScript. Both server-side and client-side components are assumed to be single-threaded and event-driven. Each component records its nondeterministic events; if a component uses a JavaScript engine, then the component also records its deterministic reads and writes to JavaScript state and the DOM (§3.2). Distributed causality between hosts, e.g., via HTTP requests, is tracked using vector clocks (§3.4). At debug time, Reverb uses the global event log to replay each client or server in isolation, or together as a single logical application (§3.3 and§3.4).

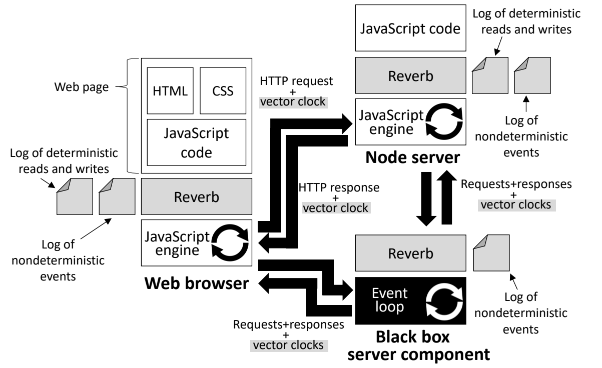

JavaScript code
Log of deterministic reads and writes
Web page
HTML
CSS
JavaScript code
HTTP request + vector clock
Reverb
JavaScript engine
Log of nondeterministic events
Node server
Log of deterministic reads and writes
Reverb
HTTP response + vector clock
Requests+responses + vector clocks
Log of nondeterministic events
JavaScript engine
Reverb
Web browser
Event loop
Log of nondeterministic events
Requests+responses + vector clocks
Black box server component

Figure 2: An overview of Reverb's architecture. Grey components are added by Reverb.

3.1 Overview of the JavaScript Execution Model

Execution environment: JavaScript exposes a single threaded, event-driven programming interface. A JavaScript file defines initialization code that runs once, at the time that the file is parsed by the JavaScript engine. The initialization code registers event handlers that the JavaScript engine will fire in response to GUI interactions, timer expirations, network activity, and so on. Once a browser has evaluated all of the JavaScript files in a page's HTML, the subsequent execution of the page is driven solely by the reception of asynchronous events.

An event handler often calls other functions. Thus, firing a handler can initiate a call chain that is rooted by the handler. A program can register multiple handlers for a single event type. Thus, the call chain for an event is the union of the call chains for the associated event handlers. In the rest of this paper, the unadorned term "call chain" refers to the aggregate call chain for a particular event.

Sources of Nondeterminism: In a JavaScript program, the primary source of nondeterminism is the order in which events arrive (and the content of those events) [38]. JavaScript code may also invoke a small number of nondeterministic functions. For example, `Math.random()` returns a random number. `Date()` returns the current time with millisecond granularity.

By default, a JavaScript program consists of a single event loop. However, a web page can incorporate multiple frames [44] or web workers [28]; each one represents a new event loop that runs in parallel with the others [40]. Concurrent execution contexts can only interact with each other via the asynchronous, pass-by-value `postMessage()` interface [46]. The browser delivers those messages by firing an event in the recipient's execution context. Thus, from the perspective of the recipient, handling message nondeterminism is no different than handling other event-driven nondeterminism like GUI interactions.

Externalizing Output: A JavaScript program can externalize three types of output:

- The DOM interface [42] lets a program update the visual content that users see. The DOM interface defines methods for dynamically manipulating a page's HTML structure, e.g., by adding new HTML tags, or by changing the CSS styles of preexisting tags.
- A JavaScript program can also write to local storage. Cookies [43] can store up to 4 KB of data, whereas IndexedDB [45] and the `localStorage` interface [47] can hold MBs of information.
- To send network data, a program uses the `XML-HttpRequest` [49] and `WebSocket` [48] interfaces. `XMLHttpRequest` is an older interface which only supports request/response interactions. `WebSocket` supports full-duplex streams.

In this paper, we ignore multimedia objects like `<video>` streams, since we focus on the debugging of pure HTML, CSS, and JavaScript state.

3.2 Analyzing Value Provenance

To track data flows, Reverb first logs nondeterministic and deterministic events. After reconstructing data flows, Reverb uses them to support flow queries, and express state divergences caused by speculative edit-and-continue.

Logging Nondeterminism: Prior work has explored various ways to deterministically replay client-side JavaScript code [11, 38]. Our Reverb prototype rewrites JavaScript source code to interpose on nondeterministic sources (§4), but Reverb's design makes no deep assumptions about how nondeterminism is logged or replayed.

A Reverb log has an entry for each nondeterministic event; each log entry contains event-specific data that is sufficient for recreating that event. For example, the log entry for a timer firing contains a reference to the timer callback. The log entry for a call to `Math.random()` contains the return value of the function. The log entry for a mouse click stores which mouse button was clicked, the x and y coordinates for the click, and so on.

At the beginning of logging, Reverb takes a snapshot of the client's local storage (e.g., cookies). Reverb also registers its own handlers for GUI events like mouse clicks. So, if the logged application only installs handlers for (say) `keypress`, but not `keydown` or `keyup`, Reverb will still log when the latter two kinds of events occur. This information is useful for handling speculative edits which add new GUI handlers (§3.3).

Logging Deterministic Reads and Writes: In JavaScript, each object is essentially a mutable dictionary, with string keys (i.e., property names) mapping to property values. The global namespace is reified via the special `window` object, such that references to a global variable `x` are implicitly translated to `window.x`. Abstractly speaking, Reverb logs reads and writes to the JavaScript heap by shimming the getters and setters for each object dictionary (including the one that belongs to `window`). Our Reverb prototype uses JavaScript rewriting to inject this shim code (§4).

Reconstructing Data Flows: Using the log of deterministic reads and writes, Reverb can reconstruct the provenance of all JavaScript variable values at any moment in a program's execution. Given a slicing criterion which mentions variable `x` at time `t`, Reverb finds the prior write for which `x` was the left-hand side. For the variables on the right-hand side, Reverb finds the prior write which assigned to *those* variables. Reverb continues this recursive process until reaching the beginning of the program; the traced path represents the provenance for the slicing criterion. Note that the path may be a tree, not a line, because a single assignment may involve multiple right-hand sides (e.g., `x=y+z`). The path may also cross the event handlers that belong to multiple high-level events like key presses or the arrival of network data.

Reverb's log associates each deterministic read or write with a source code line. Thus, Reverb can also generate source-code-level execution traces which provide a serial history of each source code line that a program ran. The core visualization tool that Reverb provides to developers is an execution trace that is overlaid with provenance information: each variable mentioned in each source code line is associated with the prior source code line which generated the variable's value. Figure 7 depicts an example of such a trace, and the extended technical report [8] (§A.3) describes some of the pruning techniques which improve the comprehensibility of traces. For now, we merely explain a developer-guided pruning approach that is simple, and important in practice: targeted dynamic tracing. A targeted dynamic trace lets a developer drill down on the executed source code lines (and associated data flows) that affected a specific variable. As the developer explores the initial trace, the developer can add or remove target variables, expanding or shrinking the targeted trace. Our case studies (§5.3) show that targeted dynamic traces are fast to generate, and provide helpful diagnostic information.

Reverb uses Scout-style dependency analysis [53] to track data flows between the JavaScript heap and the DOM. For example, the DOM tree is a data structure which mirrors a page's dynamic HTML tree; each HTML tag has an associated DOM node that is exposed to JavaScript code. Reverb understands the semantics of DOM methods like `Node.appendChild(newChild)`. Thus, Reverb can track how JavaScript values flow to DOM nodes, and how DOM values are assigned to JavaScript variables.

Reverb's logs capture a variety of additional behavior. For example, Reverb explicitly tracks aliasing relationships, as shown in Figure 3. Also, for each executed branch, Reverb records the associated source code line, and the values consumed by the branch test. This information allows Reverb to apply classical algorithms for building dynamic control flow dependencies [33]. Reverb easily handles the special case of execution flows that span `try/catch` blocks, since Reverb records both the exception-throwing line, and the catching line.

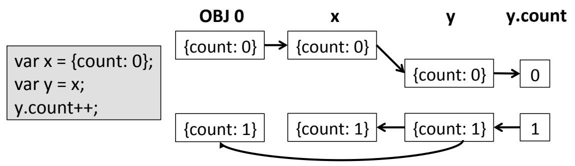


Figure 3: To capture aliasing relationships, Reverb distinguishes between an underlying object and its multiple names. Writes to an aliased object create horizontal arrows in data flow diagrams, since time flows downward and the aliases are updated simultaneously.

3.3 Speculative Edit-and-Continue Debugging

Speculative edit-and-continue debugging has five phases:

- logging the events in a baseline execution run;
- replaying the execution up to a specified point;
- changing the program's state in some way;
- resuming execution, with nondeterminism from the original run "influencing" the post-edit execution; and
- comparing the behavior of the original and altered runs to understand the effects of the speculative fix.

The nondeterministic input vectors for a JavaScript program are well-known and (compared to POSIX) very small in number [38]. However, defining post-edit replay semantics was previously an unsolved problem. Below, we define those semantics, describing how to execute post-edit code under the guidance of a log whose nondeterministic values may not cleanly apply to the post-edit execution. These post-edit replay semantics are an important contribution of the paper.

Inside the call chain that contains the edit: Once we have replayed execution to the edit point and modified the necessary state, we resume the call chain's execution. Post-edit, the chain may explore different branches than were visited in the original run. Thus, the chain may issue fewer or additional calls to nondeterministic functions like `Date()`.

- If the post-edit code makes *fewer* calls to a nondeterministic function f, we simply extract return values for f from the log, replaying the same nondeterminism that the original run experienced. Once the call chain finishes, and we must replay the next event's call chain, we replay f's values from the log, starting with the value that was first seen by the *original* execution of the call chain for the new event. For example, suppose that, during the original program execution, two events fired; the first call chain consumed random numbers $r_0 ... r_4$, and the second chain consumed $r_5 ... r_9$. Suppose that the first call chain is edited, such that it only makes two calls to `Math.random()`. When the second call chain executes in the post-edit run, `Math.random()` will return r_5, then r_6, and so on, since these are the random numbers that the second call chain saw during its original run.
- If the post-edit code generates *more* calls to a nondeterministic function than seen at logging time, we use

a function-specific extrapolation technique to generate additional values once the call chain has exhausted the values that are associated with it in the log. For `Math.random()`, we simply generate new random numbers. For time-related functions like `Date()`, we return monotonically increasing time values that are smaller than the next logged time value. Once the call chain finishes and we trigger the call chain for a new event, we return to using the log to provide values for nondeterministic functions.

Post-edit code may also generate new externalized output. For example, an edited value may be written to local storage, or sent over the network via the query string of an `XMLHttpRequest`. Post-edit code may also modify event handler state in ways that cause fewer or additional events to fire in the future. For example, post-edit code may register timers that were never created in the original run; post-edit code may also *deregister* timers that fired in the original run. Post-edit code may also generate entirely new network requests, or register/deregister handlers for GUI events. Below, we discuss how to incorporate these changes into the post-edit universe.

After the call chain which contains the edit has finished execution: At this point, the replay framework has completed execution of the call chain. The framework can now manipulate program state before releasing the next event and invoking the appropriate event handlers.

Due to the edit, the current execution context may have different event handlers than what the program had at the equivalent moment in the original execution. The replay framework must integrate any changes into the log of nondeterminism; some post-edit events in the log must be marked as "do not replay," and some new events must be added to the log:

- If the edit resulted in the deletion of a timer, we mark all of the timer's subsequent events as "do not replay." If the edit created a new timer, we inject new timer events into the log, using the logged wall-clock time of preexisting events to determine where the new timer events should go, relative to the preexisting events.
- If the edit deleted a DOM handler, and the edited program has no remaining handlers for a particular event type, we mark all post-edit instances of that event as "do not replay." For example, if the deletion of a `keypress` handler leaves the program with no `keypress` handlers at all, we suppress future dispatches of logged `keypresses` (because such events cannot trigger any call chains). If an edit registers a *new* DOM handler, then no special action is required—when the replay framework dispatches a relevant event, the framework will invoke the new handler as usual. Remember that Reverb records all GUI events at logging time, even if the application has not registered its own handlers for those events (§3.2). Thus, at replay time, Reverb can invoke new handlers for a particular event at the appropriate moment.
- If an edit closes `XMLHttpRequests` or `WebSockets`, the replay framework cancels future events that involve those network connections. If the edit creates a new, unlogged network request, then the replay framework must inject new network events into the log. If the server-side responder is also being replayed, then Reverb inserts a new request into the server-side log; the request represents a speculative server-side edit. When the response is generated, Reverb buffers it, and uses a model of network latency to determine where to inject the response into the client-side log (§3.4). If Reverb does not control the server-side responder, Reverb can terminate replay; alternatively, Reverb can issue the request to the live (but uncontrolled) responder, and then insert the response into a downstream position in the client log, using the observed network latency of the live fetch to determine where to place the response.
- The post-edit code may issue new reads or writes to local storage. The replay framework does nothing special to handle synchronous accesses to cookies or DOM storage—the framework simply passes those IOs to the underlying storage. For asynchronous accesses to `IndexedDB`, the replay framework must inject new IO events into the log, using a model for the expected latency of those events. Generating these events is logically similar to generating new network events, as explained in the previous bullet.

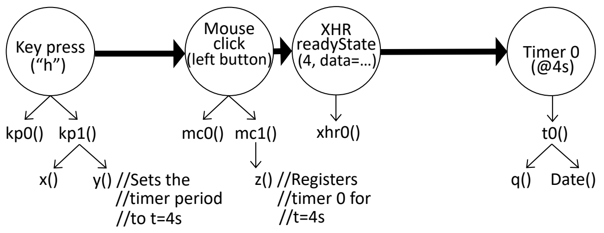
Note that the replay framework never injects new GUI events into the post-edit universe. For example, the framework will never inject new mouse clicks or key presses. Nothing prevents the framework from doing so, but, lacking a reasonable model for how user intent would change in the post-edit world, the framework is content to merely replay the GUI events from the original program run.

Once the replay framework has patched the log, the framework extracts the next high-level event from the log, and initiates the relevant call chain. The event may or may not have been seen in the original program run.

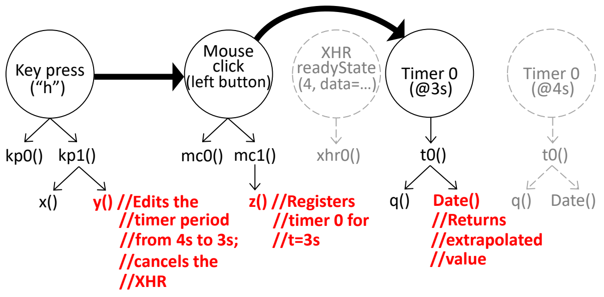
Inside the call chain for a new event which did not occur during the original execution: Replay uses extrapolation to generate return values for nondeterministic functions like `Math.random()`. When the call chain ends, we add and remove top-level events as described above.

Inside the call chain for an event which *did* occur in the original execution: We use the log to replay return values for nondeterministic functions; if the call chain's nondeterministic values are exhausted before the call chain finishes, we use extrapolation to generate additional values. When the call chain finishes, we add and remove events from the log as described above.

Figure 4 shows an end-to-end example of replaying events after an edit has been made. Once an altered replay finishes,


Key press ("h")
Mouse click (left button)
XHR readyState (4, data=...)
Timer 0 (@4s)
kp0() kp1()
mc0() mc1()
xhr0()
t0()
x() y() //Sets the //timer period //to t=4s
z() //Registers //timer 0 for //t=4s
q() Date()

(a) A snippet of the program's original execution, showing two GUI events (each of which triggers two top-level event handlers), a network event which indicates the reception of data from a remote server, and a timer which fires at a wall clock time of 4 seconds after the program started execution.


Key press ("h")
Mouse click (left button)
XHR readyState (4, data=...)
Timer 0 (@3s)
Timer 0 (@4s)
kp0() kp1()
mc0() mc1()
xhr0()
t0()
t0()
x() y() //Edits the //timer period //from 4s to 3s; //cancels the //XHR
z() //Registers //timer 0 for //t=3s
q() Date() //Returns //extrapolated //value
q() Date()

(b) During the replay process, the developer edits function `y()`. As a result, the XHR event is never replayed; additionally, the timer fires early, and receives a different value from `Date()`.

Figure 4: An example of how an edit changes the replay process. Beneath each event, we depict the associated call chains. Red indicates functions whose behavior is altered by the edit. Grey indicates events from the original execution which do not occur in the post-edit universe.

developers can compare the data flows of the original and altered executions, looking for evidence that the hypothesized bug fix actually succeeded. Reverb uses classical string diffing algorithms [10, 14] to quickly identify the reads and writes that diverge in the two provenance chains. Reverb's logs contain enough information to reconstruct execution traces at the granularity of individual source code lines (see Figure 8); thus, developers can use differential slicing [31] to align divergent executions with respect to shared and non-shared lines of executed source code.

3.4 Debugging Across the Wide Area

Node: Node [58] is a server-side implementation of the JavaScript runtime. Like a browser-based JavaScript engine, Node exposes a single-threaded, event-driven interface. A Node application runs headless, i.e., without a GUI, but otherwise has access to timers, nondeterministic functions like `Date()`, and asynchronous IO channels like network sockets. Reverb interposes on these nondeterministic inputs using the same techniques that it leverages on the client-side.

To track causality between a client and a Node server, Reverb uses vector clocks [20, 36] to establish a partial ordering over the distributed events. At logging time, when a client issues an `XMLHttpRequest`, Reverb transparently adds a new cookie value which contains the client's clock. On the server-side, Reverb transparently modifies the HTTP request handler to extract the client clock and update the server's clock appropriately. When the server generates the HTTP response, Reverb uses a `Set-Cookie` header to transmit the server's updated clock to the client;[1] the client extracts the cookie and updates the local clock. The client browser automatically persists the cookie on local storage, as the browser would do for any other type of cookie.

In JavaScript, a program can associate a single top-level event with multiple handlers. At logging time, a client or server updates the local clock at the beginning of each event dispatch, before handlers run. The use of browser cookies to store client clocks allows a client to detect when *passively-fetched content* triggers server-side JavaScript execution. For example, suppose that client-side JavaScript code injects a new `<link>` tag into the page using the `innerHTML` DOM method; such a tag might represent a new style sheet. Client-side JavaScript will not have an opportunity to inspect the HTTP response headers for the `<link>`. However, when the next JavaScript-visible event fires, the first handler for that event can inspect the cookie that was set by the `<link>` fetch, extract the server's vector clock, and then update the local vector clock appropriately.

At replay time, Reverb collates the client logs and the server logs, using logical clocks to generate a total ordering over all events. Reverb then replays events from the total ordering; at each step, Reverb moves either a client or a server one event further in the global log.

Note that each host's log contains sufficient information to replay the host in isolation—the log contains all of the external nondeterministic stimuli that affected the host, as well as internal nondeterminism like GUI events or the values returned by clock reads. So, if a host communicates with multiple parties, but only some of them run Reverb, then the host can be replayed by itself, or in concert with some or all of the Reverb-enabled hosts. However, Reverb must be vigilant for speculative edits that generate new, unlogged requests to entities that are not participating in the replay (§3.3).

Black-box components: A client-side browser and a server-side Node engine both run single-threaded, event-driven JavaScript code. In contrast, server-side components like Redis and NGINX are single-threaded and event-driven, but are written in C, C++, or another non-JavaScript language. Reverb treats each such component as a black box, logging incoming requests and outgoing responses using a proxy. For example, our Reverb prototype intercepts HTTP traffic that is exchanged with a Redis server, using Redis-specific rules to extract `get(k)` and `put(k,v)` commands,

[1] A subtlety is that, if a server is concurrently handling multiple requests for a particular client, the server must ensure that the client receives a sequence of responses whose vector clocks have strictly increasing numbers in the server's slot. This policy is necessary because the client-side browser uses a "last-write-wins" policy for cookies.

and serialize the order in which commands are sent to Redis. Reverb assumes that each event handler inside a black box is deterministic, such that replaying a serialized stream of requests will result in 1) the same internal state for the component, and 2) the same responses being returned.[2] These assumptions are reasonable for server-side components like Redis that act as fairly simple front-ends to storage; however, these assumptions may not hold for server-side components that are written in arbitrarily-expressive, non-JavaScript languages like C++ or Go.

Reverb uses vector clocks to establish causality between black-box components and JavaScript-based components. However, Reverb does not log the reads and writes that black-box components make to internal state. Thus, data flows involving black-box state originate and terminate in the high-level requests and responses that black-box components exchange with external parties. For example, Reverb can track a JavaScript value on a client to the server-side Redis `get()` responses that influenced that value; however, Reverb cannot peer inside Redis to see why those responses were completed in a particular way.

At the beginning of logging, Reverb takes a snapshot of a black-box component's initial state using native mechanisms (e.g., Redis' built-in snapshot facility). At the beginning of replay, Reverb uses the snapshot to initialize the component.

Speculative wide-area edits: Reverb allows a developer to pause the wide-area application, edit client-side or server-side JavaScript, DOM, or storage state, and then resume execution. In general, Reverb uses the techniques from Section 3.3 to handle divergence, but wide-area debugging introduces some new divergence scenarios.

Define a requestor as a component that generates a request, and the responder as the component that responds. Browsers always acts as requestors, with server-side components acting as the corresponding responders; however, as server-side components talk to each other, they may act as requestors or responders at different points in time.

An edit may cause a responder to return a different response to a particular request, where "a particular request" is defined as a request made at a specific vector clock time. Reverb can detect such divergence because, at replay time, Reverb interposes on the methods that the responder uses to return data; Reverb compares the replay-time value of the response to the logged value from the original execution. If the values are different, Reverb rewrites the appropriate requestor-side log entries, propagating the new data. Later, replaying those events will naturally inject the new data into the requestor-side execution state. Subsequent requestor-side divergence is then handled using the approaches from Section 3.3.

[2]At replay time, individual responses may be emitted in a different order than the logging-time one, due to nondeterministic replay-time access delays to storage media like SSDs. However, Reverb's distributed replay driver buffers the responses, and ensures that response data is delivered to clients in the logging-time order.

If an edit induces a requestor to send a modified request to a responder, Reverb rewrites the appropriate responder-side log entry. When the replay logic applies the log entry to the responder, the replay logic buffers the response, and then replays the response on the requestor at the moment indicated in the log; note that the response may contain altered content with respect to the original, logged version of the response.

An edit can induce a requestor to generate a completely new request at a vector clock time that was not associated with a request during the original execution. In this scenario, Reverb's requestor-side replay driver does not allow the request to hit the real network. Instead, the responder-side driver injects a fake request into the responder-side log, and then resumes the replay process. Eventually, the replaying responder will handle the new event, and generate a response. The replay driver will buffer the response, and use a network model to determine when to replay the response on the requestor.

An edit may cause a requestor to not generate a logged request. In this case, Reverb does not replay the associated downstream events on the responder or the requestor. For example, if a browser does not issue a logged `XMLHttpRequest` to a Node server, then Reverb will not replay the Node-side HTTP request event, or the downstream browser-side events corresponding to the reception of the HTTP response.

Replay subtleties: A single web page can embed content from multiple origins. Cookies are isolated using the same-origin policy [46], so a page from origin `foo.com` cannot access cookies that are set by (say) `<img>` fetches to `bar.com`. Thus, JavaScript code in the enclosing `foo.com` page cannot read `bar.com`'s latest vector clock. An in-browser implementation of Reverb can easily avoid this problem by allowing cross-origin cookie accesses when the browser is running in debug mode. A JavaScript-level implementation of Reverb must force all remote servers to reside in the same origin. This is often infeasible for the production version of a complex page, but possible for a testing version in which all page content is recorded using Mahimahi [54] or Fiddler [66], and then served from a single proxy that rewrites URLs to point to the proxy's origin.

A JavaScript-level implementation of Reverb must also be careful to replay `load` events properly. These events cannot be synthetically generated or deferred by JavaScript code, since JavaScript code has no ability to force the network stack to release bytes at controlled intervals. So, to properly replay the `load` event for a passively fetched object like an `<img>`, Reverb must ensure that, from a client's perspective, the `<img>` (and its vector-clock-containing cookie) arrive at a time that respects the vector clocks in the client-side log events. Practically speaking, this means that the server-side replay driver must coordinate with the client-side driver, and only release the last byte of a passively-fetched object when the wide-area replay has reached the appropriate point [38].

4 Implementation

To log deterministic reads and writes to the JavaScript heap and the DOM, Reverb uses a modified version of Scout [53]. The stock version of Scout rewrites JavaScript and HTML, injecting instrumentation that runs during each read or write to JavaScript or DOM state. Reverb extends Scout so that it logs nondeterministic JavaScript events like mouse clicks and timer firings. At replay time, Reverb reconstructs data flows using the low-level Scout traces. Reverb defines a default set of data flow manipulations, like targeted dynamic traces (§3.2). However, Reverb stores raw data flow logs in a simple JSON format, and defines a plugin model which allows developers to create their own queries. To display data flow graphs, Reverb uses the NEATO visualization library [25].

At replay time, Reverb injects a custom JavaScript library into the application code that runs on a browser or a Node instance. The library acts as a replay driver, dispatching high-level events from the log as requested by the human developer who is managing the debugging workflow. The event dispatch process is similar to that of prior replay frameworks like Mugshot [38] or Jardis [11], although Reverb dispatches events across multiple hosts during wide-area replay (§3.4). Black-box components like Redis are logged and replayed using a component-specific replay proxy (§3.4).

During replay, Reverb uses Mahimahi [54], a record-and-replay framework for HTTP requests, to serve browser-side content that is fetched via the `src` attribute of HTML tags. Content that is actively fetched by JavaScript code is served by the replay driver, from the log of nondeterministic events. During a wide-area replay that involves clients and server-side components, Mahimahi only returns passively-fetched content that was not returned by a server-side component during the original execution.

To support speculative edit-and-continue, Reverb must be able to modify the code or data belonging to a paused JavaScript execution context. One implementation option would be to change the C++ code inside a JavaScript engine to expose mutation hooks for internal state. Our Reverb prototype uses a different approach—it executes the JavaScript code atop MetaES [12], a JavaScript interpreter that is written in JavaScript. This approach allows Reverb to be used with arbitrary client browsers or Node implementations, since Reverb can mutate application state without assistance from the underlying JavaScript engine. A developer expresses a pause point as a 2-tuple consisting of a source code line and a trigger condition, e.g., "the i-th iteration of the enclosing loop." Reverb will pause the MetaES interpreter at the appropriate moment. The developer can inspect the program state, devise an edit, and then express that edit to Reverb in the form of a JavaScript statement for Reverb to speculatively apply to the replay (§3.3).

5 Evaluation

In this section, we demonstrate that Reverb is an *efficient, helpful tool for bug analysis.*

5.1 The Tractability of Data Flow Analysis

Intuition might suggest that tracking all deterministic and nondeterministic events would produce huge logs. However, in the Alexa Top 300 pages [3], the median number of reads and writes that occur during a page load are 13,275 and 6,328, respectively. Those numbers are surprisingly low, given the fact that an average web page includes 401 KB of JavaScript source code [70]. However, diagnosing bugs is still tricky: a graph with thousands of nodes is small enough to be efficiently analyzed by a computer, but big enough to be hard for a human to understand. For example, across the 300 test pages:

- the median number of writes per variable was 8, with a 95th percentile of 210;
- the median number of unique source code lines that wrote a variable was 5, with a 95th percentile of 22;
- when considering the final value for each variable, the median length of the value's provenance chain (§3.2) was 16, with a 95th percentile of 131.

These statistics are for the JavaScript code which executes during a page load. After the load completes, additional JavaScript executes in response to GUI interactions, the firing of timers, and so on. Executing post-load call chains results in more reads and writes for Reverb to track, but the volume is low compared to the activity that is generated by the initial page load. As a concrete example, on the `wsj.com` website, hovering over a menu item at the top of the page will trigger several event handlers for mouse activity. However, firing these handlers only generates 486 reads and 107 writes. In contrast, the initial page load generates 33,844 reads and 16,121 writes.

Using Mahimahi [54], we loaded Reverb-instrumented pages under a variety of emulated network conditions, measuring the client-perceived impact of Reverb's instrumentation. Due to space restrictions, we elide a full discussion of the results, and just note that Reverb's client-side instrumentation is fast enough to add to real, customer-facing pages; for example, on a 12 Mbits/s link with a 50 ms RTT, median page load time slows by just 5.5%. The logs for Reverb-instrumented pages also grow slowly: across our 300 page corpus, the median (gzipped) log size after a page load was 45.4 KB, with a 95th percentile size of 113.2 KB. Given such a log, Reverb required a median of 7.8 seconds to generate a full data flow graph; the 95th percentile time was 32.3 seconds. Note that graph generation can be performed in the background during the logging run. Thus, much or all of the cost can be paid before a human developer begins the debugging process.

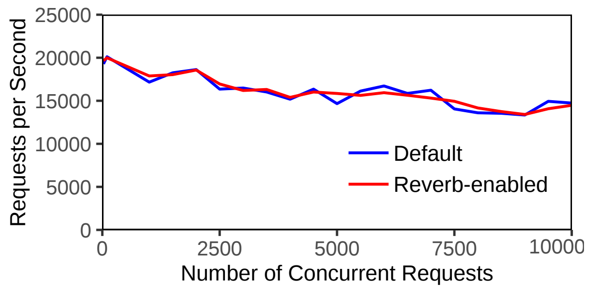


Figure 5: Response throughput for two versions of a Node server. Each data point represents the throughput across 100,000 requests.

5.2 Server-side Overheads

Reverb's logging approach for a Node server is similar to Reverb's logging approach for a client-side browser (§3.4). However, a Node server that handles many clients will produce log entries more quickly than a client browser which loads a single page and then intermittently handles user input. To examine Reverb overheads on Node, we wrote a simple Node web server. For each request, the server returned the dynamic string `''Hello world at '' + (new Date()).getTime()`. For each request, Reverb had to log the incoming HTTP request, a few dozen reads and writes inside the server's request handler, the timestamp returned by `Date()`, and the outgoing HTTP response. This toy server was a pessimistic test of Reverb's overheads, since real server code has a higher ratio of executed source code lines per nondeterministic value logged.

We used the Apache benchmarking tool `ab` [9] to generate HTTP requests. We placed the Node server and `ab` on the same machine, to emphasize Reverb's computational overheads. As shown in Figure 5, we varied the number of concurrent client requests from 25 to 10,000, measuring response throughput for a normal version of the server, and a Reverb-enabled variant. The throughputs of the two servers were within 3% of each other. CPU utilization was also similar for the two servers.

The growth of Reverb's compressed log was 258 Kbps (equivalent to 32.3 KB per second). Note that black box components like Redis have slower log growth—for these components, Reverb logs incoming requests and responses, but not deterministic reads or writes to internal black-box state.

5.3 Bug Diagnosis Case Study: EtherCalc

Evaluating a new debugging platform is tricky, and partially subjective. In this section, we provide an in-depth case study of how we used Reverb to debug a web application that we did not create, and whose code we had no previous familiarity with.

As shown in Figure 1, EtherCalc is a collaborative spreadsheet application. A single document can be simultaneously viewed and edited by multiple users, with a Node server disseminating updates across browsers, and

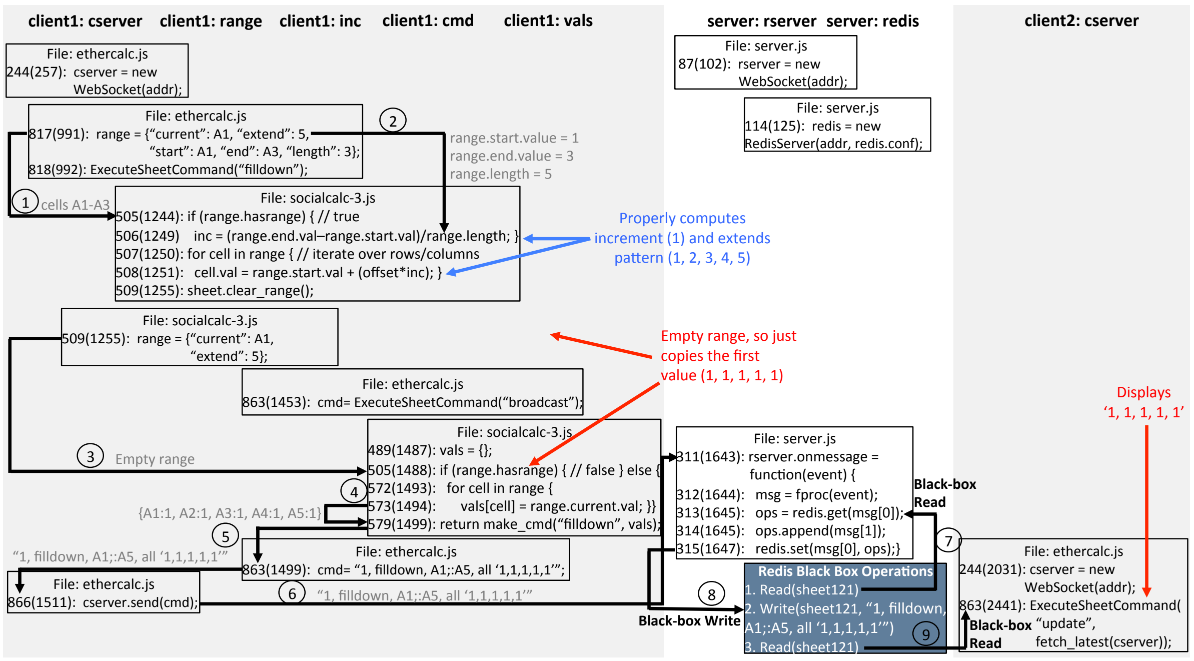
	Mailpile	EtherCalc
Total writes	24,202	31,251
Total reads	67,335	89,737
JavaScript heap objects	2,822	4,028
DOM nodes	619	1,531
Wall-clock time to bug at logging time	12.8 secs	10.4 secs
Wall-clock time to bug at replay time	3.1 secs	3.9 secs

Figure 6: Summary statistics for the Mailpile and EtherCalc case studies. Note that, during replay, Reverb can skip user think time, so Reverb can replay a buggy execution faster than it originally occurred.

storing the canonical spreadsheet state in a Redis database. EtherCalc is the largest application that we examined, consisting of 36 HTML files, 899 JavaScript files, and 232,662 total lines of code. Figure 6 provides additional statistics about the application.

Bug #314 involves a broken propagation of auto-fill operations between two browsers. In an auto-fill operation, a user enters data (e.g., "1,2,3") into a few exemplar cells; the user then highlights the cells, and drags the bottom edge of the highlighted region downward, causing the spreadsheet to guess the pattern in the exemplar cells and automatically apply the pattern (e.g., "4,5") to subsequent cells. In Bug #314, auto-fill operations that are generated on one browser are not properly delivered to other browsers. In the example above, the first browser (`client1`) would correctly display "1,2,3,4,5", but the second browser (`client2`) would display "1,1,1,1,1". We recreated this problem, recording a buggy session that involved two browsers, a Node server, and a Redis server.

Diagnosing the bug: Figure 7 annotates a targeted dynamic trace for the buggy execution; to make room for the annotations, we removed the more obvious data flows. When `client1`'s user initiates an auto-fill, EtherCalc creates a `range` object which describes the auto-fill operation; for example, the `range` object contains the start cell and ending cell for the base pattern, as well as the start cell and ending cell for the range where the extrapolated data should be placed. EtherCalc then calls `ExecuteSheetCommand()`, using the `filldown` parameter to indicate a pattern extension request. The function checks whether a valid `range` object is present (1), and if it exists, the function uses values in the object to determine the appropriate increment value for the pattern extension (2). After applying the auto-fill to `client1`'s GUI and JavaScript state, `ExecuteSheetCommand()` overwrites `client1`'s `range` object, effectively removing several properties like `start` and `extend`. `client1` then calls `ExecuteSheetCommand()` again, passing a different parameter called `broadcast`. This parameter specifies that `ExecuteSheetCommand()` should *not*



```
File: ethercalc.js
244(257):  cserver = new
           WebSocket(addr);
```

```
File: ethercalc.js
817(991):  range = {“current”: A1, “extend”: 5,
                    “start”: A1, “end”: A3, “length”: 3};
818(992): ExecuteSheetCommand(“filldown”);
```

```
File: socialcalc-3.js
505(1244): if (range.hasrange) { // true
506(1249)    inc = (range.end.val–range.start.val)/range.length; }
507(1250): for cell in range { // iterate over rows/columns
508(1251):   cell.val = range.start.val + (offset*inc); }
509(1255): sheet.clear_range();
```

```
File: socialcalc-3.js
509(1255):  range = {“current”: A1,
                     “extend”: 5};
```

```
File: ethercalc.js
863(1453):  cmd= ExecuteSheetCommand(“broadcast”);
```

```
File: socialcalc-3.js
489(1487): vals = {};
505(1488): if (range.hasrange) { // false } else {
572(1493):   for cell in range {
573(1494):       vals[cell] = range.current.val; }}
579(1499): return make_cmd(“filldown”, vals);
```

```
File: ethercalc.js
863(1499):  cmd= “1, filldown, A1;:A5, all ‘1,1,1,1,1’”;
```

```
File: ethercalc.js
866(1511):  cserver.send(cmd);
```

```
File: server.js
87(102):  rserver = new
          WebSocket(addr);
```

```
File: server.js
114(125):  redis = new
RedisServer(addr, redis.conf);
```

```
File: server.js
311(1643): rserver.onmessage =
              function(event) {
312(1644):   msg = fproc(event);
313(1645):   ops = redis.get(msg[0]);
314(1645):   ops.append(msg[1]);
315(1647):   redis.set(msg[0], ops);}
```

```
Redis Black Box Operations
1. Read(sheet121)
2. Write(sheet121, “1, filldown,
A1;:A5, all ‘1,1,1,1,1’”)
3. Read(sheet121)
```

```
File: ethercalc.js
244(2031): cserver = new
           WebSocket(addr);
863(2441): ExecuteSheetCommand(
             “update”,
             fetch_latest(cserver));
```

Figure 7: A buggy EtherCalc session. The i-th executed source code line is prefixed with `lineNumInSrcFile(i)`. Black arrows represent data flows between executed source code lines: data written by the source code at the base of an arrow is read by source code at the head of the arrow. The blue and red text was manually added to highlight specific parts of the debugging narrative; Reverb generates the information in the rest of the diagram.

apply the operation to local state, but instead send that operation to the Node server, who will persist the operation in Redis and then distribute the operation to other clients. As in the first execution of `ExecuteSheetCommand()`, the function checks whether a valid `range` object exists. However, in this case, because the prior function execution partially cleared the `range` object, the validity check fails (3). As a result, `ExecuteSheetCommand()` simply generates an operation which copies the value in `range.current` to all cells covered by `range.current` to `range.length` (4); note that these two properties were not removed during the earlier reset of the `range` object. The resulting operation (5) is what will eventually create the autofill “1, 1, 1, 1, 1” (rather than “1, 2, 3, 4, 5”) on `client2`. `client1` sends the operation to the Node server (6), triggering a server-side `onmessage` handler. The handler issues a black-box read to Redis, fetching the list of all operations that have been applied to the spreadsheet (7). The handler appends the new operation to the list, and then uses a black-box write to store the updated list on Redis (8). Later, when `client2` opens the spreadsheet (9), `client2` will fetch the buggy operation list and use the list to update the local GUI.

Fixing the bug: Reverb made it easy for us to generate a wide-area data flow graph. However, these graphs do not automatically provide a bug fix; instead, the graphs help to localize where buggy state is being created, and how that state is being propagated. Thus, our next task was to try to actually fix the bug. An obvious potential fix was to modify `ExecuteSheetCommand()` so that the first invocation did not reset the `range` object. We made this edit and then performed a speculative replay. The edit initially appeared successful—the Node server received the correct auto-fill operation, stored it on Redis, and then sent it to the second browser, who correctly applied the operation. However, our recorded session contained *two* auto-fill operations involving two distinct sets of cells; our hypothesized fix prevented the second auto-fill operation from appearing in the GUI of the first browser or the second browser. Looking at the distributed data flow, we saw that the first browser was not generating a second auto-fill locally (and therefore was not sending a second auto-fill operation to the Node server).

Further investigation of `ExecuteSheetCommand()`'s code revealed that the first call in a pair of invocations expects the `range` object to be set to a default value—otherwise, `ExecuteSheetCommand()` terminates without updating the local spreadsheet or sending an update to remote clients via the Node server. We tried a different bug fix in which the second call to `ExecuteSheetCommand()` clears the `range` object at the *end* of `ExecuteSheetCommand()`'s execution. The speculative replay for this fix led to no problems—both auto-fill operations were properly displayed on both browsers.

Of course, the successful speculative replay was not a proof of the fix's correctness; the successful replay was essentially the successful passing of a unit test involving a particular usage scenario. However, this case study demonstrates how replay debugging, wide-area data flow tracking, and speculative edits work in concert to ease the cognitive overhead of understanding large code bases.

5.4 Additional Case Studies

We have used Reverb to diagnose a variety of additional bugs. The appendix (§A.1 and §A.2) of the extended technical report [8] provides detailed case studies for two of them. The first case study demonstrates Reverb's usefulness in debugging visual errors involving DOM misconfiguration; the second case study shows how Reverb helps developers to fix errors in third-party JavaScript code that local developers did not write.

5.5 Speculatively Replaying Known-Good Bug Fixes

As another test of Reverb's efficacy, we randomly examined five resolved bugs[3] contained in the public bug database of jQuery [67]. jQuery is a popular client-side JavaScript library for DOM manipulation; the library consists of roughly 6,600 lines of code. For each of the resolved bugs, we did the following:

- First, we downloaded the buggy version of jQuery that immediately preceded the patched version.
- We verified that Reverb could reproduce the bug using traditional (i.e., non-speculative) deterministic replay.
- We then replayed the library to the moment that preceded the faulty behavior. We paused the replay at that point, applied the known-good bug fix from the bug database, and then resumed the now-speculative replay to see whether the replay would finish without displaying the faulty behavior.

For all five cases, Reverb's edited replay correctly indicated that the "speculative" bug fix was indeed a correct one.

5.6 User Study

To determine whether Reverb would be useful to people besides the paper authors, we performed a small user study involving six participants. All participants had prior experience with front-end web development, and all possessed at least some familiarity with traditional in-browser debuggers. All participants brought their own laptops to the user study, but debugging exercises were performed inside of a VM provided by the paper authors, to ensure uniformity of experience.

For each user, we first provided a refresher tutorial about how the traditional debugger works; we discussed topics like watchpoints, breakpoints, and code prettification. We also explained how Reverb's data flow graphs are generated and refined via human-driven queries. Once both tutorials were complete, we presented the user with a real bug to diagnose. The bug involved a JavaScript exception being thrown by a real, complex web page; refer to Section A.2 in the extended technical report [8] for a detailed description of the bug. We divided the participants equally, creating two groups of three; the first group was asked to use Reverb to diagnose the bug, whereas the second group was asked to use the traditional in-browser debugger. Each person was given ten minutes to diagnose the bug. When a user believed that she had found the root cause for the bug, she informed the paper authors, who then verified whether the hypothesized root cause was correct. If it was not, the user was told to keep working until a correct diagnosis was generated, or ten minutes elapsed.

Two of the Reverb users diagnosed the bug in less than five minutes, with the third user did so within ten minutes. In contrast, one user of the traditional debugger failed to diagnose the error within the ten minute window. The remaining two users of the traditional debugger correctly diagnosed the fault before the timer elapsed, but required more than five minutes. Thus, these results suggest that Reverb is a more powerful diagnostic tool than a traditional debugger.

At the end of the study, we asked the participants some qualitative questions. In response to the question "Would you prefer to use Reverb over a traditional debugger?", five out of six participants said yes. The one person who disagreed complained about Reverb's GUI (which is admittedly rudimentary in our prototype). In particular, the complaining user said that graph querying and pruning was unnecessarily awkward. When asked "Would Reverb-style data flow operations be a useful compliment to standard debugging primitives?", all six participants said yes. Furthermore, all three Reverb users declared, without prompting, that speculative edit-and-continue would be a powerful debugging feature.

Testing bug fixes is inherently unsound, even without Reverb (§1); unsurprisingly, the replay of an edited execution may occasionally lead to confusing results. In the authors' own experience, these incidents usually involve the replaying of GUI events. For example, if an edit changes the visual locations of DOM nodes, then replaying (say) a mouse click to a particular (x,y) coordinate may result in unexpected event handlers firing. Reverb's ability to diff the data flows and control flows of a logged execution and an edited one can identify the reason for divergence, but developers must be diligent about checking the diffs when exploring counterintuitive post-edit behaviors.

6 Conclusion

Reverb is the first replay debugger that tracks fine-grained, wide-area data flows while also supporting speculative edit-and-continue. Such capabilities were impossible in prior debugging frameworks because those frameworks logged program behavior at the wrong level of abstraction; in contrast, Reverb efficiently tracks behavior at the level of managed code and single-threaded event loops. Case studies demonstrate that Reverb is a powerful tool for diagnosing real, complex bugs.

[3]We examined bugs #3439, #3472, #3571, #3573, and #3579.

References

[1] H. Agrawal, R. A. DeMillo, and E. H. Spafford. Dynamic slicing in the presence of unconstrained pointers. In *Proceedings of the Symposium on Testing, Analysis, and Verification*, TAV4. ACM, 1991.

[2] H. Agrawal and J. R. Horgan. Dynamic Program Slicing. In *Proceedings of the ACM SIGPLAN 1990 Conference on Programming Language Design and Implementation*, PLDI. ACM, 1990.

[3] Alexa. Top Sites in the United States. `http://www.alexa.com/topsites/countries/US`.

[4] B. Alpern, T. Ngo, J.-D. Choi, and M. Sridharan. DejaVu: Deterministic Java Replay Debugger for JalapeÑO Java Virtual Machine. In *Proceedings of OOPSLA*. ACM, 2000.

[5] Anonymous. Anonymized for double-blind reviewing.

[6] Anonymous. Anonymized for double-blind reviewing.

[7] Anonymous. Anonymized for double-blind reviewing.

[8] Anonymous. Reverb Technical Report. `https://github.com/anonymous-tr/Reverb_SOCC19_Technical_Report/blob/master/reverb_technical_report.pdf`.

[9] Apache Software Foundation. `https://httpd.apache.org/docs/2.4/programs/ab.html`, 2017.

[10] G. V. Bard. Spelling-error tolerant, order-independent pass-phrases via the damerau-levenshtein string-edit distance metric. In *Proceedings of the Fifth Australasian Symposium on ACSW Frontiers*, ACSW. Australian Computer Society, Inc., 2007.

[11] E. T. Barr, M. Marron, E. Maurer, D. Moseley, and G. Seth. Time-Travel Debugging for JavaScript/Node.js. In *Proceedings of the 2016 International Symposium on the Foundations of Software Engineering*, FSE. ACM, 2016.

[12] Bartosz Krupa. Metaes. `https://github.com/metaes/metaes`.

[13] J.-F. Bergeretti and B. A. Carré. Information-flow and Data-flow Analysis of While-programs. *ACM Trans. Program. Lang. Syst.*, 7(1), Jan. 1985.

[14] P. Bille. A survey on tree edit distance and related problems. *Theor. Comput. Sci.*, 337(1-3):217–239, June 2005.

[15] D. Binkley, M. Harman, and J. Krinke. Empirical Study of Optimization Techniques for Massive Slicing. *ACM Trans. Program. Lang. Syst.*, 30(1), November 2007.

[16] G. W. Dunlap, S. T. King, S. Cinar, M. A. Basrai, and P. M. Chen. ReVirt: Enabling Intrusion Analysis Through Virtual-machine Logging and Replay. *SIGOPS Oper. Syst. Rev.*, 36(SI), Dec. 2002.

[17] Eclipse. FAQ What is hot code replace? `https://goo.gl/brp5oQ`, 2016.

[18] S. I. Feldman and C. B. Brown. IGOR: A System for Program Debugging via Reversible Execution. In *Proceedings of the 1988 ACM SIGPLAN and SIGOPS Workshop on Parallel and Distributed Debugging*, PADD. ACM, 1988.

[19] J. Ferrante, K. J. Ottenstein, and J. D. Warren. The Program Dependence Graph and Its Use in Optimization. *ACM Trans. Program. Lang. Syst.*, 9(3):319–349, July 1987.

[20] C. J. Fidge. Timestamps in message-passing systems that preserve the partial ordering. *Proceedings of the 11th Australian Computer Science Conference*, 10:56–66, 1988.

[21] Firebug. Javascript debugger and profiler. `http://getfirebug.com/javascript`.

[22] GDB: The GNU Project Debugger. GDB and Reverse Debugging. `https://www.gnu.org/software/gdb/news/reversible.html`, November 2012.

[23] D. Geels, G. Altekar, S. Shenker, and I. Stoica. Replay Debugging for Distributed Applications. In *Proceedings of the USENIX Annual Technical Conference*, ATEC. USENIX, 2006.

[24] Google Developers. Debug. `https://developers.google.com/web/tools/chrome-devtools/debug/?hl=en`.

[25] Graphviz. Drawing Graphs with NEATO. `http://www.graphviz.org/pdf/neatoguide.pdf`.

[26] T. Gyimóthy, A. Beszédes, and I. Forgács. An Efficient Relevant Slicing Method for Debugging. In *Proceedings of the 7th European Software Engineering Conference Held Jointly with the 7th ACM SIGSOFT International Symposium on Foundations of Software Engineering*, ESEC/FSE-7, London, UK, UK, 1999. Springer-Verlag.

[27] C. Hammer and G. Snelting. Flow-sensitive, Context-sensitive, and Object-sensitive Information Flow Control Based on Program Dependence Graphs. *Int. J. Inf. Secur.*, 8(6), Oct. 2009.

[28] I. Hickson. Web workers. `https://www.w3.org/TR/workers/`, 2015.

[29] S. Hong, Y. Park, and M. Kim. Detecting Concurrency Errors in Client-Side Java Script Web Applications. In *Proceedings of the 2014 IEEE International Conference on Software Testing, Verification, and Validation*, ICST. IEEE Computer Society, 2014.

[30] J. Howell, B. Parno, and J. R. Douceur. Embassies: Radically Refactoring the Web. In *Proceedings of the 10th USENIX Conference on Networked Systems Design and Implementation*, NSDI. USENIX, 2013.

[31] N. M. Johnson, J. Caballero, K. Z. Chen, S. McCamant, P. Poosankam, D. Reynaud, and D. Song.

Differential Slicing: Identifying Causal Execution Differences for Security Applications. In *Proceedings of the 2011 IEEE Symposium on Security and Privacy*, SP. IEEE Computer Society, 2011.

[32] A. J. Ko and B. A. Myers. Debugging Reinvented: Asking and Answering Why and Why Not Questions About Program Behavior. In *Proceedings of the 30th International Conference on Software Engineering*, ICSE. ACM, 2008.

[33] B. Korel and J. Laski. Dynamic Program Slicing. *Information Processing Letters*, 29(3), Oct. 1988.

[34] A. Lienhard, T. Gîrba, and O. Nierstrasz. Practical Object-Oriented Back-in-Time Debugging. In *Proceedings of the 22Nd European Conference on Object-Oriented Programming*, ECOOP, Berlin, Heidelberg, 2008.

[35] Mailpile. `https://github.com/mailpile/Mailpile`, 2017.

[36] F. Mattern. Virtual time and global states of distributed systems. In M. C. et. al., editor, *Parallel and Distributed Algorithms: proceedings of the International Workshop on Parallel & Distributed Algorithms*, pages 215–226. Elsevier Science Publishers B. V., 1989.

[37] J. Mickens and M. Dhawan. Atlantis: Robust, Extensible Execution Environments for Web Applications. In *Proceedings of the Twenty-Third ACM Symposium on Operating Systems Principles*, SOSP. ACM, 2011.

[38] J. Mickens, J. Elson, and J. Howell. Mugshot: Deterministic Capture and Replay for Javascript Applications. In *Proceedings of NSDI*, 2010.

[39] Microsoft. Edit and continue. `https://msdn.microsoft.com/en-us/library/bcew296c.aspx`.

[40] Mozilla Developer Network. Concurrent model and Event Loop. `goo.gl/UmzCa5`.

[41] Mozilla Developer Network. Debugger. `https://developer.mozilla.org/en-US/docs/Tools/Debugger`.

[42] Mozilla Developer Network. Document Object Model (DOM). `https://developer.mozilla.org/en-US/docs/Web/API/Document_Object_Model`, August 2016.

[43] Mozilla Developer Network. HTTP Cookies. `https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies`, 2016.

[44] Mozilla Developer Network. ¡iframe¿. `https://developer.mozilla.org/en-US/docs/Web/HTML/Element/iframe`, 2016.

[45] Mozilla Developer Network. IndexedDB API. `https://developer.mozilla.org/en-US/docs/Web/API/IndexedDB_API`, 2016.

[46] Mozilla Developer Network. Same-origin Policy. `https://developer.mozilla.org/en-US/docs/Web/Security/Same-origin_policy`, 2016.

[47] Mozilla Developer Network. Web Storage API. `https://developer.mozilla.org/en-US/docs/Web/API/Web_Storage_API`, 2016.

[48] Mozilla Developer Network. WebSocket. `https://developer.mozilla.org/en-US/docs/Web/API/WebSocket`, 2016.

[49] Mozilla Developer Network. XMLHttpRequest. `https://developer.mozilla.org/en-US/docs/Web/API/XMLHttpRequest`, 2016.

[50] K.-K. Muniswamy-Reddy, D. Holland, U. Braun, and M. Seltzer. Provenance-Aware Storage Systems. In *Proceedings of USENIX ATC*, 2006.

[51] E. Mutlu, S. Tasiran, and B. Livshits. Detecting JavaScript Races That Matter. In *Proceedings of the 2015 10th Joint Meeting on Foundations of Software Engineering*, ESEC/FSE. ACM, 2015.

[52] N. Nethercote and A. Mycroft. Redux: A dynamic dataflow tracer. In *Electronic Notes in Theoretical Computer Science*. Elsevier, 2003.

[53] R. Netravali, A. Goyal, J. Mickens, and H. Balakrishnan. Polaris: Faster Page Loads Using Fine-grained Dependency Tracking. In *Proceedings of NSDI*. USENIX Association, 2016.

[54] R. Netravali, A. Sivaraman, S. Das, A. Goyal, K. Winstein, J. Mickens, and H. Balakrishnan. Mahimahi: Accurate Record-and-Replay for HTTP. In *Proceedings of ATC*, Santa Clara, CA, 2015. USENIX Association.

[55] NGINX Inc. Nginx. `https://www.nginx.com/`, 2017.

[56] H. V. Nguyen, C. Kästner, and T. N. Nguyen. Building Call Graphs for Embedded Client-side Code in Dynamic Web Applications. In *Proceedings of the 22Nd ACM SIGSOFT International Symposium on Foundations of Software Engineering*, FSE. ACM, 2014.

[57] H. V. Nguyen, C. Kästner, and T. N. Nguyen. Cross-language Program Slicing for Dynamic Web Applications. In *Proceedings of the 2015 10th Joint Meeting on Foundations of Software Engineering*, ESEC/FSE. ACM, 2015.

[58] Node.js Foundation. Node.js. `https://nodejs.org/en/`, 2017.

[59] F. S. Ocariza, K. Bajaj, K. Pattabiraman, and A. Mesbah. An empirical study of client-side javascript bugs. In *2013 ACM / IEEE International Symposium on Empirical Software Engineering and Measurement*, 2013.

[60] F. S. Ocariza, G. Li, K. Pattabiraman, and A. Mesbah. Automatic fault localization for client-side javascript. *Softw. Test. Verif. Reliab.*, 26(1), Jan. 2016.

[61] F. S. Ocariza, K. Pattabiraman, and B. Zorn. JavaScript Errors in the Wild: An Empirical Study. In *Proceed-*

ings of the 2011 IEEE 22Nd International Symposium on Software Reliability Engineering, ISSRE. IEEE Computer Society, 2011.

[62] Redis Labs. Redis. `https://redis.io/`, 2017.

[63] S. Shah, C. Soules, G. Ganger, and B. Noble. Using Provenance to Aid in Personal File Search. In *Proceedings of USENIX ATC*, 2007.

[64] M. Tancreti, V. Sundaram, S. Bagchi, and P. Eugster. TARDIS: Software-only System-level Record and Replay in Wireless Sensor Networks. In *Proceedings of the 14th International Conference on Information Processing in Sensor Networks*, IPSN. ACM, 2015.

[65] A. Tang. EtherCalc: A Web Spreadsheet. `https://ethercalc.net/`, 2017.

[66] Telerik. Fiddler. `http://www.telerik.com/fiddler`.

[67] The jQuery Foundation. jQuery. `https://jquery.com/`, 2018.

[68] F. Tip. A Survey of Program Slicing Techniques. Technical report, CWI (Centre for Mathematics and Computer Science), Amsterdam, The Netherlands, 1994.

[69] N. Viennot, S. Nair, and J. Nieh. Transparent Mutable Replay for Multicore Debugging and Patch Validation. In *Proceedings of ASPLOS*, 2013.

[70] WebPagetest. HTTP Archive - Interesting Stats. `https://goo.gl/9V4KJn`, 2016.

[71] Y. Wu, A. Haeberlen, W. Zhou, and B. T. Loo. Automated Bug Removal for Software-Defined Networks. In *Proceedings of NSDI*, 2017.

[72] Y. Wu, M. Zhao, A. Haeberlen, W. Zhou, and B. T. Loo. Diagnosing Missing Events in Distributed Systems with Negative Provenance. In *Proceedings of SIGCOMM*, 2014.

[73] Y. Zheng, T. Bao, and X. Zhang. Statically Locating Web Application Bugs Caused by Asynchronous Calls. In *Proceedings of the 20th International Conference on World Wide Web*, WWW. ACM, 2011.

[74] W. Zhou, Q. Fei, N. Arjun, A. Haeberlen, B. T. Loo, and M. Sherr. Secure Network Provenance. In *Proceedings of SOSP*, 2011.

[75] W. Zhou, M. Sherr, T. Tao, X. Li, B. T. Loo, and Y. Mao. Efficient Querying and Maintenance of Network Provenance at Internet-Scale. In *Proceedings of SIGMOD*, 2010.

A Appendix

A.1 Case Study: Mailpile

Mailpile [35] is an email client which uses a browser-based GUI. The GUI, shown in the top part of Figure 8, is a sophisticated piece of software that contains 121 HTML files, and 70 JavaScript files that span 15,329 lines of code. As shown in Figure 6, Mailpile is one of the most complicated sites in our test corpus.

Mailpile has a public bug database, so we decided to use Reverb to diagnose some unresolved bugs. For example, Bug #1771 is triggered when a user tries to archive the messages in an email thread. The thread should disappear from Mailpile's display of active, non-archived threads; instead, the GUI does not change, and Mailpile throws a JavaScript exception (`‘‘Uncaught TypeError: Cannot read property ‘split’ of undefined’’`). We recreated this bug, recording a session in which the user composes and sends two new emails, reads several preexisting emails, archives an email thread (generating an exception), and then composes a new email.

The exception was thrown by a loop inside of Mailpile's event handler for clicks on the "archive thread" button. The loop iterated through DOM nodes whose class name started with `.pile-message-`. For each such node, the loop tried to access the `.tids` property of each node. In particular, the failing line of code tried to perform `$(‘.pile-message-’ + i).data(‘tids’).split(/,/)`. Finding the source code location of this problematic line was easy with both Reverb and the browser's standard JavaScript debugger. However, using Reverb, we could quickly explore the temporal evolution of program state, try speculative bug fixes, and then observe how post-edit replays unfolded.

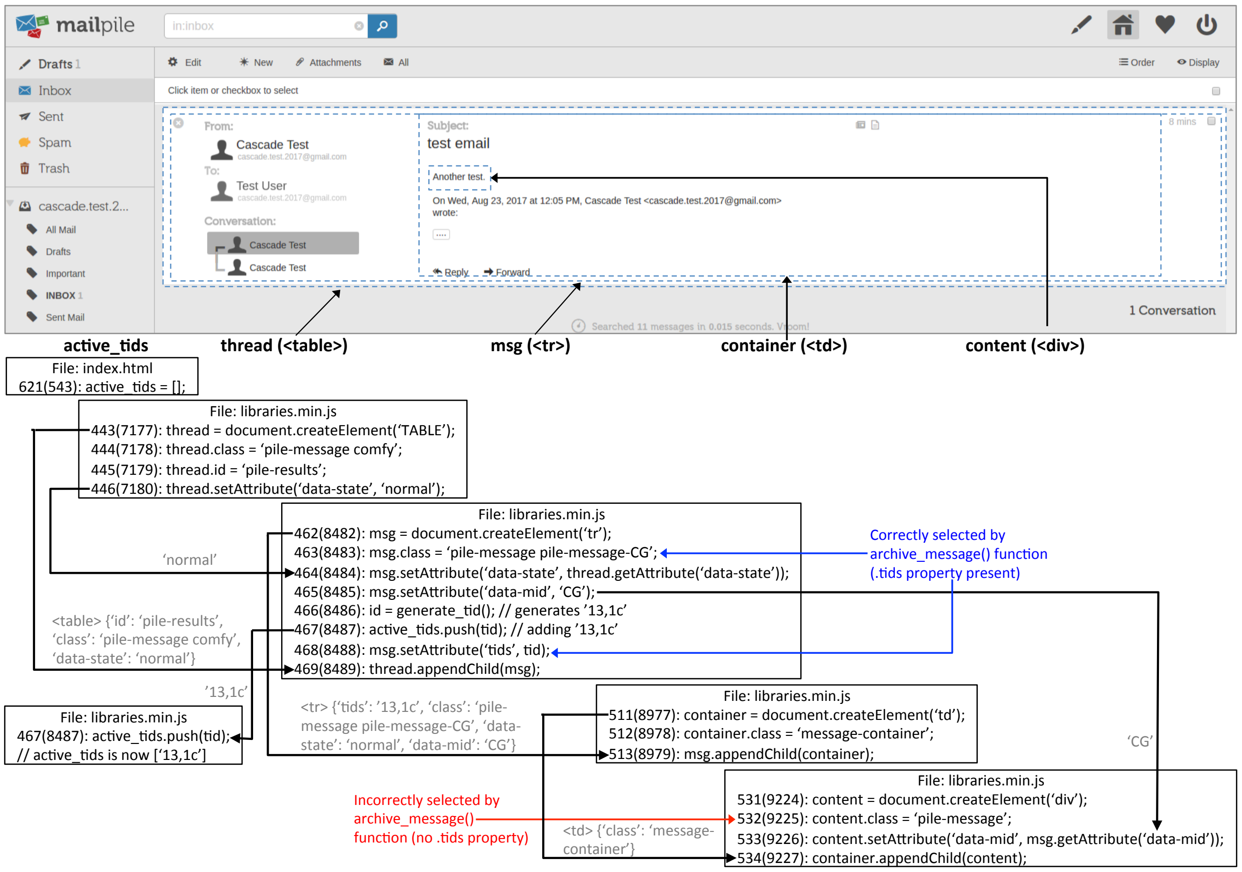
The first debugging task was to learn which DOM nodes *did* have `.tids` properties, and how those properties were assigned. To discover this information, we replayed the program to just before the exception, and searched backwards through the dynamic trace of the loop to find DOM nodes which did not trigger exceptions. For each of those nodes, we then traced backwards through the targeted dynamic trace for that node (§3.2); computing and rendering each targeted dynamic trace took 2 seconds on average. The bottom part of Figure 8 shows a simplified dynamic trace for the DOM node which triggered an exception (the content `<div>`) and a DOM node which did not trigger an exception (the message `<tr>`). The targeted traces quickly allowed us to determine that `.tids` properties were set by the Mailpile event handler for clicking upon the "send mail" button; each `.tids` value was a random string created by the `generate_tid()` function.

Having identified the proximate cause of the exception, our next task was to devise a bug fix. Hypothesizing that 1) *all* instances of the `.pile-message-*` class should have `.tids` properties, and 2) the failure to assign such a property was a bug, we edited the mail-sending event handler to forcibly assign `.tids` to every DOM node that was associated with the message-to-send. We performed this edit at the beginning of replay, before Reverb had dispatched any events. We then started the replay. The edit successfully removed the exception and allowed Mailpile to refresh the GUI. Replay proceeded, with the composition of the new email succeeding. However, throughout the post-edit replay, the GUI displayed improperly-large counts for the number of messages in each thread. Dynamic traces for state touched by the counting code revealed that every DOM node with a `.tids` property was counted as a message.

The failure of this fix suggested that the problem lay not in the mail-sending function, but in the thread-archiving function—perhaps the thread-archiving function had a mistaken belief (not shared by the rest of the code) that all instances of the `.pile-message-*` class should have `.tids` properties. We tried another, more trivial fix in which we injected a `try/catch` block around the exception-generating statement in the thread-archiving function, such that the `catch` block issued a `continue` statement which resumed the function's iteration through the messages in the thread. This fix resulted in Mailpile successfully clearing the GUI of the archived message. The GUI's message counts were correct, and replay continued past the (no-longer-thrown) exception to the composition of a new email.

By diffing the data flow graphs of the original execution and the speculative execution with the second fix, we verified that the second fix only led to state changes in archived messages—the rest of the application was unaffected. However, this observation did not prove that the fix was "correct" in a deep sense. Indeed, the fix was distressingly shallow; the exception-throwing line of code implied a mismatch between the expectations of the developer and the actuality of the program with respect to which DOM nodes had `.tids` fields. However, we had not identified the precise mismatch. To further analyze the problem, we examined the targeted dynamic traces for all of the DOM nodes which visually represented messages in the GUI. We saw that Mailpile represented each email thread as an HTML table, assigning each table element (i.e., each `<td>` and `<tr>` element) a class with a prefix of `.pile-message-`. However, the mail-sending function only assigned `.tids` properties to `<td>` elements, which represented the subject line in an email thread. The thread-archiving function was the only part of the dynamic trace which (mistakenly) assumed that *all* `.pile-message-*` DOM nodes would have a `.tids` property (hence the exception thrown when trying to access a method on a non-existent property).

Diagnosing this problem would certainly be possible with a traditional debugger. However, Reverb's speculative edits and targeted dynamic traces made it easy for us to explore a buggy execution and test hypotheses without deep,


mailpile
Drafts 1
Inbox
Sent
Spam
Trash
cascade.test.2...
All Mail
Drafts
Important
INBOX 1
Sent Mail
From:
Cascade Test
To:
Test User
Conversation:
Subject:
test email
Another test.
On Wed, Aug 23, 2017 at 12:05 PM, Cascade Test <cascade.test.2017@gmail.com> wrote:
Reply
Forward
1 Conversation
active_tids
thread (<table>)
msg (<tr>)
container (<td>)
content (<div>)
'normal'
<table> {'id': 'pile-results', 'class': 'pile-message comfy', 'data-state': 'normal'}
'13,1c'
<tr> {'tids': '13,1c', 'class': 'pile-message pile-message-CG', 'data-state': 'normal', 'data-mid': 'CG'}
'CG'
<td> {'class': 'message-container'}
Correctly selected by archive_message() function (.tids property present)
Incorrectly selected by archive_message() function (no .tids property)

```
File: index.html
621(543): active_tids = [];
```

```
File: libraries.min.js
443(7177): thread = document.createElement('TABLE');
444(7178): thread.class = 'pile-message comfy';
445(7179): thread.id = 'pile-results';
446(7180): thread.setAttribute('data-state', 'normal');
```

```
File: libraries.min.js
462(8482): msg = document.createElement('tr');
463(8483): msg.class = 'pile-message pile-message-CG';
464(8484): msg.setAttribute('data-state', thread.getAttribute('data-state'));
465(8485): msg.setAttribute('data-mid', 'CG');
466(8486): id = generate_tid(); // generates '13,1c'
467(8487): active_tids.push(tid); // adding '13,1c'
468(8488): msg.setAttribute('tids', tid);
469(8489): thread.appendChild(msg);
```

```
File: libraries.min.js
467(8487): active_tids.push(tid);
// active_tids is now ['13,1c']
```

```
File: libraries.min.js
511(8977): container = document.createElement('td');
512(8978): container.class = 'message-container';
513(8979): msg.appendChild(container);
```

```
File: libraries.min.js
531(9224): content = document.createElement('div');
532(9225): content.class = 'pile-message';
533(9226): content.setAttribute('data-mid', msg.getAttribute('data-mid'));
534(9227): container.appendChild(content);
```

Figure 8: A buggy Mailpile session. The bottom part of the diagram shows targeted dynamic traces for several DOM nodes. The i-th executed source code line is prefixed with `lineNumInSrcFile(`i`)`.

a priori knowledge of the code. At the time of this paper's writing, Bug #1771 had been unresolved for over eleven months. We have reported our findings to the Mailpile dev team, and we are awaiting their response.

A.2 Case Study: An `nba.com` page

The DOM interface is complex, and a rich source of bugs [59]. Reverb tracks data flows through both the JavaScript heap and the DOM, so Reverb can diagnose faults that involve buggy DOM interactions. For example, when one of the authors was browsing a page hosted by `nba.com`, the author noticed that the site threw an exception: `''TypeError: Cannot set property 'innerHTML' of null''`. The `.innerHTML` property is defined by DOM nodes; writing to the property dynamically overwrites a node's set of child HTML tags. For some reason, the `nba.com` page had a `null` reference that should have pointed to a DOM node.

Using Reverb, we were able to quickly determine the provenance of this erroneous value, *without possessing deep, a priori understanding of the code*. We determined that the error arose from confusion between the page's HTML and two JavaScript libraries that were written by different parties. The page's statically-defined HTML file contained a `<div>` tag with an `id` of "Popular Topics." An inline script (written by the developers at `nba.com`) used the `.getElementById()` and `.firstChild()` DOM methods to generate a reference to the "Popular Topics" tag. The script then added new DOM nodes to the tag, and changed the tag's `id` to be "Latest News." Later in the page's statically-declared HTML, there was an external script from a third party. The goal of this script was to add new headlines from third-party-affiliated sources. This external script used `.getElementById(''Popular Topics'')` to ostensibly assign a DOM node reference to a variable named `z`. The script then tried to invoke a method on `z`, unaware that the DOM call had returned `null` because the page no longer contained a tag with an `id` of "Popular Topics."

This gory example demonstrates the importance of threading data flows through the JavaScript heap and the DOM. Using Reverb's data flow analysis, we traced the provenance of the `null` value, and determined that the page expected to find a DOM node with an `id` of "Popular Topics." We then searched the full-program data flow graph for the creation of a DOM node with that id. Once that object was found, we rolled forward in the data flow graph and watched the evolution of the object, seeing it receive new children and then have its `id` reset to "Latest News." Diagnosing this kind of fault is extremely tedious with standard breakpoints or watchpoints—developers must repeatedly guess where to place breakpoints, or which state to watch, and then re-execute the program, hoping that the bug reoccurs, and that the new breakpoints or watchpoints were correctly positioned to catch the error.

A.3 Pruning Data Flow Graphs

As shown in Figure 8, Reverb's primary visualization depicts a dynamic execution trace. Each column expresses the source code lines that wrote or read a particular JavaScript variable or DOM node; arrows that are rooted in a particular source code line X indicate which temporally-subsequent source code lines read data that was written by X. For a single web page load, the visualization for a full dynamic trace is typically thousands of columns wide (because the distributed application has many variables) and tens of thousands of rows tall (because the distributed program executes many source code lines). Thus, pruning strategies are important for maintaining the readability of dynamic traces. Reverb exposes several pruning techniques to developers:

- The most important one is the ability for developers to specify which subset of variables should be analyzed by Reverb. Starting from zero variables, a developer iteratively adds new variables (or deletes old ones) as new diagnostic hypotheses are generated. This pruning approach underlies the notion of a targeted dynamic trace (§3.2,§A.1); as a side effect, this approach prunes the number of rows in the visualization, since most variables are only updated a few dozen times at most.
- Reverb also allows developers to vertically prune a graph, by specifying a particular time period for which Reverb should display data flows for the targeted variables. Such temporal bracketing prunes columns as a side effect, since Reverb will ignore variables that send or receive values to/from a target variable if those source/sink operations are outside the bracketed time window.
- A developer can prune by the origin of JavaScript code, such that Reverb only visualizes trace data for variables that were written by code from a particular hostname. This pruning strategy is useful for assigning blame if an application contains multiple server-side Node instances, and/or multiple client-side browsers which load JavaScript libraries from multiple origins.
- Reverb allows developers to selectively disable trace output for all JavaScript heap variables, or for all DOM state. This pruning technique is useful when a bug is hypothesized to involve only JavaScript state, or only DOM state. This technique is also useful when a bug involves both types of state, but, e.g., the developer already understands how the JavaScript state evolved during the logged execution, and desires to focus on how the DOM state changed.
- For a particular variable, a developer can enable or disable the visualization of control flow dependencies. The developers can also globally enable or disable these visualizations.
- Finally, Reverb supports the visual diffing of two traces. This is useful to understand divergences between a logged execution, and a speculatively-edited replay.

In our experience, these techniques make the comprehension of trace data tractable for a human developer.

A.4 Additional Related Work

In Section 2, we provided a broad overview of prior debugging work. Here, we briefly provide more specific comparisons between Reverb and AutoFlox and WebSlice, which are web-specific tools for program slicing. We also discuss Whyline, a replay debugger which provides limited support for automated data flow analysis.

AutoFlox [60] uses dynamic slicing of JavaScript code to debug null reference exceptions. AutoFlox assumes that the root cause is always a faulty invocation of a DOM interface that returns a null value; thus, AutoFlox diagnosis consists of traversing backwards in the slice until a null-returning DOM call is found. To simplify its analysis, AutoFlox assumes that the execution trace between the exception and the buggy DOM invocation has no recursive function calls or access to object properties. Reverb is much more general: it assumes nothing about code behavior in a dynamic slice, and can debug program faults besides null reference exceptions, across the client-server divide.

WebSlice [57] generates static slices that include source code lines on both the client and the server. Using symbolic execution, WebSlice generates the HTML output of server-side PHP code. That HTML, which contains both concrete and symbolic values, is then fed to a variability-aware parser [56]; the parser builds a multiverse DOM tree that contains all possible DOM trees, as well as the symbolic value constraints that would generate each tree. The multiverse DOM tree also contains multiverse JavaScript code and the associated symbolic constraints. Given a data object in PHP, WebSlice can provide a forward slice using the symbolic data constraints to trace paths along the static control flows. Such forward slices help developers to identify the potential impact of modifying PHP code. Reverb provides wide-area dynamic traces for only one language (JavaScript), but supports replay debugging, precise value provenance, and speculative edit-and-continue, none of which are provided by WebSlice.

To reduce the cognitive overhead on developers, the front-end for a replay debugger can use heuristics to propose explanations for incorrect program behavior. For example, Whyline [32] leverages Java's static typing and object-oriented nature to answer procedurally-generated questions like "Why is this Java object's `.id` field equal to 12?" However, Whyline relies on static analyses which are difficult or impossible to apply to the weakly-typed languages like JavaScript [1] that are often used to write web applications. Furthermore, for a particular program, Whyline's set of procedurally-generated questions is small compared to the total universe of questions that could be asked. Reverb records fine-grained data flows and control flows, and then allows developers to pose arbitrary queries on those flows.