Protecting JavaScript Source Code in Web Runtime

Roger Wang
Tizen Developer; node-webkit creator
Intel Open Source Technology Center
Agenda

- Problem statement
- Existing solutions
- Proposed solution
- Internals and considerations
Problem statement

- Application is written in JS
- JS programmers need a way to protect their code
Obfuscation / Minifying

YUI Compressor
Google Closure Compiler
UglifyJS
Bubble Sort in JS

```javascript
function bubbleSort(a)
{
    var swapped;
    do {
        swapped = false;
        for (var i=0; i < a.length-1; i++) {
            if (a[i] > a[i+1]) {
                var temp = a[i];
                a[i] = a[i+1];
                a[i+1] = temp;
                swapped = true;
            }
        }
    } while (swapped);
}
```

```javascript
window.bubbleSort=function(b){
    var c;
    do{
        c=!1;
        for(var a=0;a<b.length-1;a++)
            if (b[a]>b[a+1]&&
                (c=b[a],b[a]=b[a+1],b[a+1]=c,c=!0))
            }while(c);
};
```
function bubbleSort(a) {
    var swapped;
    do {
        swapped = false;
        for (var i=0; i < a.length-1; i++) {
            if (a[i] > a[i+1]) {
                var temp = a[i];
                a[i] = a[i+1];
                a[i+1] = temp;
                swapped = true;
            }
        }
    } while (swapped);
}

window.bubbleSort = function(b) {
    var c;
    do {
        c = !1;
        for(var a = 0;a < b.length - 1;a++) {
            b[a] > b[a + 1] && (c = b[a],
            b[a] = b[a + 1],
            b[a + 1] = c,
            c = !0)
        }
    } while(c)
};
On-disk encryption
On-disk Encryption

- Increase the time to hack
- Weakness
  - Encrypting on installation
    - HTTP(s) MITM w/ private certificate
  - Function.toString()
  - Hook on JS engine calls
  - Memory dumping
Other Solutions

Put logic on server
Compile to JS
License & Lawyer
Compile JS to Machine Code
Compiling and Distribution

- Development phase
  - Compiler
  - Minimal changes to application manifest and `<script>` tag
- Distribution with the binary only
  - Application store
- Leveraging the difference between Web Runtime & Browser
- Experimental feature in node-webkit
Details of Implementation

- **Heap dumping**
  - Objects
  - Functions (JITed)
- **V8 Snapshot**
  - Size
  - Performance: full-codegen & crankshaft
- **JSC API shim layer**
- **Plan on JSC**
JSC API Shim Layer

- JSC public API wrapper on v8
- Derivative work based on qtwebkit-v8
- Switch to v8 DOM binding in WebKit
- Components accessing JSC public API
  - Injected Bundle
  - Plugin
Solutions

- Obfuscation / Minifying
  - YUI Compressor
  - Google Closure Compiler
  - UglifyJS
- On-disk encryption
- Less JavaScript
  - Put logic on server
  - Compile to JS
- License & Lawyer