Strider HoneyMonkeys: Active Client-Side Honeypots for Finding Web Sites That Exploit Browser Vulnerabilities

Yi-Min Wang

Group Manager & Senior Researcher

Cybersecurity & Systems Management Research Group

Microsoft Research, Redmond

Joint work with Doug Beck, Xuxian Jiang, Roussi Roussev, Chad Verbowski, Shuo Chen, and Sam King

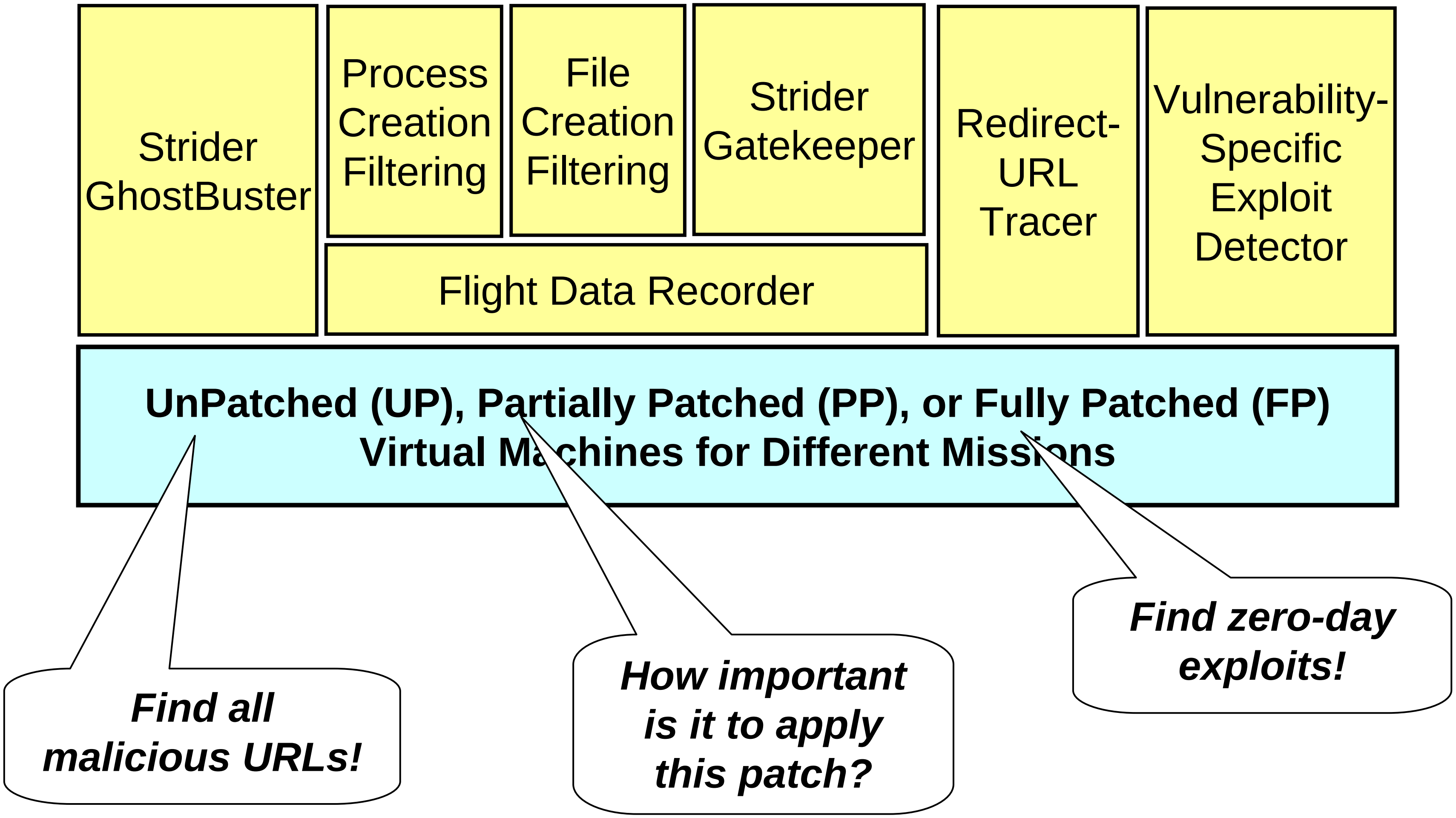
Problem Space

- You use a browser to visit a URL
  - Multiple URLs are visited behind the scene
  - Exploit page may go through multiple stages of code obfuscation
  - Exploit page(s) may attempt exploits on multiple vulnerabilities
  - Multiple malware programs may get installed

Strider HoneyMonkeys

- HoneyMonkey
  - Monkey programs that drive browser software to visit URLs just like humans
  - Act as active, client-side honeypots to attract malicious Web sites to exploit browser-based vulnerabilities
  - Use VMs with different patch levels
- Black-box Exploit Detection
  - Detecting software installation following a successful vulnerability exploit

HoneyMonkeys with Different Missions



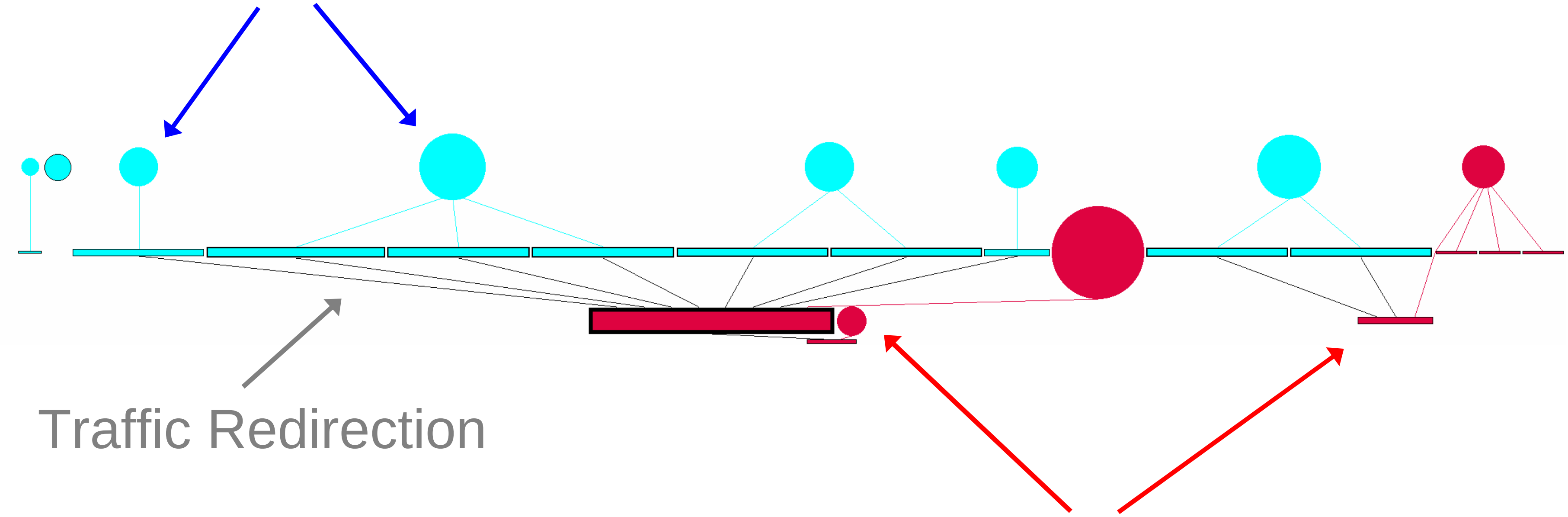
Strider GhostBuster
Process Creation Filtering
File Creation Filtering
Strider Gatekeeper
Flight Data Recorder
Redirect-URL Tracer
Vulnerability-Specific Exploit Detector
UnPatched (UP), Partially Patched (PP), or Fully Patched (FP) Virtual Machines for Different Missions
Find all malicious URLs!
How important is it to apply this patch?
Find zero-day exploits!

Finding Exploit URLs in the “Bad Neighborhoods”

- Windows “hosts” files, known spyware sites, etc.
- Crawling of exploit pages with lots of links
- Capture all redirect-URLs

	# Exploit URLs	# Exploit Sites
Total	**752**	**287**
WinXP SP1-UP	688	270
WinXP SP2-UP	204	115
WinXP SP2-PP	17	10
WinXP SP2-FP	0	0

SP2-PP: 17 URLs from 10 sites

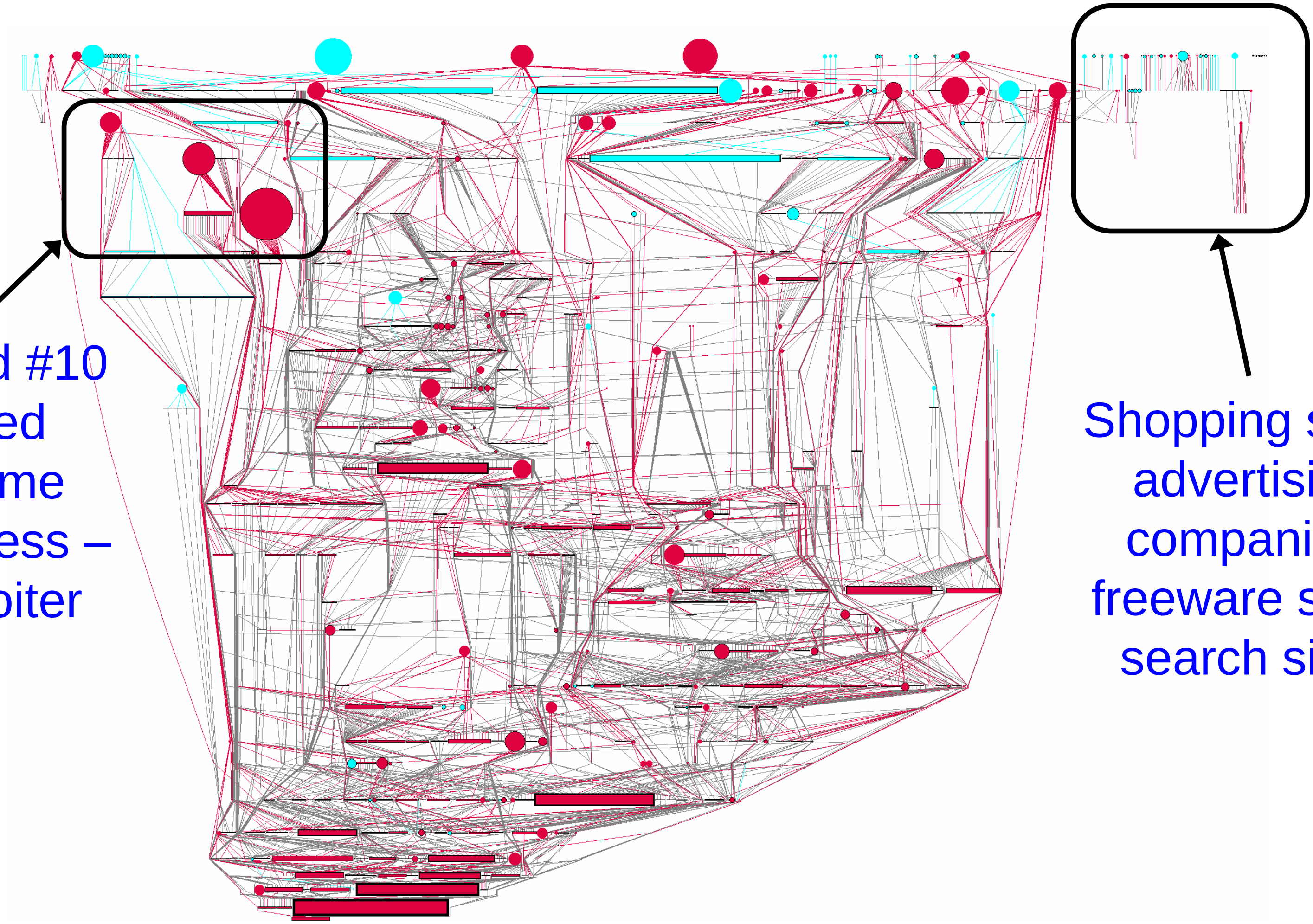


Content Providers: Attract browser traffic and sell/redirect them

Traffic Redirection

Exploit Providers:
Perform vulnerability exploits and install spyware

SP1-UP: 688 URLs from 270 sites

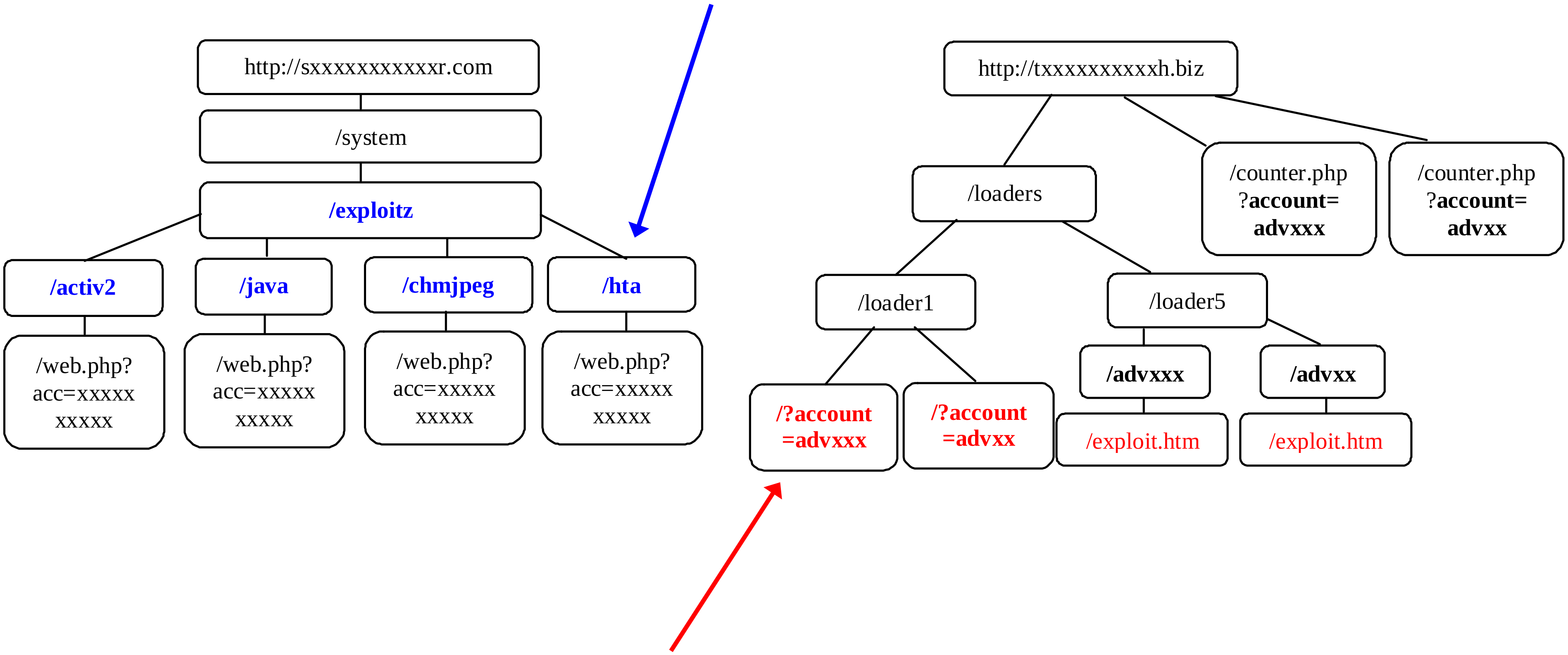


#1, #3, and #10 registered to the same email address – Top Exploiter

Shopping sites, advertising companies, freeware sites, search sites

How Exploit Sites Organize Their Pages

Vulnerability names



http://sxxxxxxxxxxxr.com

/system

/exploitz

/activ2

/java

/chmjpeg

/hta

/web.php?
acc=xxxxx
xxxxx

/web.php?
acc=xxxxx
xxxxx

/web.php?
acc=xxxxx
xxxxx

/web.php?
acc=xxxxx
xxxxx

http://txxxxxxxxxxh.biz

/loaders

/counter.php
?**account=**
advxxx

/counter.php
?**account=**
advxx

/loader1

/loader5

/?account
=advxxx

/?account
=advxx

/advxxx

/advxx

/exploit.htm

/exploit.htm

Account numbers

Are There Exploit URLs in the "Good Neighborhoods"?

- Top one million click-through links from a search engine
- Preliminary results
  - Contaminated Web pages that unknowingly serve exploiting ads may be a serious concern

Zero-Day Exploit Detection

- In early July 2005, HoneyMonkey discovered its first zero-day exploit of the javaprxy.dll vulnerability
  - Detected within 2.5 hours of scanning
  - Confirmed to be the first in-the-wild exploit URL reported to MSRC
- Over 40 of the monitored 752 URLs upgraded within 2 weeks, all redirected traffic to 3 exploit providers
  - As predicted, the top exploiter and SP2-PP exploiters upgraded

For More Information

- See MSR Technical Report at

http://research.microsoft.com/HoneyMonkey