Our Observation

The “data rate” obtained through probing is very low. Attackers thus need a large amount of repeated operations to extract useful information.

- History sniffing: Repeatedly enumerating links and checking link color
- Cache sniffing: Repeatedly accessing web resources
- Internal network probing: Repeatedly requesting resources from local network

Indirect Probing of Sensitive Information

- Different origins share the same browser environment
- Sensitive information can be inferred from indirect probing

Protection Mechanisms in Browsers

- Same Origin Policy (SOP).
- Origin is defined by (protocol, host, port)
- SOP prevents one origin from accessing resources in other origins.
- Sandbox confines accesses to browser resources

Browser Environment States

- History sniffing
- Cache sniffing
- Internal network probing

Approach Overview

Monitoring untrusted web sites in an instrumented Chromium browser.

- Extracting browser behaviors
  - Security relevant events
  - Descriptive information
- Analysing behavior descriptions
  - Statistics from multiple dimensions
  - Identifying abnormal and unreasonable behaviors

Browser Events

- JavaScript: The driving force in browsers
- Focusing on JavaScript interactions with the rest of browser components
  - DOM, Network, Environment states

Analyzing Behaviors

- Simple statistical analysis on behavior descriptions
  - Number of the repetitive API calls
  - Identifying features distinguishing normal websites from probing ones
  - Challenges: difficulty in benign sites involving large amounts repetitive behaviors
- Multiple dimension analysis on behavior descriptions
  - Analyzing behavior descriptions in different dimensions, e.g., time, involved element, API properties, etc.
  - Establishing heat map representation on different dimensions to detect probing behaviors

Conclusion

- Indirect probing extracts sensitive information in browser environment, with a low “data rate.”
- Detecting browser-based probing behaviors via multiple dimension analysis of browser events.