Comparison of Proposed Alerting and Data Collection Techniques

Casey Deccio

Purpose

- to explain and compare
    - Passive Collision Assessment (PCA)
    - Active Collision Assessment (ACA)
    - Controlled Interruption (CI)

What is being compared?

- Alerting effectiveness
  - *What population of potentially affected users, systems, and applications are expected to be reached by the alerting mechanism?*
- Operational continuity, security, and privacy
  - *How might users or systems be negatively impacted by interruption to service or subjected to exploit or privacy violations?*
- User experience
  - *What is the experience of the end user, in terms of application behavior, path to resolution, etc?*
- Root cause identification
  - *How useful is the technique in leading users towards the root cause and a possible resolution?*
- Public reception
  - *In what ways might the techniques be received in the public, with ICANN and others being accountable for complaints and fallout associated with design and execution of the mechanism?*
- Telemetry
  - *How much data is available to investigative parties, and what type of effort will it take to collect and analyze it?*

Alerting Effectiveness and Coverage

	CI	ACA	PCA
DNS Resolution of Queried Names	Dependent on DNS configuration and system mobility	Dependent on DNS configuration and system mobility	No resolution
Application Coverage	All applications	All applications	No applications
IPv4/IPv6 Availability	IPv4 only	IPv4 and IPv6	Not applicable

User Experience

	CI	ACA	PCA
Error Response - Application Experience	Quick-Response Error	Dependent on Network Configuration and Port	No Error
Error Response - User Experience	Application Dependent	Application Dependent	No Error
User Experience - HTTP / HTTPS Browsers	Not applicable	HTTP: unexpected content received HTTPS: TLS certificate errors anticipated	Not applicable
User Experience - Other Clients and Protocols	Not applicable	Non-browser HTTP: unexpected content received, unknown errors Applications that use TLS: TLS certificate errors SSH: man-in-the-middle attack errors	Not applicable
User Experience - Local Firewall Alerts	Rare but possible	Not applicable	Not applicable

Operational Continuity; RCI; Public Reception; Telemetry

	CI	ACA	PCA
Operational Continuity, Security, and Privacy	DNS Query Surveillance: all qnames Communication Interruption: all Application Inference: none Communication Interception: none Data Exfiltration: none	DNS Query Surveillance: all qnames Communication Interruption: all Application Inference: all Communication Interception: select Data Exfiltration: select	DNS Query Surveillance: some qnames Communication Interruption: none Application Inference: none Communication Interception: none Data Exfiltration: none
Root Cause Identification	Low - hint often not observed or not understood	Low - name collisions in Web browser few	Not applicable
Public Reception	95% Neutral, based on actual deployment experience	Unknown; Possibly negative, based on experience with Site Finder	No reactions anticipated
Telemetry	DNS queries: all qnames IPv4/IPv6: none Application none	DNS queries: all qnames IPv4/IPv6: both Application: destination ports and application-layer data	DNS queries: some qnames IPv4/IPv6: none Application none

Further work

- If/how to add RIPE Atlas Probes, Ad Measurement?

- Several of the comparisons led to updates to the Root Cause Analysis report
  - updated sections 3.4 and 5.3;
  - updated references across the document;
  - added any references to section 5 in the rest of the document, including in the "Discussion" section (section 10); and
  - added an appendix with the data from the Web search results.