CLAIMS

1. A computer implemented method for detecting bypass of an authentication system of a web application, the method being executed by one or more processors and comprising:

receiving one or more webpage logs comprising web traffic associated with a web application during a defined time period;

receiving one or more authentication logs associated with one or more authentication appliances providing authentication services for the web application, the one or more authentication logs comprising one or more time-stamped authentication factor entries for the one or more authentication appliances;

determining, based on the one or more webpage logs, one or more webpage log entries corresponding to a user and the defined time period;

determining, based on the one or more authentication logs, a total number of correct authentication factors provided by the user during the defined time period; and

determining, based on the one or more webpage log entries corresponding to the user and the defined time period and the total number of correct authentication factors provided by the user, that the user bypassed an authentication system of the web application, wherein determining that the user bypassed the authentication system of the web application comprises:

determining an expected number of authentication factors for the user for the defined time period based on a number of authentication factors ~~i)~~ required for the user to access each of one or more uniform resource locators (URLs) associated with the web application and accessed by the user during the defined time period, wherein the number of authentication factors required for the user to access each of the one or more URLs associated with the web application is ~~and ii) that are~~ controllable by the user; and

determining that the total number of correct authentication factors provided by the user during the defined time period is less than the expected number of authentication factors for the user for the defined time period.

2. The method of claim 1, wherein each authentication log entry corresponding to the user indicates a correct authentication factor provided by the user.

3. The method of claim 1, wherein determining the expected number of authentication factors for the user for the defined time period comprises:

determining, based on the one or more webpage log entries corresponding to the user and the defined time period, the one or more URLs associated with the web application and accessed by the user during the defined time period;

obtaining one or more tables, each of the one or more tables comprising a mapping between each of the one or more URLs and the number of authentication factors required for the user to access to each of the one or more URLs; and

determining, based on the one or more URLs and the one or more tables, the expected number of authentication factors for the user for the defined time period.

4. The method of claim 3, wherein a type of authentication factors required for the user to access to each of the one or more URLs are controllable by the user.

5. The method of claim 1, further comprising:

generating a score for the user based on the user’s conformance with one or more categories of web browsing behavior.

6. The method of claim 5, wherein the one or more categories of web browsing behavior comprise at least one of multiple bypasses, anomalous URLs, previous flagging of the user, blacklisted Internet protocol address, foreign Internet protocol address, and failure to provide any valid authentication information.

7. The method of claim 5, wherein conformance with at least one of the one or more categories of web browsing behavior indicates an intentional bypass of the authentication system of the web application.

8. A non-transitory computer-readable storage medium coupled to one or more processors and having instructions stored thereon which, when executed by the one or more processors, cause the one or more processors to perform operations for detecting bypass of an authentication system of a web application, the operations comprising:

receiving one or more webpage logs comprising web traffic associated with a web application during a defined time period;

receiving one or more authentication logs associated with one or more authentication appliances providing authentication services for the web application, the one or more authentication logs comprising one or more time-stamped authentication factor entries for the one or more authentication appliances;

determining, based on the one or more webpage logs, one or more webpage log entries corresponding to a user and the defined time period;

determining, based on the one or more authentication logs, a total number of correct authentication factors provided by the user during the defined time period; and

determining, based on the one or more webpage log entries corresponding to the user and the defined time period and the total number of correct authentication factors provided by the user, that the user bypassed an authentication system of the web application, wherein determining that the user bypassed the authentication system of the web application comprises:

determining an expected number of authentication factors for the user for the defined time period based on a number of authentication factors ~~i)~~ required for the user to access each of one or more uniform resource locators (URLs) associated with the web application and accessed by the user during the defined time period, wherein the number of authentication factors required for the user to access each of the one or more URLs associated with the web application is ~~and ii) that are~~ controllable by the user; and

determining that the total number of correct authentication factors provided by the user during the defined time period is less than the expected number of authentication factors for the user for the defined time period.

9. The non-transitory computer-readable storage medium of claim 8, wherein each authentication log entry corresponding to the user indicates a correct authentication factor provided by the user.

10. The non-transitory computer-readable storage medium of claim 8, wherein determining the expected number of authentication factors for the user for the defined time period comprises:

determining, based on the one or more webpage log entries corresponding to the user and the defined time period, the one or more URLs associated with the web application and accessed by the user during the defined time period;

obtaining one or more tables, each of the one or more tables comprising a mapping between each of the one or more URLs and the number of authentication factors required for the user to access to each of the one or more URLs; and

determining, based on the one or more URLs and the one or more tables, the expected number of authentication factors for the user for the defined time period.

11. The non-transitory computer-readable storage medium of claim 10, wherein a type of authentication factors required for the user to access to each of the one or more URLs are controllable by the user.

12. The non-transitory computer-readable storage medium of claim 8, further comprising:

generating a score for the user based on the user’s conformance with one or more categories of web browsing behavior.

13. The non-transitory computer-readable storage medium of claim 12, wherein the one or more categories of web browsing behavior comprise at least one of multiple bypasses, anomalous URLs, previous flagging of the user, blacklisted Internet protocol address, foreign Internet protocol address, and failure to provide any valid authentication information.

14. The non-transitory computer-readable storage medium of claim 12, wherein conformance with at least one of the one or more categories of web browsing behavior indicates an intentional bypass of the authentication system of the web application.

15. A system, comprising:

one or more processors; and

a computer-readable storage device coupled to the one or more processors and having instructions stored thereon which, when executed by the one or more processors, cause the one or more processors to perform operations for detecting bypass of an authentication system of a web application, the operations comprising:

receiving one or more webpage logs comprising web traffic associated with a web application during a defined time period;

receiving one or more authentication logs associated with one or more authentication appliances providing authentication services for the web application, the one or more authentication logs comprising one or more time-stamped authentication factor entries for the one or more authentication appliances;

determining, based on the one or more webpage logs, one or more webpage log entries corresponding to a user and the defined time period;

determining, based on the one or more authentication logs, a total number of correct authentication factors provided by the user during the defined time period; and

determining, based on the one or more webpage log entries corresponding to the user and the defined time period and the total number of correct authentication factors provided by the user, that the user bypassed an authentication system of the web application, wherein determining that the user bypassed the authentication system of the web application comprises:

determining an expected number of authentication factors for the user for the defined time period based on a number of authentication factors ~~i)~~ required for the user to access each of one or more uniform resource locators (URLs) associated with the web application and accessed by the user during the defined time period, wherein the number of authentication factors required for the user to access each of the one or more URLs associated with the web application is ~~and ii) that are~~ controllable by the user; and

determining that the total number of correct authentication factors provided by the user during the defined time period is less than the expected number of authentication factors for the user for the defined time period.

16. The system of claim 15, wherein each authentication log entry corresponding to the user indicates a correct authentication factor provided by the user.

17. The system of claim 15, wherein determining the expected number of authentication factors for the user for the defined time period comprises:

determining, based on the one or more webpage log entries corresponding to the user and the defined time period, one or more URLs associated with the web application and accessed by the user during the defined time period;

obtaining one or more tables, each of the one or more tables comprising a mapping between each of the one or more URLs and the number of authentication factors required for the user to access to each of the one or more URLs; and

determining, based on the one or more URLs and the one or more tables, the expected number of authentication factors for the user for the defined time period.

18. The system of claim 17, wherein a type of authentication factors required for the user to access to each of the one or more URLs are controllable by the user.

19. The system of claim 15, further comprising:

generating a score for the user based on the user’s conformance with one or more categories of web browsing behavior.

20. The system of claim 19, wherein the one or more categories of web browsing behavior comprise at least one of multiple bypasses, anomalous URLs, previous flagging of the user, blacklisted Internet protocol address, foreign Internet protocol address, and failure to provide any valid authentication information.