

WHAT IS CLAIMED IS:

1. In a network security system implemented in a computer or electronic device, coupled to secured online resources for detecting unauthorized accesses of those secured online resources, a method comprising:
 - monitoring a user activity session; and
 - determining if the user activity session is indicative of a hidden session by an attacker, wherein determining includes comparing the user activity session to an average user activity session.
2. The method of claim 1 further comprising collecting average parameter values during a data collection period.
3. The method of claim 2 wherein the average parameter values include an average time between clicks for an average session, wherein determining includes comparing user time between clicks for the user activity session to the average time between clicks for the average session.
4. The method of claim 2 wherein the average parameter values include a website page view order in an average session, wherein determining includes comparing website page view order for the user activity session with the website page view order in the average session.
5. The method of claim 2 wherein the average parameter values include an average time between clicks for a specified page, wherein determining includes comparing the time between clicks for the specified page during the user activity session to the average time between clicks for the specified page.
6. The method of claim 1 further comprising synchronizing transaction records.
7. The method of claim 6 wherein synchronizing transaction records includes correcting for errant clock settings among all active clients using a website during a data collection period.
8. The method of claim 6 wherein synchronizing transaction records includes adjusting for transmission time between clients and servers.

9. The method of claim 6 wherein synchronizing transaction records includes adjusting for client service load time.
10. The method of claim 6 wherein synchronizing transaction records includes estimating service timing characteristics for each service provided by a website during a data collection period.
11. The method of claim 10 wherein synchronizing transaction records includes estimating server delay statistics for each service provided by a server during the data collection period.
12. The method of claim 10 wherein synchronizing transaction records includes measuring and modeling echo delay statistics.
13. The method of claim 6 wherein synchronizing transaction records includes forming a server timing model with an affine function of service duration.
14. The method of claim 13 wherein the server timing model includes a multiplicative rate parameter selected from receive rate, send rate and sent rate.
15. The method of claim 13 wherein the server timing model includes an additive bias parameter selected from a receive bias, send bias and sent bias.
16. The method of claim 1 wherein determining includes comparing a session event to an event model to produce an anomaly score.

CLAIMS

1. In a network security system implemented in a computer or electronic device, coupled to secured online resources for detecting unauthorized accesses of those secured online resources, a method comprising:
 - monitoring a user activity session; and
 - determining if the user activity session is indicative of a hidden session by an attacker, wherein determining includes comparing the user activity session to an average user activity session;
 - wherein the method further comprises collecting average parameter values during a data collection period;
 - wherein the average parameter values include an average time between clicks for an average session, wherein determining includes comparing user time between clicks for the user activity session to the average time between clicks for the average session; and
 - wherein the average parameter values further include a website page view order in the average session, wherein determining further includes comparing website page view order for the user activity session with the website page view order in the average session.
2. A method as in claim 1, wherein the average parameter values include an average time between clicks for a specified page, wherein determining includes comparing the time between clicks for the specified page during the user activity session to the average time between clicks for the specified page.
3. The method of claim 2 further comprising synchronizing transaction records.
4. The method of claim 3 wherein synchronizing transaction records includes correcting for errant clock settings among all active clients using a website during a data collection period.
5. The method of claim 3 wherein synchronizing transaction records includes adjusting for transmission time between clients and servers.
6. The method of claim 3 wherein synchronizing transaction records includes adjusting for client service load time.

7. The method of claim 3 wherein synchronizing transaction records includes estimating service timing characteristics for each service provided by a website during a data collection period.
8. The method of claim 7 wherein synchronizing transaction records includes estimating server delay statistics for each service provided by a server during the data collection period.
9. The method of claim 7 wherein synchronizing transaction records includes measuring and modeling echo delay statistics.
10. The method of claim 3 wherein synchronizing transaction records includes forming a server timing model with an affine function of service duration.
11. The method of claim 10 wherein the server timing model includes a multiplicative rate parameter selected from receive rate, send rate and sent rate.
12. The method of claim 10 wherein the server timing model includes an additive bias parameter selected from a receive bias, send bias and sent bias.
13. An electronic apparatus, coupled to secured online resources, constructed and arranged to detect unauthorized accesses of those secured online resources, the apparatus comprising:
 - a network interface;
 - memory; and
 - a controller including controlling circuitry coupled to the memory, the controlling circuitry being constructed and arranged to:
 - monitor a user activity session; and
 - determine if the user activity session is indicative of a hidden session by an attacker, wherein determining includes comparing the user activity session to an average user activity session;
 - wherein the method further comprises collecting average parameter values during a data collection period;
 - wherein the average parameter values include an average time between clicks for an average session, wherein determining includes comparing user time between

clicks for the user activity session to the average time between clicks for the average session; and

wherein the average parameter values further include a website page view order in the average session, wherein determining further includes comparing website page view order for the user activity session with the website page view order in the average session.

14. A computer program product having a non-transitory, computer-readable storage medium which stores instructions which, when executed by a computer coupled to secured online resources, cause the computer to perform a method of detecting unauthorized accesses of those secured online resources, the method comprising:

monitoring a user activity session; and

determining if the user activity session is indicative of a hidden session by an attacker, wherein determining includes comparing the user activity session to an average user activity session;

wherein the method further comprises collecting average parameter values during a data collection period;

wherein the average parameter values include an average time between clicks for an average session, wherein determining includes comparing user time between clicks for the user activity session to the average time between clicks for the average session; and

wherein the average parameter values further include a website page view order in the average session, wherein determining further includes comparing website page view order for the user activity session with the website page view order in the average session.