

CLAIMS

1. A client system comprising at least one hardware processor configured to execute a target entity, a reputation manager, and an anti-malware engine, wherein:

the reputation manager is configured to:

in response to receiving a first reputation indicator of the target entity from a reputation server, the first reputation indicator indicative of a probability that the target entity is malicious, transmit the reputation indicator to the anti-malware engine,

in response to receiving the first reputation indicator, update the first reputation indicator by determining a second reputation indicator of the target entity, the second reputation indicator differing from the first reputation indicator by a reputation change, and

in response to determining the second reputation indicator, transmit the second reputation indicator to the anti-malware engine and to the reputation server,

wherein determining the second reputation indicator comprises:

in response to receiving the first reputation indicator, determining a first time interval,

in response to determining the first time interval, determining whether the target entity has performed any of a set of pre-determined actions during the first time interval,

in response, if the target entity has not performed any of the set of pre-determined actions during the first time interval, determining the reputation change to indicate a reduction in the probability that the target entity is malicious, and

if the target entity has performed a first action of the set of pre-determined actions during the first time interval, determining the reputation change to indicate an increase in the probability that the target entity is malicious; and wherein

the anti-malware engine is configured to:

in response to receiving the first reputation indicator, employ a first protocol to determine whether the target entity is malicious, and

in response to receiving the second reputation indicator, employ a second protocol to determine whether the target entity is malicious, wherein the second protocol is less computationally expensive than the first protocol when the second reputation indicator indicates a decreased probability of malice compared to the first reputation indicator, and wherein the second protocol is more computationally expensive than the first protocol when the second reputation indicator indicates an increased probability of malice compared to the first reputation indicator.

2. The client system of claim 1, wherein the reputation manager is further configured,

in response to determining the second reputation indicator, to update the second reputation indicator by determining a third reputation indicator of the target entity, the third reputation indicator differing from the second reputation indicator by another reputation change, wherein determining the third reputation indicator comprises:

determining a second time interval subsequent to the first time interval;

in response to determining the second time interval, determining whether the target entity has performed any of the set of pre-determined actions during the second time interval;

in response, if the target entity has not performed any of the set of pre-determined actions during the second time interval, determining the another reputation change to indicate another reduction in the probability that the target entity is malicious; and

if the target entity has performed a second action of the set of predetermined actions, determining the another reputation change to indicate another increase in the probability that the target entity is malicious.
3. The client system of claim 2, wherein a size of the second time interval is determined according to a size of the first time interval.
4. The client system of claim 2, wherein the another reputation change is determined according to a size of the first time interval.
5. The client system of claim 1, wherein the reputation manager is further configured to determine the reputation change according to a time elapsed since a launch of the target entity on the client system.
6. The client system of claim 1, wherein the first time interval is determined according to a time elapsed since a launch of the target entity on the client system.
7. The client system of claim 1, wherein the first time interval is determined according to the first reputation indicator.
8. The client system of claim 1, wherein the first time interval is determined according to whether the target entity has performed a second action of the set of pre-determined actions prior to the first time interval.
9. The client system of claim 1, wherein the reputation change is determined according to a type of the first action.
10. The client system of claim 1, wherein the reputation change is determined according to whether the target entity has performed a second action prior to the first action.
11. The client system of claim 1, wherein the reputation manager is further configured to,

in response to determining the second reputation indicator, to update another reputation indicator of another entity executing on the client system, the another entity comprising a component of the target entity, the another reputation indicator indicative of a probability that the another entity is malicious.

12. The client system of claim 1, wherein the first action comprises the target entity injecting a section of code into another entity executing on the client system, and wherein the reputation manager is further configured, in response to determining the third reputation indicator, to determine another reputation indicator of the another entity executing on the client system, the another reputation indicator indicating that the another entity is as likely to be malicious as the target entity.

13. A server computer system comprising at least one hardware processor configured to perform reputation management transactions with a plurality of client systems, wherein a reputation management transaction comprises:

in response to a request received from a client system of the plurality of client systems, the client system executing a target entity, retrieving a first reputation indicator of a target entity from an entity reputation database, the first reputation indicator indicative of a probability that the target entity is malicious;

in response to retrieving the first reputation indicator, transmitting the first reputation indicator to the client system;

in response to transmitting the first reputation indicator, receiving a second reputation indicator of the target entity from the client system;

in response to receiving the second reputation indicator, comparing the first and second reputation indicators;

in response, when the second reputation indicator indicates a lower probability that the target entity is malicious than indicated by the first reputation indicator, adding the second reputation indicator to a collection of reputation indicators received from the plurality of client systems, wherein all members of the collection are determined for instances of the target entity;

in response to adding the second reputation indicator to the collection, determining whether a reputation update condition is satisfied; and

in response, when the update condition is satisfied, replacing the first reputation indicator in the reputation database with an updated reputation indicator determined according to the collection;

wherein the second reputation indicator differs from the first reputation indicator by a reputation change, and wherein determining the second reputation indicator comprises employing the client system to:

in response to receiving the first reputation indicator, determine a first time interval,

in response to determining the first time interval, determine whether the target entity has performed any of a set of pre-determined actions during the first time interval,

in response, if the target entity has not performed any of the set of pre-determined actions during the first time interval, determine the reputation change to indicate a reduction in the probability that the target entity is malicious, and

if the target entity has performed a first action of the set of pre-determined actions, determine the reputation change to indicate an increase in the probability that the target entity is malicious.

14. The server computer system of claim 13, wherein determining whether the update condition is satisfied comprises determining a time elapsed since adding the first member to the collection.
15. The server computer system of claim 13, wherein determining whether the update condition is satisfied comprises determining a count of the members of the collection.
16. The server computer system of claim 13, wherein determining the updated reputation indicator comprises formulating the updated reputation indicator to indicate a highest probability that the target entity is malicious of all members of the collection.
17. The server computer system of claim 13, further configured, in response to receiving the second reputation indicator, to receive from the client system a third reputation indicator determined for the target entity, the third reputation indicator differing from the second reputation indicator by another reputation change, and wherein determining the third reputation indicator by the client system comprises:

determining a second time interval subsequent to the first time interval;

in response to determining the second time interval, determining whether the target entity has performed any of the set of pre-determined actions during the second time interval;

in response, if the target entity has not performed any of the set of pre-determined actions during the second time interval, determining the another reputation change to indicate another reduction in the probability that the target entity is malicious; and

if the target entity has performed a second action of the set of predetermined actions, determining the another reputation change to indicate another increase in the probability that the target entity is malicious.

18. The server computer system of claim 13, wherein the reputation change is determined according to a time elapsed since a launch of the target entity on the client system.

19. The server computer system of claim 13, wherein the first time interval is determined according to a time elapsed since a launch of the target entity on the client system.
20. The server computer system of claim 13, wherein the first time interval is determined according to the first reputation indicator.
21. The server computer system of claim 13, wherein the first time interval is determined according to whether the target entity has performed a second action of the set of pre-determined actions prior to the first time interval.
22. A non-transitory computer-readable medium storing a set of instructions which, when executed by a hardware processor of a client system, cause the client system to form a reputation manager and an anti-malware engine, wherein:

the client system is configured to execute a target entity;

the reputation manager is configured to:

in response to receiving a first reputation indicator of the target entity from a reputation server, the first reputation indicator indicative of a probability that the target entity is malicious, transmit the reputation indicator to the anti-malware engine,

in response to receiving the first reputation indicator, update the first reputation indicator by determining a second reputation indicator of the target entity, the second reputation indicator differing from the first reputation indicator by a reputation change, and

in response to determining the second reputation indicator, transmit the second reputation indicator to the anti-malware engine and to the reputation server,

wherein determining the second reputation indicator comprises:

in response to receiving the first reputation indicator, determining a first time interval,

in response to determining the first time interval, determining whether the target entity has performed any of a set of pre-determined actions during the first time interval,

in response, if the target entity has not performed any of the set of pre-determined actions during the first time interval, determine the reputation change to indicate a reduction in the probability that the target entity is malicious, and

if the target entity has performed a first action of the set of pre-determined actions during the first time interval, determining the reputation change to indicate an increase in the probability that the target entity is malicious; and wherein

the anti-malware engine is configured to:

in response to receiving the first reputation indicator, employ a first protocol to determine whether the target entity is malicious, and

in response to receiving the second reputation indicator, employ a second protocol to determine whether the target entity is malicious, wherein the second protocol is less computationally expensive than the first protocol when the second reputation indicator indicates a decreased probability of malice compared to the first reputation indicator, and wherein the second protocol is more computationally expensive than the first protocol when the second reputation indicator indicates an increased probability of malice compared to the first reputation indicator.