## CLAIMS

What is claimed is:

1. A method for starting an application on a target platform, wherein the target platform comprises at least a verifiable startup chip and a trusted execution environment, and the method comprises:

sequentially starting a plurality of system startup items based on a predetermined startup order, wherein starting a first startup item comprised in the plurality of system startup items comprises: measuring a next startup item of the first startup item, and recording a measurement result into the verifiable startup chip, and wherein starting a last system startup item comprised in the plurality of system startup items comprises: measuring an attestation proxy program, and recording a measurement result into the verifiable startup chip;

starting an attestation proxy program based on the trusted execution environment; and

starting a first user application based on the trusted execution environment, and determining, by the attestation proxy program, first attestation information corresponding to the first user application based on local attestation in the trusted execution environment.

2. The method according to claim 1, further comprising: recording the first attestation information into the verifiable startup chip.

3. The method according to claim 2, further comprising:

in response to an access request of a remote user of the target platform for the verifiable startup chip, providing, for the remote user, a first record generated by the verifiable startup chip based on the first attestation information, so that the remote user determines security of the first user application and/or security of the target platform based on the first record.

4. The method according to claim 1, wherein the first attestation information is maintained by the attestation proxy program, and the method further comprises:

in response to an access request of a remote user for the verifiable startup chip, providing a second record for the remote user, wherein the second record is generated by the verifiable startup chip based on a first measurement result recorded when a tail startup item in the plurality of system startup items is started; and

in response to a connection request of the remote user based on the first measurement result, establishing, by the attestation proxy program, a trust channel with the remote user, and providing the first attestation information for the remote user by using the trust channel.

5. The method according to claim 4, wherein the second record is used by the remote user to determine security of the target platform based on the second record.

6. The method according to claim 4, wherein the first attestation information is used by the remote user to determine security of the first user application based on the first attestation information.

7. The method according to claim 5, wherein the determining security of the target platform based on the second record comprises: attesting, based on the second record, whether a version of an operating system (OS) and/or a virtual machine monitor (VMM) that are/is started on the target platform is a predetermined version, and determining security of the target platform based on an attestation result.

8. The method according to claim 1, wherein the verifiable startup chip comprises one of a trusted platform module (TPM) chip, a trusted cryptography module (TCM) chip, a trusted platform control module (TPCM) chip, and a Titan chip.

9. The method according to claim 1, further comprising: after the first user application is started,

starting a second user application based on the trusted execution environment; and

determining, by the attestation proxy program, second attestation information corresponding to the second user application based on local attestation in the trusted execution environment.

10. The method according to claim 1, wherein the first startup item in the plurality of system startup items is a core root of trust measurement (CRTM).

11. The method according to claim 10, wherein the plurality of system startup items further comprise several of a bootloader, an operating system (OS), and a virtual machine monitor (VMM).

12. The method according to claim 1, wherein the attestation proxy program comprises at least a trusted part;

the starting an attestation proxy program comprises at least: executing the trusted part in the trusted execution environment; and

starting the last item in the plurality of system startup items comprises: measuring the trusted part, and recording a measurement result into the verifiable startup chip.

13. The method according to claim 1, wherein the first user application comprises at least a trusted part;

the starting a first user application based on the trusted execution environment comprises at least: executing the trusted part in the trusted execution environment; and

the determining, by the attestation proxy program, first attestation information of the first user application based on local attestation in the trusted execution environment comprises:

determining, by the attestation proxy program, the first attestation information corresponding to the first user application based on local attestation in the trusted execution environment and the trusted part.

14. The method according to claim 1, wherein the determining, by the attestation proxy program, first attestation information corresponding to the first user application based on local attestation in the trusted execution environment comprises: invoking, by the attestation proxy program, a local attestation instruction of software guard extensions (SGX) to obtain the first attestation information corresponding to the first user application.

15. An apparatus for starting an application on a target platform, wherein the target platform comprises at least a verifiable startup chip and a trusted execution environment, and the apparatus comprises:

a system start unit, configured to sequentially start a plurality of system startup items based on a predetermined startup order, wherein starting a first startup item comprised in the plurality of system startup items comprises: measuring a next startup item of the first startup item, and recording a measurement result into the verifiable startup chip, and wherein starting a last system startup item comprised in the plurality of system startup items comprises: measuring an attestation proxy program, and recording a measurement result into the verifiable startup chip;

an attestation proxy start unit, configured to start an attestation proxy program based on the trusted execution environment; and

a user application start unit, configured to start a first user application based on the trusted execution environment, and determine, by the attestation proxy program, first attestation information corresponding to the first user application based on local attestation in the trusted execution environment.

16. A computer-readable storage medium that stores a computer program, wherein when the computer program is executed on a computer, the computer is enabled to perform the method according to any one of claims 1 to 14.

17. A computing device, comprising a memory and a processor, wherein the memory stores executable code, and when executing the executable code, the processor implements the method according to any one of claims 1 to 14.