over the previous technology (e.g., magnetic strip cards) for in-person purchases, account access still may rely on log-in credentials (e.g., username and password) to confirm a cardholder's identity. However, if the log-in credentials are compromised, another person could have access to the user's account.

[0006] These and other deficiencies exist. Accordingly, there is a need to provide users with an appropriate solution that overcomes these deficiencies to provide data security, authentication, and verification for contactless cards. Further, there is a need for both an improved method of activating a card and an improved authentication for account access and signaling an attack on cryptographic devices such as contactless cards.

SUMMARY

[0007] Aspects of the disclosed technology include systems and methods for cryptographic authentication of contactless cards. Various embodiments describe systems and methods for implementing and managing cryptographic authentication of contactless cards.

[0007a] An aspect of the present disclosure provides a contactless card, comprising a processor, and a memory. The processor is configured to set one or more of a first input data and a second input data to a first data value and a second data value respectively, create a one-time password (OTP) value from the first data value and the second data value, wherein the OTP value is indicative of a potential attack on the contactless card, and transmit the OTP value to a server.

[0007b] Another aspect of the present disclosure provides a method comprising receiving, by a processor, a one-time password (OTP) value, determining, by the processor, that the OTP value is indicative of a potential attack against a contactless card, wherein the OTP value corresponds to a counter having an invalid value and one or more keys having a zero value, and initiating, by the processor, a protective action responsive to the potential attack.

[0007c] Another aspect of the present disclosure provides a server comprising a memory and a processor. The processor is configured to receive a one-time password (OTP) value, the OTP value indicative of a potential attack against a contactless card, wherein the OTP value is generated from a counter having a maximum value and one or more keys having a zero value, and initiate a protective action responsive to the potential attack.

[0008] There is also disclosed an attack signaling system comprising: a contactless card including a substrate, one or more processors, and a memory; and one or more servers in data communication with the contactless card, wherein the contactless card is configured to, upon detection of a potential attack, create a one-time password (OTP) value that is transmitted to the one or more servers, the OTP value indicative of the potential attack; and wherein the one or more servers, upon receipt of the OTP value, are configured to perform one or more protective actions.

[0009] There is also disclosed a method for signaling a potential attack by a contactless card in data communication with a server, comprising: receiving, by the server, one or more codes from the contactless card; determining, by the server that the

CLAIMS

1. A contactless card, comprising:

a processor; and

a memory,

wherein the processor is configured to:

set one or more of a first input data and a second input data to a first data value and a second data value respectively,

create a one-time password (OTP) value from the first data value and the second data value, wherein the OTP value is indicative of a potential attack on the contactless card, and

transmit the OTP value to a server.

2. The contactless card of claim 1, wherein the processor is further configured to create the OTP value upon detection of a potential attack.

3. The contactless card of claim 1, wherein:

the processor is further configured to create the OTP value using an OTP generation algorithm, and

the first input data is based on at least one selected from the group of a counter, time, and a challenge-response data.

4. The contactless card of claim 3, wherein:

the first input data corresponds to an invalid OTP counter value, and

the second input data corresponds to a key of the contactless card set to a zero value.

5. The contactless card of claim 3, wherein the processor is further configured to create the OTP value by switching from a first OTP generation algorithm to a second OTP generation algorithm upon detection of a potential attack.

6. The contactless card of claim 3, wherein:

the first input data corresponds to a time value, and

the first data value is set to at least one selected from the group of a time value of zero, a time value prior to an activation of the contactless card, and a time value exceeding a maximum possible lifetime of the contactless card.

7. The contactless card of claim 3, wherein:

the first input data corresponds to the challenge-response data, and

the first data value is set to one of a value which is identical to a challenge value and a value that is configured to exceed a maximum value for a response associated with the OTP generation algorithm.

8. The contactless card of claim 1, wherein a plurality of counter-based OTP values are indicative of different potential attacks.

9. The contactless card of claim 1, wherein the processor is further configured to transmit the OTP value to the server via an intermediary device.

10. The contactless card of claim 4, wherein the invalid value of the OTP counter corresponds to one of a zero value and a maximum value of the OTP counter.

11. A method, comprising:

receiving, by a processor, a one-time password (OTP) value;

determining, by the processor, that the OTP value is indicative of a potential attack against a contactless card, wherein the OTP value corresponds to a counter having an invalid value and one or more keys having a zero value; and

initiating, by the processor, a protective action responsive to the potential attack.

12. The method of claim 11, further comprising determining, by the processor, whether a plurality of contactless cards have been subject to the potential attack during a predetermined time period.

13. The method of claim 11, wherein the protective action includes at least one selected from the group of:

generating a plurality of event logs associated with the attack of the contactless card,

transmitting a notification to threat response personnel,

rendering the contactless card mute,

initiating a replacement request of the contactless card,

initiating a communication session with a device so as to indicate compromise of the contactless card, and

establishing data communication with an engine so as to adjust a risk level of the user based on the detection of the potential attack.

14. The method of claim 11, further comprising determining, by the processor, when a first OTP generation algorithm is switched to a second OTP generation algorithm to generate the OTP value.

15. The method of claim 11, wherein an output of the second OTP generation algorithm is of the same format as an output of the first OTP generation algorithm.

16. A server, comprising:

a memory, and

a processor, wherein the processor is configured to:

receive a one-time password (OTP) value, the OTP value indicative of a potential attack against a contactless card, wherein the OTP value is generated from a counter having a maximum value and one or more keys having a zero value, and

initiate a protective action responsive to the potential attack.

17. The server of claim 16, wherein the processor is further configured to determine whether a plurality of contactless cards have been subject to the potential attack during a predetermined time period.

18. The server of claim 16, wherein:

the OTP value is generated using an OTP generation algorithm, and

the processor is further configured to determine when a first OTP generation algorithm is switched to a second OTP generation algorithm to generate the OTP value.

19. The server of claim 16, wherein the processor is further configured to receive the OTP value from a contactless card via an intermediary device.

20. The server of claim 16, wherein the potential attack comprises least one selected from the group of a code-modification attack, a fuzzing attack, and a clock jitter attack.