December 2022

Alternate Emergency Application Environment

Dillon Amadeo

Nizam Anuar

Yohan Launay

Kiat Chuan Tan

ALTERNATE EMERGENCY APPLICATION ENVIRONMENT

Introduction

Users of financial and banking applications and services generally have an authentication method (e.g., a personal identification number (PIN)) that allows them to access their financial information such as bank accounts. Traditionally, an authentication method is unique to the user, such as one PIN that allows access to the user's financial accounts. Therefore, the only way for a user to access an account on a mobile device is to open a financial or banking application, view the display to input the authentication method, and input the authentication method. As a result, a bad actor can force a user to withdraw or transfer money from the user's account to the bad actor because the user can only input their one authentication method on the one application display. Therefore, a user under duress does not have a mechanism to stop a bad actor from accessing the user's financial accounts through the user's financial applications and services.

Such a scenario has become more common, as forcing a user to withdraw funds from their financial accounts can be done virtually anywhere a user carries a mobile device with a financial or banking application. Consequently, some users have opted to not have any financial or banking applications on their mobile devices. Providing users with the ability to enter an alternate application environment in emergency situations will allow all users to have financial and banking applications on their mobile devices, increase the safety of the application's users, and deter robbers and other bad actors from accessing users' financial accounts.

Summary

Computer-implemented systems and methods for providing an alternate application environment in emergency situations with the disclosed technology can be accomplished by

allowing a user to perform an action in a financial application that indicates it is an emergency situation, displaying an alternative application environment that shows alternate (e.g., false) information about the user's accounts, and initiating safety measures while the user is using the alternative application environment. A user action in a financial application that indicates it is an emergency situation and allows the user to enter the alternative application environment may be any entry mechanism that is to be used exclusively in emergency situations (e.g., entering an emergency second PIN, performing a gesture that indicates there is an emergency, etc.).

In some instances, a user may use an entry mechanism that is exclusively for emergency situations in a financial or banking application on a computing device and view a display of alternative, false financial information in order to deter a bad actor from accessing the user's financial accounts. For example, a user may have a financial or banking application on their mobile device that allows access to the user's bank account or other financial accounts when the user opens the application and inputs a first, non-emergency PIN on a display. The application may display the user's balance in their accounts and allow the user to transfer money from one account to another account of the user's or an account of another entity. The user may also create a second, emergency PIN to use when the user is under duress from a bad actor. When a financial or banking application is opened and the second, emergency PIN is input on the display, the user may view an alternative application environment that displays alternate information about the user's account information, such as false account balances and transfer history. As a result, a bad actor will view incorrect information about the user's account, such as a very low balance, to deter the bad actor from forcing the user to transfer the displayed funds. In another example, the user may define a gesture to perform that is different from normal usage when the user is under duress from a bad actor, such as three taps on a display

button instead of one tap. When the financial or banking application is opened and the user performs the gesture, the user may view the alternative application environment that displays alternate information.

In some instances, a user may use an entry mechanism that is exclusively for emergency situations in a financial or banking application on a computing device and enter an alternative application environment where the user may not have the ability to perform financial transactions. For example, when the user attempts to transfer money to the bad actor, the alternative application environment may display an error message (e.g., error on the network, error on the receiver bank, error on the sender side, etc.) to show the bad actor that the transaction failed. The error message may be randomly selected in order to allow the user to attempt multiple tries to transfer money to the bad actor and display a different error message for each try. In another instance, the user may predefine a number of failed transactions to try before the transaction does go through and get processed by the user's financial institution in order to alleviate retaliation by the bad actor when there have been many failed transactions. In this scenario, although the user may lose funds from their account to the bad actor, it may delay the transaction in order to provide enough time for law enforcement to arrive. In another instance, the user may predefine one or more of a number of successful transactions or a monetary amount that may successfully go through and get processed by the user's financial institution in order to satisfy the bad actor so the bad actor will leave.

In some instances, a user may use an entry mechanism that is exclusively for emergency situations in a financial or banking application on a computing device and the application may perform security measures and collect information related to the crime in the background (e.g., starting a recording through a camera and/or microphone on the computing device, logging the

user's location, alerting law enforcement authorities of the user's location, flagging the transaction to allow for reversal of the transaction, etc.). For instance, when the user has many failed transactions so that a real transaction is triggered, the transaction may have been delayed for long enough to allow law enforcement to arrive because law enforcement was notified of the user's location when the user input the second, emergency PIN into the application or performed the emergency gesture. The computing device may also record the robbery, log the robber's bank account information, and flag the robber's bank account when the user enters the alternative application environment.

In some instances, a user may configure the alternative application environment that displays when the user uses an entry mechanism that is exclusively for emergency situations in a financial or banking application on a computing device. For example, a user can choose for the alternative application environment to display an account balance of zero or another amount. A user may also change the appearance of contact names in the transaction history display, such as deciding to show randomly generated names or to hide names entirely. A user may also choose the transfer status message that appears on the display when the user attempts to perform a transaction in the alternative application environment. For instance, the user can select a configuration that shows that a transaction "failed" or that a transaction is "pending" every time a money transfer transaction is attempted in the alternative application environment, or to show "failed" for a predetermined number of transaction and "pending" for another predetermined number of transactions.

Detailed Description

Figure 1 depicts an example computing system 100 in which systems and methods in accordance with the present disclosure can be executed. The computing system comprises a user

computing device 102 containing one or more processors 112, memory 114 which may contain data 116 and instructions 118 configured to carry out the methods disclosed herein, and a user input component 122. The user computing device 102 can be, for example, a personal computer (e.g., desktop or laptop), mobile device (e.g., tablet or smartphone), or wearable computing device. The user input component can be, for example, a touch display or physical buttons within the user computing device 102. The computing system 100 further comprises a network 180 and a server computing system 130. The server computing system 130 comprises one or more processors 132, and memory 134 which may contain data 136 and instructions 138 configured to carry out the methods disclosed herein. It should be appreciated that any combination or order of systems and methods disclosed herein can be performed on the user computing device, server computing system, or similar. For example, all processes can be performed on the user computing device 102 or the server computing system 130.

Figure 2 depicts an example embodiment of accessing an alternative application environment 200. A user may open an application (e.g., a financial or banking application) on a user computing device 102 and a display to input a PIN 202 may be presented to the user. The user may input a first PIN to access the real application 204 or the user may input a second PIN to access the application when under duress 206. The second PIN may be created by the user exclusively for use in emergencies, such as when the user is under duress from a bad actor attempting to force a transaction from the user to the bad actor, that is different from the first PIN.

When the user inputs the first, non-emergency PIN to access the real application 204, the display of the user computing device 102 may display the real application environment 208, showing the user's real financial and bank account information. For example, the real application

environment 208 may show the user's real financial and bank account information, such as an accurate account balance 210 and an accurate transaction history 212 with the correct contact names listed.

When the user inputs the second, emergency PIN to access the application 206, the display of the user computing device 102 may show an alternative application environment 214. The alternative application environment 214 may be a display of alternative, false financial information about the user's financial and bank accounts. For example, the alternative application environment 214 may display an account balance of zero 216 and a transaction history with incorrect amounts and contact names 218. The user may configure the alternative application environment 214 to display an account balance of zero or another amount 216 when the alternative application environment 214 is active. The user may also configure the transaction history 218 in the alternative application environment 214 to display contact names that are randomly selected from a group of incorrect contact names or to hide contact names from the display. Therefore, a user who is under duress from a bad actor trying to access the user's financial or bank information may input the second, emergency PIN 206 and the bad actor may view a display of the alternative application environment 214 with false information, deterring the bad actor from accessing the user's accounts.

Referring now to Figure 3, an example embodiment of an alternative application environment when a user uses an entry mechanism that is exclusively for emergency situations 300. A user may open an application (e.g., a financial or banking application) on a user computing device 102, a display to input a PIN 202 may be presented, the user may use an emergency entry mechanism 206 (e.g., a second, emergency PIN or emergency gesture), and the display of the user computing device 102 may show an alternative application environment 214.

The alternative application environment 214 may not allow the user to perform financial transactions, such as transferring money from one account to another account of the user's or an account of another entity.

For example, when using the alternative application environment 214 while under duress from a robber, a user may be forced to select an element of the display to transfer funds 302 to the bad actor. A user may select the element of the display to transfer funds 302 and input information such as an amount of money to transfer and the entity receiving the transferred funds. As a result, the alternative application environment 214 may display an error message 304, displaying to the bad actor that the transaction failed. The error message 304 may display one of several error messages, such as, for example, an error on the network, error on the receiver bank, or error on the sender side. The error message 304 may be randomly selected from a group of error messages in order to allow for multiple different "failures" of the transfer while the user is in the alternative application environment 214. The user may also configure the alternative application environment 214 to display a predefined number of different error messages 304, thus predefining a number of "failed" transactions to try. In this implementation, once the predefined number of error messages 304 are all displayed, the transaction (e.g., transfer of funds to the robber) may go through to be processed by the user's financial institution.

Figure 4 depicts an example embodiment of security measures implemented when a user uses an entry mechanism that is exclusively for emergency situations 400. A user may open an application (e.g., a financial or banking application) on a user computing device 102, a display to input a PIN 202 may be presented, the user may use an entry mechanism 206 (e.g., a second, emergency PIN or emergency gesture), and one or more security measures 402 may be automatically initiated. For example, when a user inputs the emergency PIN 206, the user

computing device 102 may start a recording through the device's microphone and/or camera. The location of the user computing device 102 may also be automatically logged and stored on the user computing device 102 when the user inputs the emergency PIN 206. The log of the location of the user computing device 102 may also be transmitted to law enforcement in order to alert the authorities of the user's location. When the user inputs the account information of the bad actor forcing the transaction, the user computing device 102 may record the account information. The security measures 402 may be implemented in the background of the user computing device 102 instead of appearing to the user on the user interface. The user information related to the crime (e.g., the recording, location, account information, etc.) may also be automatically collected and stored on the user computing device 102.

Figures

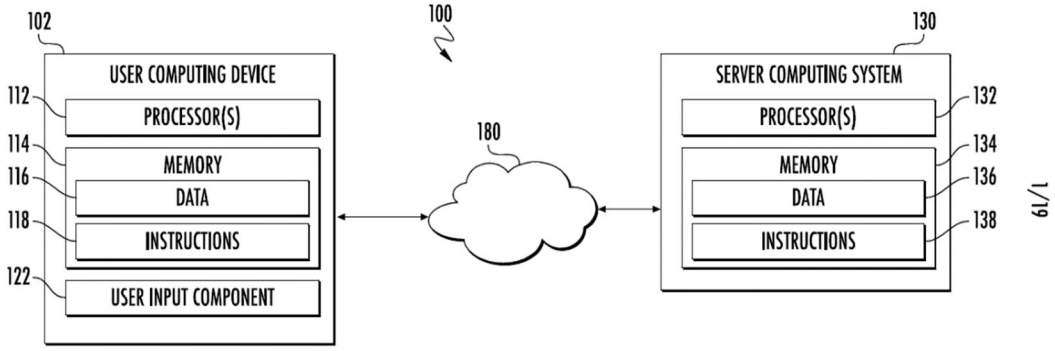

FIG. 1

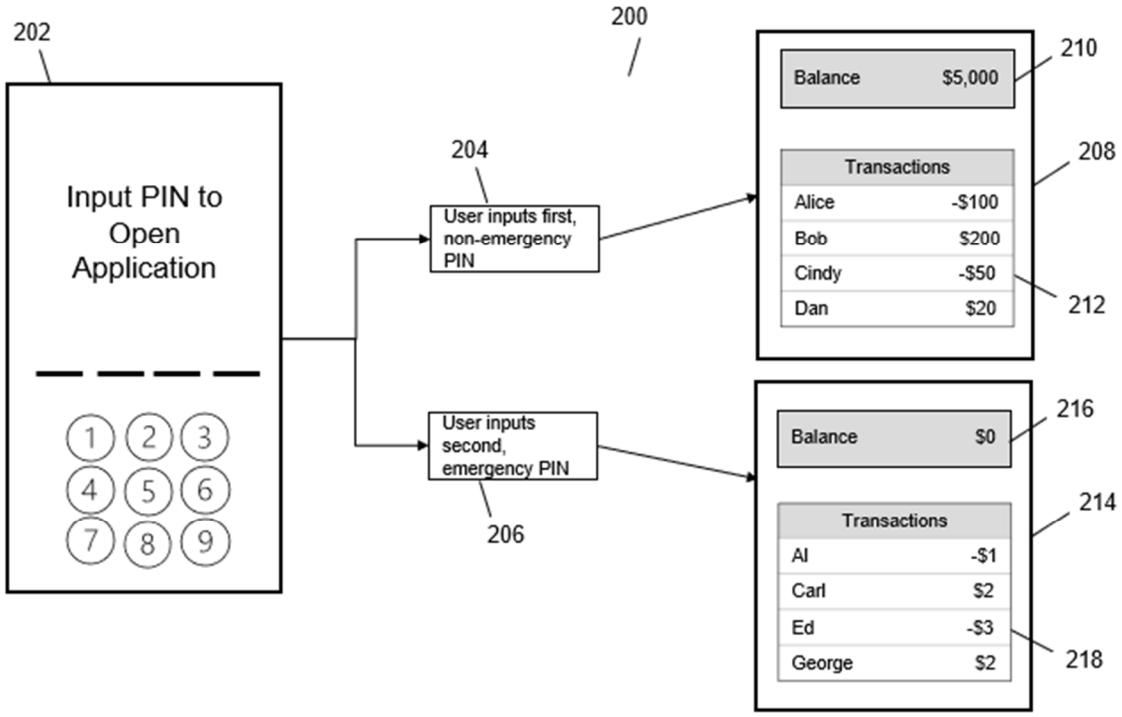
202
200
Input PIN to Open Application
1 2 3
4 5 6
7 8 9
204
User inputs first, non-emergency PIN
User inputs second, emergency PIN
206
Balance $5,000
210
Transactions
Alice -$100
Bob $200
Cindy -$50
Dan $20
208
212
Balance $0
216
Transactions
Al -$1
Carl $2
Ed -$3
George $2
214
218

FIG. 2

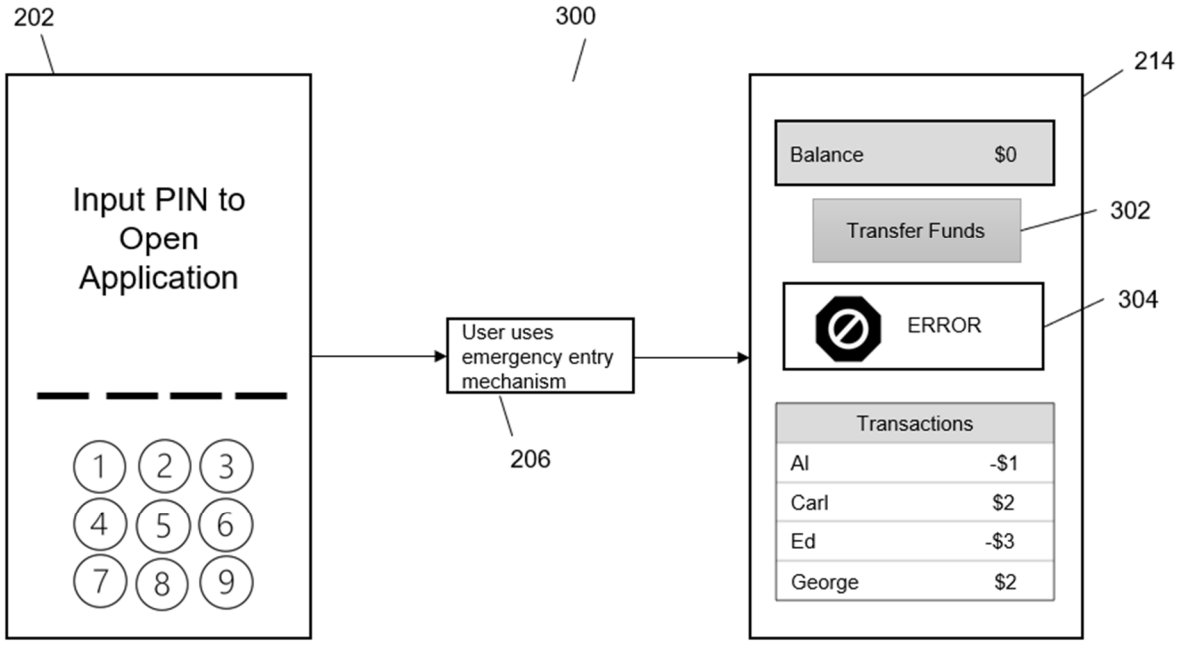
202
300
Input PIN to Open Application
1 2 3
4 5 6
7 8 9
User uses emergency entry mechanism
206
214
Balance $0
Transfer Funds
302
ERROR
304
Transactions
Al -$1
Carl $2
Ed -$3
George $2

FIG. 3

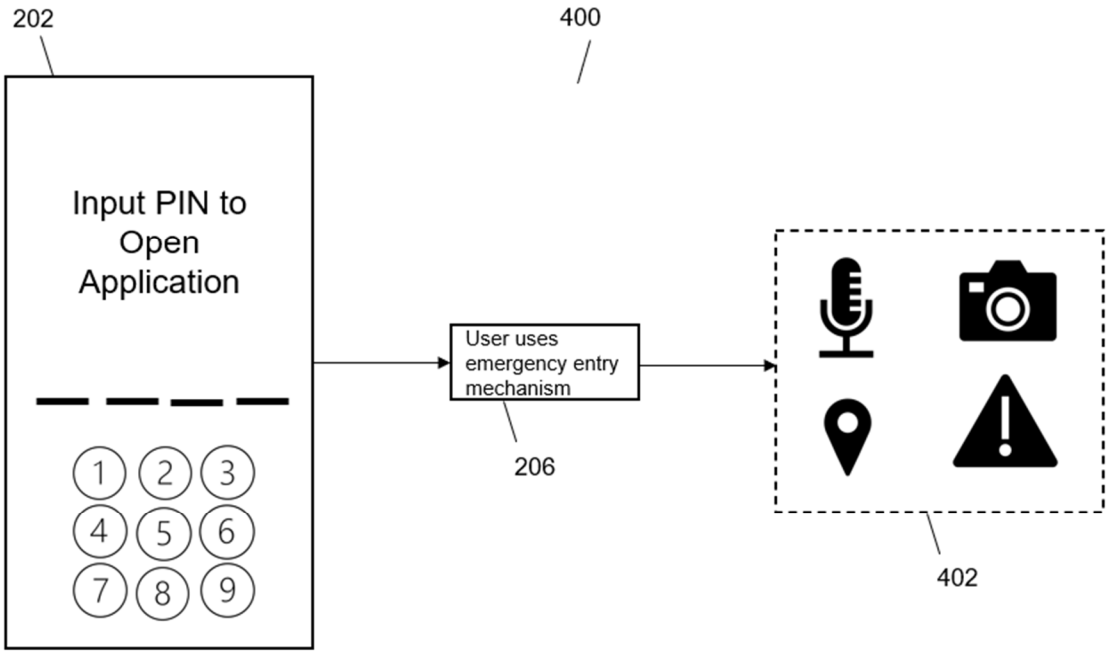

FIG. 4

Abstract

The present disclosure describes computer-implemented systems and methods for providing an alternate application environment in emergency situations by allowing a user to use an entry mechanism that is for use in emergency situations (e.g., input an alternative PIN or emergency gesture) to enter a financial or banking application on a user computing device. The input of the emergency entry mechanism may display an alternative application environment that shows alternative information about the user's accounts, prevents the transfer of funds to another entity, and initiates security measures while the user is in the alternative application environment. As a result, the safety of users of financial and banking applications can be increased, and bad actors can be deterred from accessing users' financial accounts.