iSECpartners
part of nccgroup

Automated PIN Cracking

Justin Engler
Senior Security Engineer
iSEC Partners

Paul Vines
Security Engineering Intern
iSEC Partners

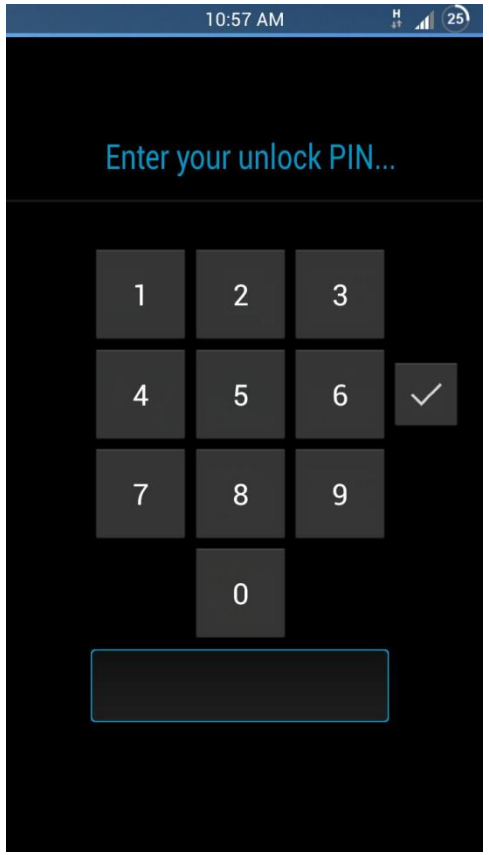
Agenda

iSECpartners part of nccgroup

- Current PIN Cracking Methods
- Cracking with Robots
- R2B2
- C3BO
- Defeating the Robots

PINs

- One of the most popular ways to lock mobile devices
  - Commonly still only 4-digit despite ability to be longer
  - User chosen, so typically low-entropy



iSECpartners
part of nccgroup

PIN Cracking Now

- Jailbreak and Crack
- Keyboard Emulation
- Punish an Intern

iSECpartners part of nccgroup

Jailbreak and Crack

- Use jailbreaking/rooting exploits on the device
- Bypass the lock screen with these new user capabilities
- **Problem:** not all devices have known exploits for gaining root (and without wiping the device)

iSECpartners
part of nccgroup

Keyboard Emulation

- If the device supports a keyboard attachment
  - Make a device that emulates a keyboard and tries all the different PIN combinations automatically
- **Problem:** not all devices support an external keyboard being added

iSECpartners
part of nccgroup

Punish an Intern

- Forcing your intern to try all 10,000 4-digit combinations will surely be more productive than anything else they could have been doing, except maybe getting coffee
- **Problem:** Interns are universally bad at their jobs, so they might miss some of the combinations

iSECpartners
part of nccgroup

PIN Cracking with Robots

- Required Abilities:
  - "Push" buttons in sequence
  - Remember what buttons were pushed
  - (Recognize success)

iSECpartners
part of nccgroup

Robotic Reconfigurable Button Basher (R2B2)

- Homemade Delta Robot body
- Arduino Uno brain
- Total cost: < $200

Delta Robot

- Designed for fast precision industrial work
- Simple combination of 3 single-motor arms gives precision 3D movement with somewhat small range of motion
- Fairly simple motion control

Humanrobo, Wikipedia.
CC-BY-SA

iSECpartners
part of nccgroup

Arduino Uno

- Standard robotic hobby microcontroller board
- Open source code for controlling a delta robot by Dan Royer (marginallyclever.com)
  - Uses serial port communication to control the movement of the robot
- Easy to tweak functionality for pressing buttons instead of manufacturing
- Easy to control with a Python program

iSECpartners
part of nccgroup

Modifications

- The original delta robot kit was modified to have its tool be a touch-screen stylus tip for pressing buttons
- A camera was added to allow easier user interface with the robot to set up the PIN cracking task
- The motion control software was modified to speed up movement, up to 5 presses/second

iSECpartners
part of nccgroup

Wrap Everything in Python

- Controls the robot movement through the serial port
- Performs image analysis of the camera feed
- Provides a simple interface for the user to set the robot up for PIN cracking
- Detects success of PIN cracking to stop robot and alert user

iSECpartners
part of nccgroup

(a bit) Better than brute-forcing

- Compiled the various password datasets and extracted 4-digit PINs to generate a frequency table of the 10,000 possibilities.

Challenges

- Detecting button values:
  - Too tough to reliably do on all devices
  - User set up time is negligible for a 10-digit keypad
- Recognizing delays:
  - Some devices have more easily recognized delay messages than others
  - If necessary, the user can manually input the delay pattern of a device (i.e. 30 seconds every 5 tries)

iSECpartners
part of nccgroup

Real Buttons Too!

- R2B2 can of course also be used for brute-force PIN cracking of physical buttons as well
- Electronic keypads or completely mechanical keys, provided it can detect when it has succeeded

iSECpartners
part of nccgroup

Capacitive Cartesian Coordinate Bruteforcing Overlay (C3BO)

- Attach a grid of electrodes to the device's virtual keyboard
- Trigger electrodes via an Arduino to trick the device into thinking the screen was touched at that point
- No mechanical motion = faster button pressing
- More user configuration required to manually place the electrodes

iSECpartners
part of nccgroup

C3BO continued

- Cheaper than R2B2 (~ $50)
- Nearly the same software for controlling/detecting device state changes with camera

iSECpartners
part of nccgroup

Defeating the Robots

- Forced delay timer after X attempts
  - On Android this is always 30 seconds regardless of previous attempts
    - R2B2 would succeed in a worst case of ~20 hours
- User Lockout after X attempts
  - On iOS this occurs after 11 attempts
    - R2B2 would be defeated, unless the PIN was one of the 10 most popular

iSECpartners
part of nccgroup

Are these robots useful, then?

- Compared to R2B2:
  - Jailbreak + Bypass: Best if available
  - Keyboard Emulator: The fastest brute-forcing
  - C3BO: Usable on any capacitive touch keyboard, a bit slower and more setup required than a keyboard emulator
  - R2B2: Flexible and usable on basically any PIN protected device but slower and more cumbersome

iSECpartners
part of nccgroup

Acknowledgments

- Thanks to iSEC Partners and the NCC Group for supporting this research
- Thanks to Dan Royer for providing the initial motion control code and robot build plans