HACKING THE PLANET (UNDER GLASS)

Rich Wickersham

WHOAMI

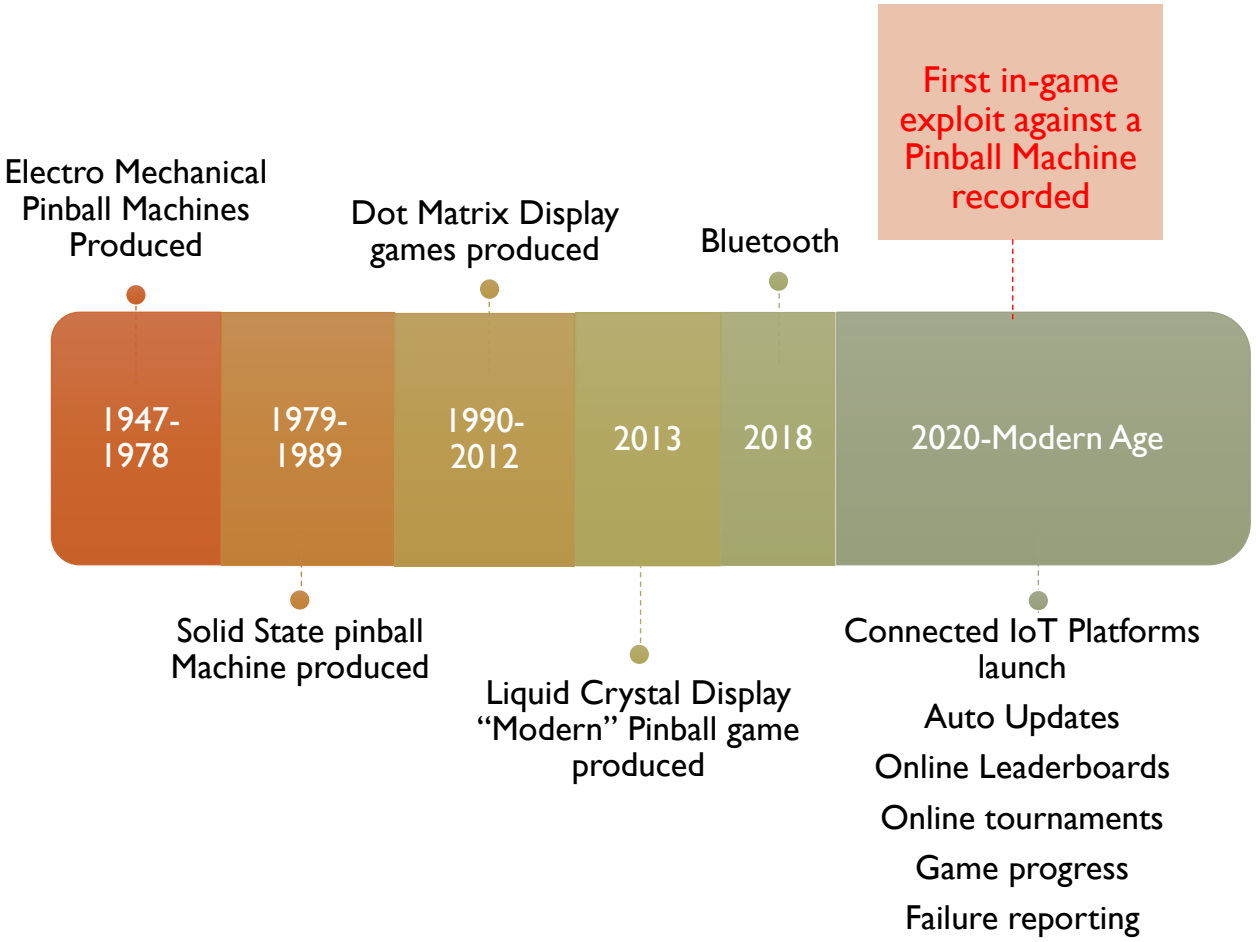
Rich Wickersham

- World Ranked Pinball Player!
- Hobbyist Operator, Restorer and Modifier of Pinball Machines
- Core Organizer at BSides NoVA
- OSINT & Security Researcher with past speaking engagements including DEF CON and Voice of America
- 23+ years in Cyber Security field, former Fortune 500, DHS and US HoR leadership experience
- Follow me
  - On X @richwickersham
  - Or my research via Github https://github.com/TheShadoru

WHAT IS A PINBALL MACHINE?

- Pinball = a physical skill game where a metal ball is propelled by a plunger and flipped by flippers in order to solve a complex puzzle and achieve a high score.
- Components = Flippers, Steel balls, Pop Bumpers, Slingshots, Coils, Relays, Switches, and today pinball machines are IoT devices….

TIMELINE OF PINBALL MACHINE MODERNIZATION



PINBALL MODERNIZATION

Electro Mechanical
1947-1978

Solid State
1979-1989

Dot Matrix
1990-2012

Liquid Crystal
2013

Modern Connected
2018 +

POTENTIAL THREATS

- Financial Threats
  - Tournament Prizes
- Score Integrity
  - Cheating and Interference
- Loss of Availability of IoT pinball machines
- Loss of income for Pinball operators
- IoT pinball Botnets

MOTIVE = CHEATING

ars TECHNICA BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE STO

SMILE, YOU'RE ON CANDID CAMERA —

Donkey Kong cheating case rocked by photos of illicit joystick modification

Tall, red-topped stick could prove crucial in Mitchell's defamation suit.

KYLE ORLAND - 2/3/2023, 1:02 PM

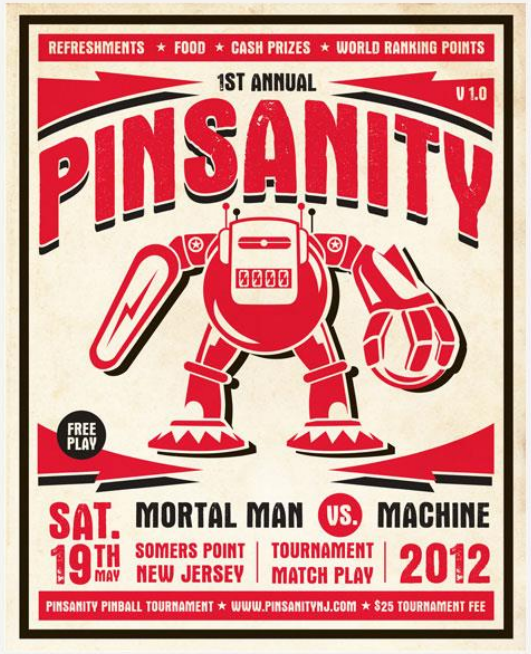
The biggest esports scandals of the past 10 years

By Luke Winkle | Contributions from Tyler Wilde published January 13, 2023

Corporate catastrophes, cheating incidents, and heated gamer moments.

COMMENTS

MOTIVE = FINANCIAL GAIN



PINBALL VULNERABILITY

- Brought an IoT Pinball Machine to BSides NoVA in 2020
- This was the first Pinball Machine to include Bluetooth connectivity via a mobile app
- Found an exploitable Bluetooth vulnerability/Bug on code version 1.73
- Determined that the vulnerability could impact players during an active game
- Mobile Applications were removed from Apple and Google app stores
- Code version 1.75 was released which deprecated support for the BT app

THREAT MODEL

1

2

3

DISCLOSURE

- Reached out to Leadership of pinball company prior to bringing the game to the security conference
- Reached again out after finding the vulnerability in code version 1.73
- Code version 1.75 removed support for the mobile app entirely
- The mobile app was removed from the app stores
- Paused research due to the Pandemic
- Reached out to Pinball Developers after selection for this talk
- Working with developers now

CODE 1.75 READ ME

```
================================================================================
=
==                                Version 01.75     October 14, 2021
==
==                        ISO MD5 Checksum: fc8d0c02e9535bd08a9c15b2431bcfae
==
================================================================================
=

- NOTE: This is a FULL INSTALL release

=== Game Code
+ added achievements with Scorbit
+ added score tracking and mode display info with Scorbit
* tweaked ball save time for Quantum City Multiball
* tweaked Big Bang points in competition mode
- the Dialed In! mobile app is not supported from this version forward
* various bug fixes and improvements

=== Core Code
+ Added WiFi and hard-wired networking. This allows for future online update
  support. You'll need to install a WiFi dongle or hardwire the game to your
  network for this feature to work
+ added the option to opt-in to Beta Network Updates
+ Added Player Menu, accessing it by holding the right flipper button in
  Attract Mode. This allows for connecting of Bluetooth headphones. You'll
  need to install a Bluetooth dongle for this feature to work
+ added a shaker motor test
+ added shaker motor option to Matrixed Switches Test to help find flaky
  switches without having to pound on the playfield
+ enhanced Camera Diagnostic screen with basic camera adjustments. added test
  picture capability
* various bug fixes and improvements
```

NAMING THE VULNERABILITY

BT MOBILE APP RECOMMENDATIONS

1. **Remove the Bluetooth Dongle** from pinball machines during tournament play!
2. Release code that allows an operator to Switch Off the device's Bluetooth to prevent other devices from pairing.
3. Release code that prevents Bluetooth pairing during a multi-player game.
4. Limit the number of apps/devices that have access to the device's Bluetooth connection to 1 or less*.
5. Release or validate code update to prevent in game pairing.
6. Release code update to display currently paired devices to active players.
7. Clear a history/memory of previously paired devices after a game completes.
8. Keep the device updated with the latest code updates, turn auto-update on.

SMALL BUSINESS RECOMMENDATIONS

1. Every Small Business should have a Dedicated email for reporting security vulnerabilities(e.g. security security@pinballcompany.com)
2. Provide an automated response to the email to let researchers know they are emailing a legitimate and monitored account. “thank you for your submission. We will validate and respond to you within ## business days ”
3. Make sure someone technical is responding to the researcher.
4. Provide a PGP key to allow encrypted technical details of the vulnerability to be transmitted.
5. Harness the power of your highly technical and enthusiastic customer base.

LESSONS LEARNED

- Security is not priority one for most small businesses. Getting a response from the pinball company was a major challenge.
- Reaching out to developers first is better than directly contacting corporate leadership.
- If you have a passion for something **don’t get discouraged** and **don’t give up**, you will eventually make a positive difference!

NEXT STEPS FOR PROJECT STEEL BALL

- Approached the Largest Pinball Company in the world with a proposal to bring IoT Pinball to Hacker Summer Camp for a sanctioned activity!
- Registered PinballVulnerabilities.com
- Established contacts with 3 of the largest Pinball Companies in the world to collaborate on security
- Brought the security community and pinball community together
- Secure pinball for current & future generations

THANK YOU

And sorry I broke my promise regarding DPRK!

Additional Research: https://github.com/TheShadoru/Project-Steel-ball

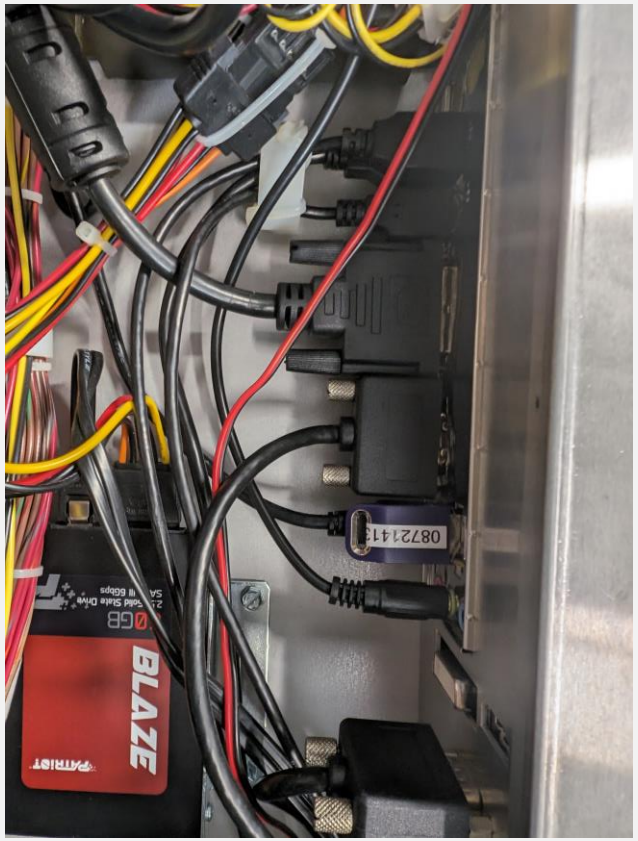
CREDIT GIVEN

- Sophia Fadli & the BSIDES Nova Team
- Jason B
- Scott Sidley
- A human(that validated the issue) and shall remain unnamed due to employer challenges!

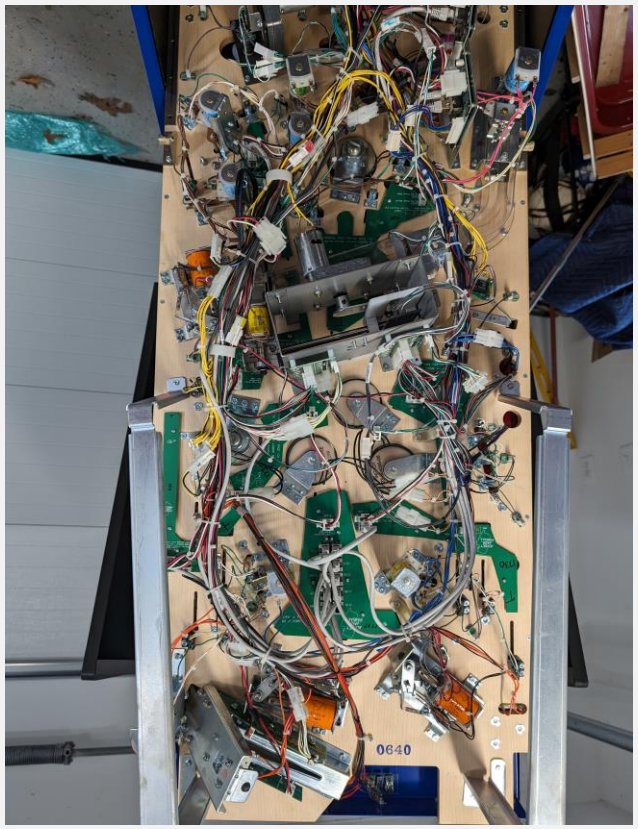
BACKUP

- Backup slides

DETAILED COMPONENTS OF A PINBALL MACHINE



Hard drive, USB interfaces and USB security key



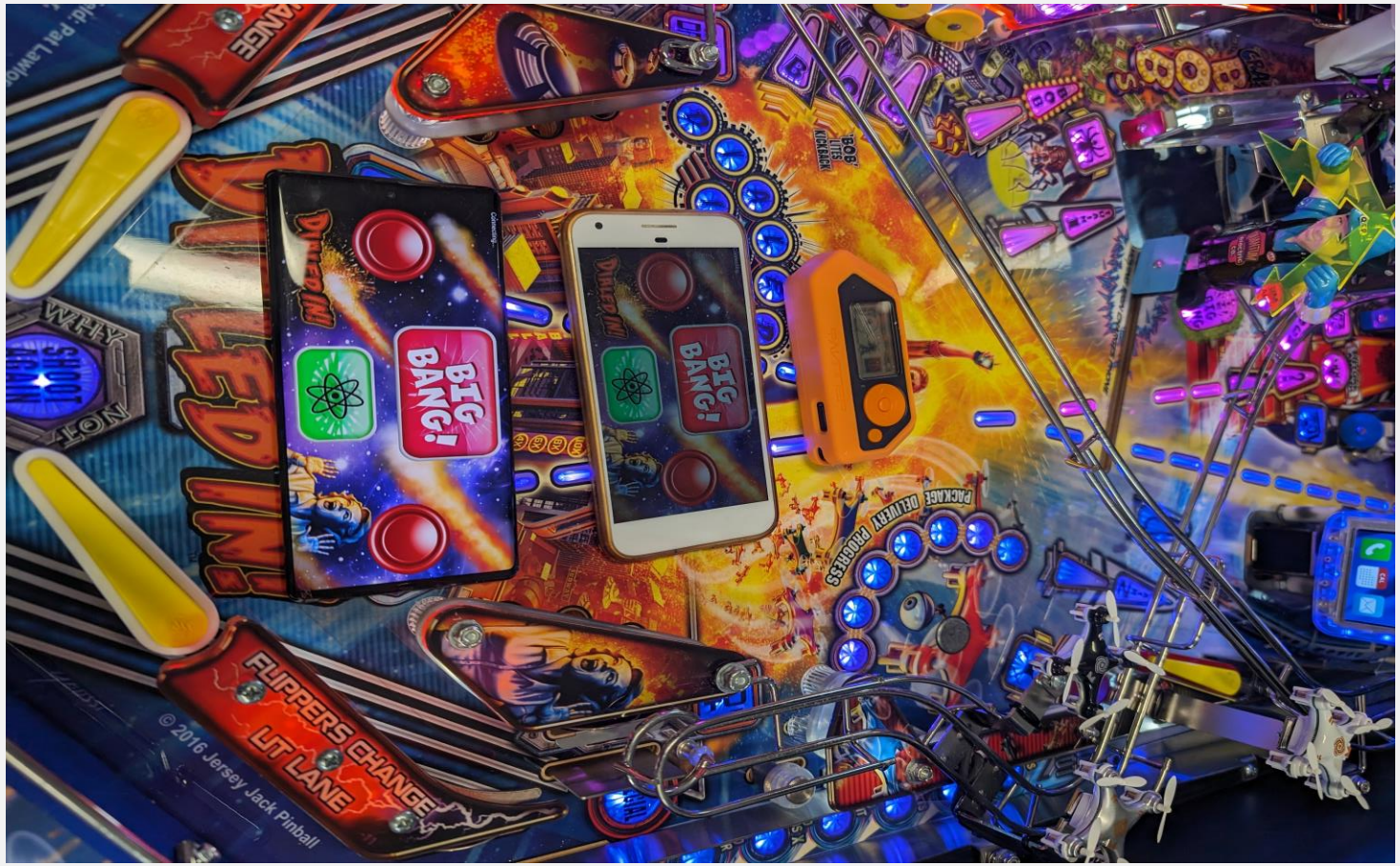
Underside of playfield

Bluetooth dongle location

FINANCIAL THREATS

- Prize pools for competitive Pinball are high(in excess of **$100k** at large events)
- Online competitions with large payouts are emerging
- Full payment system integration may emerge soon
- Gambling on e-sports(including pinball) is emerging
- When money is involved the potential for a direct competitor or outsider to interfere increases
- If we are not careful the integrity of the game could be at risk

MOBILE APP TESTING V1.75



GEN AI THREAT MODEL

IN THE BEGINNING