Cyber-Physical Vulnerabilities in Automated Teller Machines: An Analysis of Jackpotting Attacks

Ethan Molder
Role: Research, Threat Modeling, & Risk Analysis
emolder@vols.utk.edu

Harrison Crettol
Role: Research, Physical Simulation, & Hardware Integration
hcrettol@vols.utk.edu

***Abstract*—Automated Teller Machines (ATMs) represent a critical intersection of cyber and physical infrastructure within the financial sector. Since 2020, a sophisticated cyber-physical attack vector known as "Jackpotting" has surged, resulting in significant financial losses. This paper analyzes the physical and digital vulnerabilities exploited during these attacks, specifically focusing on the Ploutus malware utilized by organized crime syndicates such as Tren de Aragua. We present a comprehensive threat model, conduct a quantitative and qualitative risk analysis, and propose mitigation strategies involving hardware compartmentalization and cryptographic validation. Furthermore, we detail a physical simulation of the exploit using an ESP32 microcontroller, demonstrating the direct translation of network compromise to hardware actuation.**

***Index Terms*—Cyber-Physical Systems, Jackpotting, Ploutus, Hardware Security, Critical Infrastructure**

I. Introduction

Automated Teller Machines (ATMs) are ubiquitous cyber-physical systems (CPS) providing essential financial services. While their physical cash vaults are heavily fortified, the underlying computational architecture often relies on outdated or poorly secured commercial off-the-shelf (COTS) operating systems. Beginning in 2020, a resurgence of "ATM Jackpotting" attacks highlighted these structural weaknesses [1].

Jackpotting is a targeted attack where malicious actors gain physical access to the ATM's internal computer (often located in a less secure "top box") and deploy malware. This malware bypasses the machine's standard network authorizations and directly commands the internal cash dispenser to release all available currency. These attacks have resulted in millions of dollars stolen, often allegedly funding broader operations by transnational organized crime groups, notably Tren de Aragua (TdA) [1]. This paper dissects the mechanics of these attacks, models the associated risks, and explores viable defenses.

II. Threat Model

The attack chain for ATM jackpotting necessitates a combination of physical intrusion and cyber manipulation, defining a unique CPS threat model.

A. Reconnaissance

The attack lifecycle begins with physical surveillance. Threat actors monitor target ATMs to determine cash replenishment schedules, periods of low foot traffic, camera placements, and estimated law enforcement response times. This data dictates the optimal attack window.

B. Physical Intrusion

Unlike brute-force attacks on the secure cash vault (the safe), jackpotting targets the upper cabinet containing the ATM's PC and communication bus. As shown in Fig. 1, attackers often exploit structural weaknesses or the commonality of physical keys across ATM models to access the internal hardware without triggering physical breach alarms.

Fig. 1. Surveillance footage of a physical intrusion into an ATM cabinet during a jackpotting attack.

C. Cyber Compromise (The Ploutus Payload)

Once physical access to the internal PC is achieved, attackers introduce malware, predominantly variants of the *Ploutus* family. This is typically achieved via an infected USB drive or a rogue hardware device patched directly into the bus, such as the modified interface tool recovered by law enforcement shown in Fig. 2.

Ploutus targets the XFS (eXtensions for Financial Services) middleware, which acts as the bridge between the ATM's operating system and its peripheral hardware (e.g., the cash dispenser). By hooking into the XFS layer, Ploutus allows attackers to issue direct API calls to the dispenser mechanism,

effectively bypassing the bank's core network authentication protocols.

Fig. 2. A modified hardware device recovered by law enforcement, used to inject malware into the ATM's internal PC.

III. Risk Analyses

The risks associated with jackpotting extend beyond immediate financial loss, affecting institutional stability and broader societal security.

A. Quantitative Impact

While ATMs generally hold localized cash reserves to balance availability and risk, individual machines can contain between $10,000 and $100,000. Since 2020, the United States has seen approximately 1,900 jackpotting incidents, with over 700 occurring in 2025 alone. These attacks have resulted in an estimated total loss exceeding $20 million, averaging $30,000 per successful breach [1].

B. Qualitative Impact

While large institutional banks can absorb these financial shocks, smaller regional branches may face severe operational disruptions. The sudden depletion of on-hand cash restricts withdrawal capabilities, leading to immediate customer dissatisfaction. Prolonged or repeated attacks can erode consumer trust, potentially triggering localized liquidity crises if customers rapidly withdraw funds.

Furthermore, the secondary impact of these stolen funds is profound. The proceeds from jackpotting attacks, particularly those orchestrated by syndicates like TdA, are often diverted to finance severe illicit activities, including human trafficking, arms smuggling, and narcotics distribution [1].

IV. Defense, Response, and Mitigation Strategies

The root cause of jackpotting vulnerabilities lies in the assumption that physical security of the external cabinet guarantees the integrity of the internal network. Mitigating this threat requires a defense-in-depth approach spanning both domains.

A. Physical and Environmental Controls

The reliance on universal master keys for ATM top boxes must be eliminated in favor of unique, cryptographic locking mechanisms. Furthermore, regulatory bodies should mandate enhanced environmental monitoring, including advanced telemetry that instantly alerts law enforcement to unauthorized access of the PC cabinet, independent of the main vault sensors.

B. Cyber-Physical Isolation

A significant vulnerability is the lack of physical security surrounding the internal hard drive. Moving the computational core inside the hardened cash vault would physically secure the operating system, though this introduces engineering challenges regarding cable routing and potential structural weaknesses.

C. Cryptographic Validation

The most robust cyber mitigation involves implementing Full Disk Encryption (FDE) coupled with Secure Boot protocols. The ATM must cryptographically validate the integrity of the operating system and the XFS middleware before authorizing any hardware actuation. For instance, employing a Hardware Security Module (HSM) to verify the hash of the system state against a known-good signature would prevent unauthorized malware execution. While robust, this approach requires careful optimization to ensure the hashing process does not induce unacceptable latency during legitimate customer transactions.

V. Simulation: Hardware Override Demonstration

To practically validate the threat model, our team designed and constructed a physical simulation demonstrating the core mechanic of a jackpotting exploit: bypassing network controls to directly actuate physical hardware via a local interface.

As seen in Fig. 3, the simulation utilizes an ESP-32S NodeMCU microcontroller to represent the compromised ATM architecture. An SG90 Micro Servo motor, acting as the cash dispenser mechanism, was integrated into a constructed physical chassis. The ESP-32S was programmed to host an independent wireless access point and a local "Command & Control" web terminal.

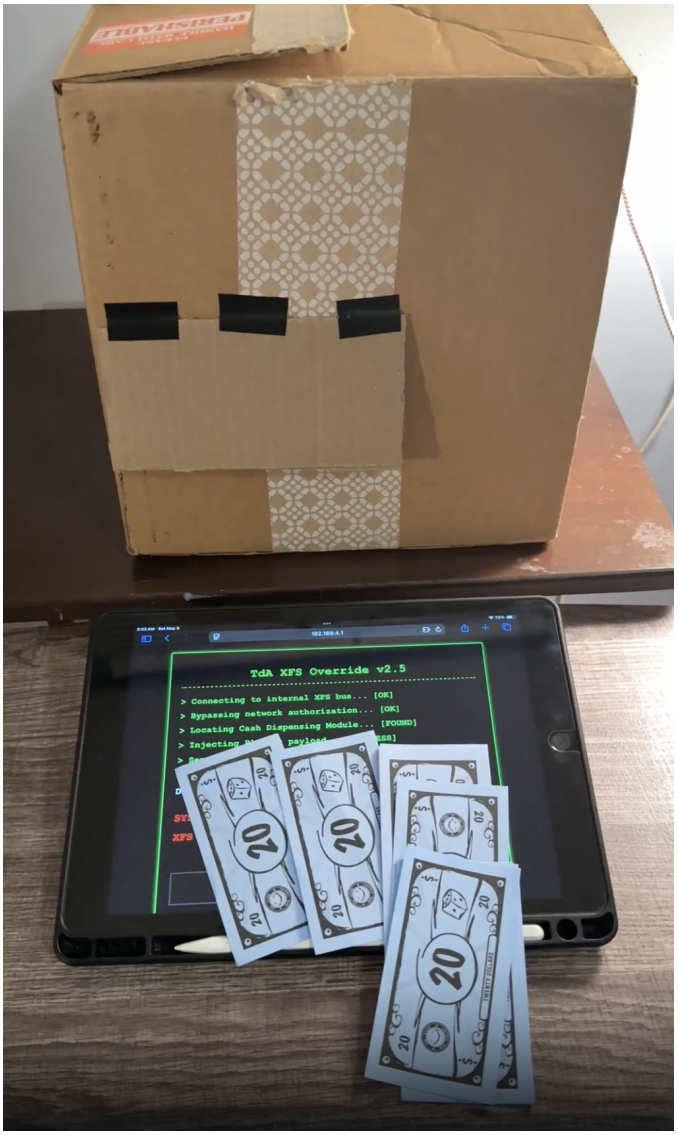

Fig. 3. Physical simulation of the ATM jackpotting exploit utilizing an ESP-32S and SG90 servo motor.

Upon accessing this local network (simulating the physical breach and malware injection), a user can trigger the web interface. This action bypasses any external ”bank” authorization and sends a direct signal to the microcontroller’s GPIO 13, rotating the servo 180 degrees to release a physical payload. This simulation successfully modeled the translation of a cyber-exploit (local network access and unauthorized API calls) into unauthorized physical actuation.

VI. Discussion & Limitations

The rise of ATM jackpotting underscores a prevalent flaw in critical infrastructure security: the failure to continuously update threat models against evolving cyber-physical attack vectors. Many system owners rely on outdated security policies or assume that complex attacks are improbable. Modern breaches frequently exploit small, systemic vulnerabilities—such as shared physical keys or unencrypted communication buses—rather than relying on highly sophisticated, ”Hollywood-style” hacking techniques.

A limitation of our proposed cryptographic mitigation (FDE and Secure Boot) is the significant hardware overhaul required across legacy ATM fleets. Implementing HSMs and ensuring low-latency hash validation on older processors presents a substantial financial and logistical hurdle for financial institutions.

VII. Conclusion

ATM jackpotting represents a severe cyber-physical threat that leverages physical intrusion to deploy sophisticated middleware exploits. The financial losses, while significant, are overshadowed by the utilization of these funds to support transnational organized crime. Securing these systems requires an integrated approach that eliminates universal physical access, implements rigorous cryptographic validation of system software, and ensures continuous, hardened communication between the cyber architecture and physical actuation mechanisms.

References

[1] Office of Public Affairs, “Investigation into international ‘ATM jackpotting’ scheme and Tren de Aragua results in additional indictment and 87 total charged defendants,” United States Department of Justice, Apr. 2026. [Online]. Available: https://www.justice.gov/opa/pr/investigation-international-atm-jackpotting-scheme-and-tren-de-aragua-results-additional