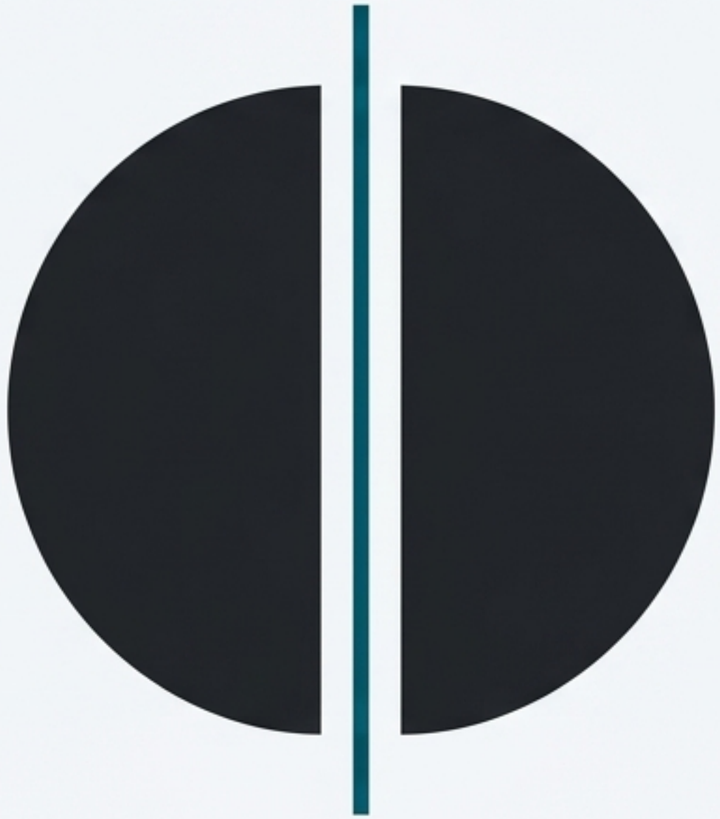
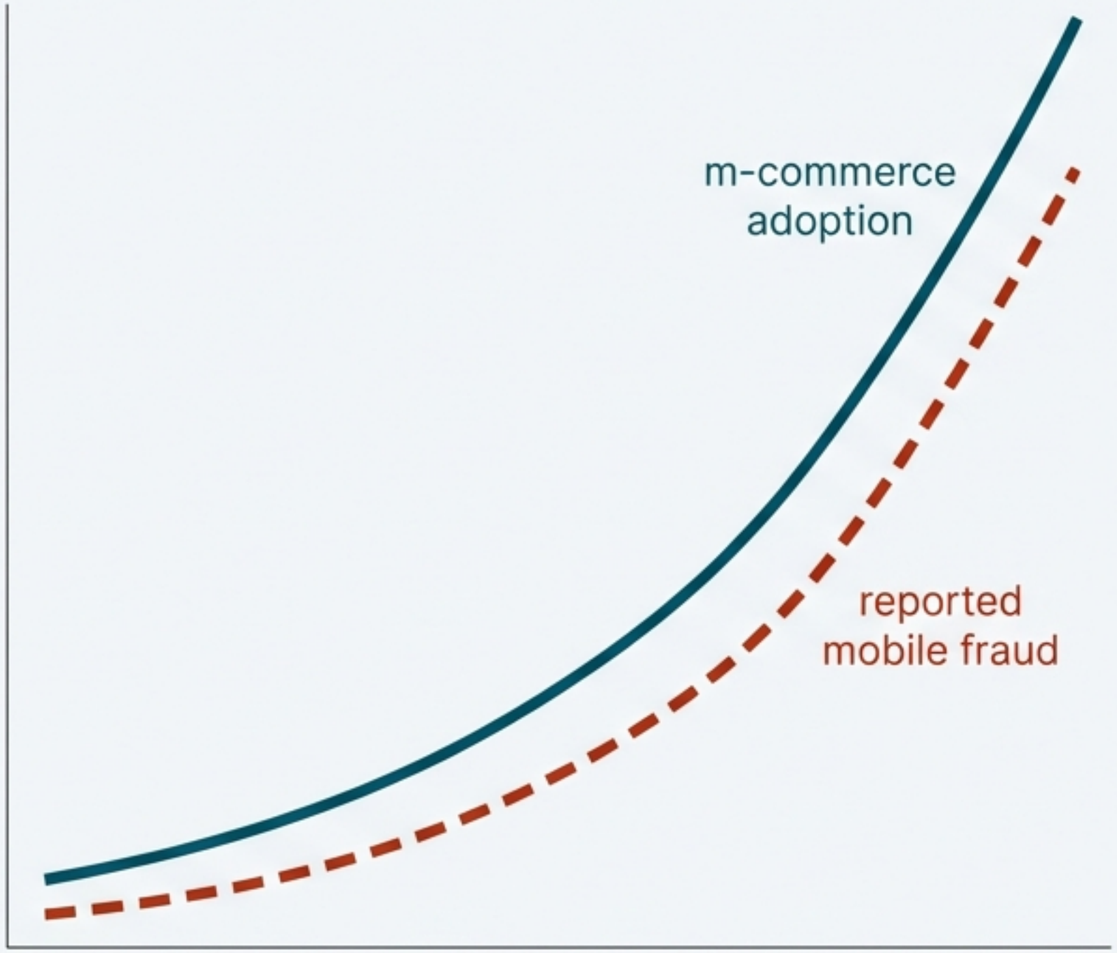
Rethinking Mobile Security: A Distributed Approach to PIN Verification

A probabilistic analysis of a surgical solution to the vulnerabilities of Personal Trusted Devices (PTDs).



Mobile Commerce is Exploding, But Its Security Foundation is Brittle



The rapid adoption of Personal Trusted Devices (PTDs) for e-commerce has outpaced the evolution of their security, creating significant financial and privacy risks.

"Credit card fraud was the most common complaint, with 50% of complainants reporting credit cards opened in their name or similar activities."

"Mobile telephone fraud came in second, accounting for 28% of reported complaints [to the FTC's identity theft hotline]."

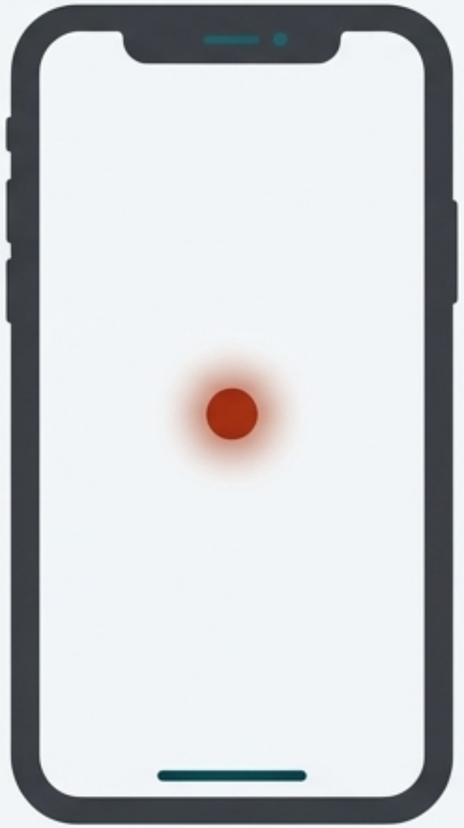
"In Britain...up to 1,000 digital mobile telephones are stolen each month and that up to forty per cent of car break-ins in London are for the purpose of stealing a mobile telephone."

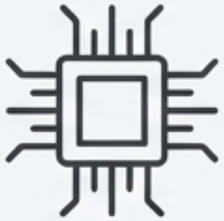
The Central Flaw: A Stolen Device Can Mean a Stolen PIN

Storing the PIN (or its hash value) entirely on the mobile device or SIM card creates a single point of failure. Physical access to the device gives a sophisticated attacker a direct path to uncovering the user's credentials.

Shoulder Surfing: Spying on users in public, often with cameras, to capture their PIN entry.

Malware: Infecting PTDs with viruses or Trojans that capture the PIN as it's typed and transmit it to the attacker.





Cracking/Scanning: Using computer programs to systematically attempt all possible PIN combinations.

Social Engineering: Tricking users into revealing their PIN under the guise of a legitimate request.

Current Security Measures are Cosmetic. A Surgical Approach is Needed.

The Cosmetic Approach
(The Status Quo)

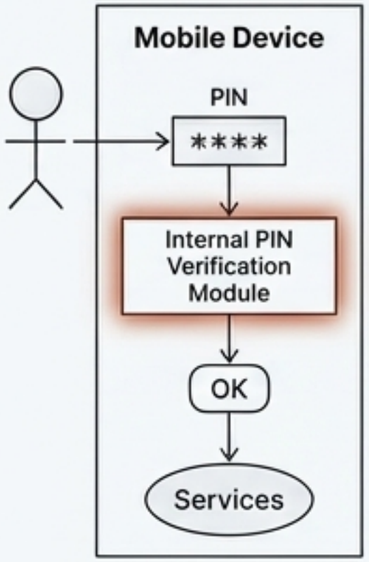
- **Philosophy:** Views the PIN as the smallest security unit. Focuses on using sophisticated methods to hide the *entire* PIN on the device.
- **Examples:** Storing the PIN in a "highly safe place" in memory, hashing the PIN into a non-reversible value.
- **The Weakness:** "Under our assumption that thieves nowadays become increasingly skillful in digging out a PIN in its entirety, cosmetic approaches are facing an unprecedented challenge."

The Surgical Approach
(The Proposed Shift)

- **Philosophy:** Views the PIN as divisible into smaller parts. Security is achieved by requiring all parts to be present for verification.
- **The Idea:** Distribute the PIN between the device and the network, fundamentally breaking the single point of failure.
- **The Advantage:** "Its safety measure incorporates probability, which is unbeatable by any skilled thief."

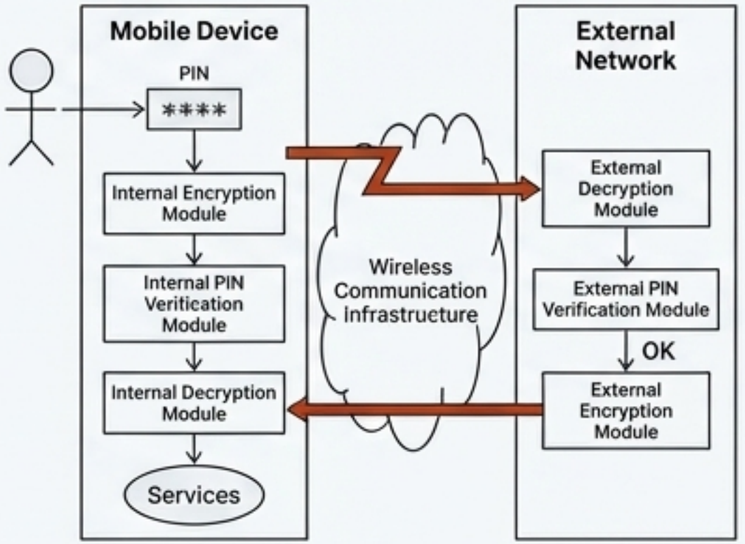
Three Architectures for PIN Verification

Scheme 1: Stored Entirely on Device



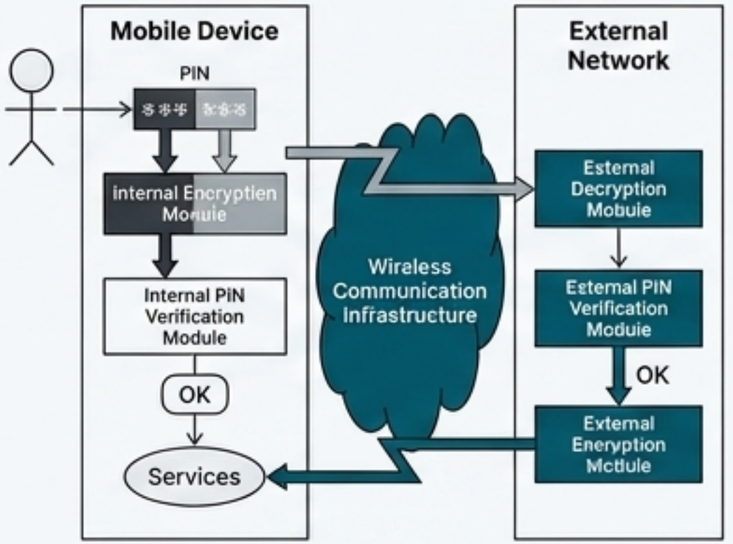
Current Standard. Simple and offline, but a single point of failure. If the device is cracked, the entire PIN is exposed.

Scheme 2: Stored Entirely on Network



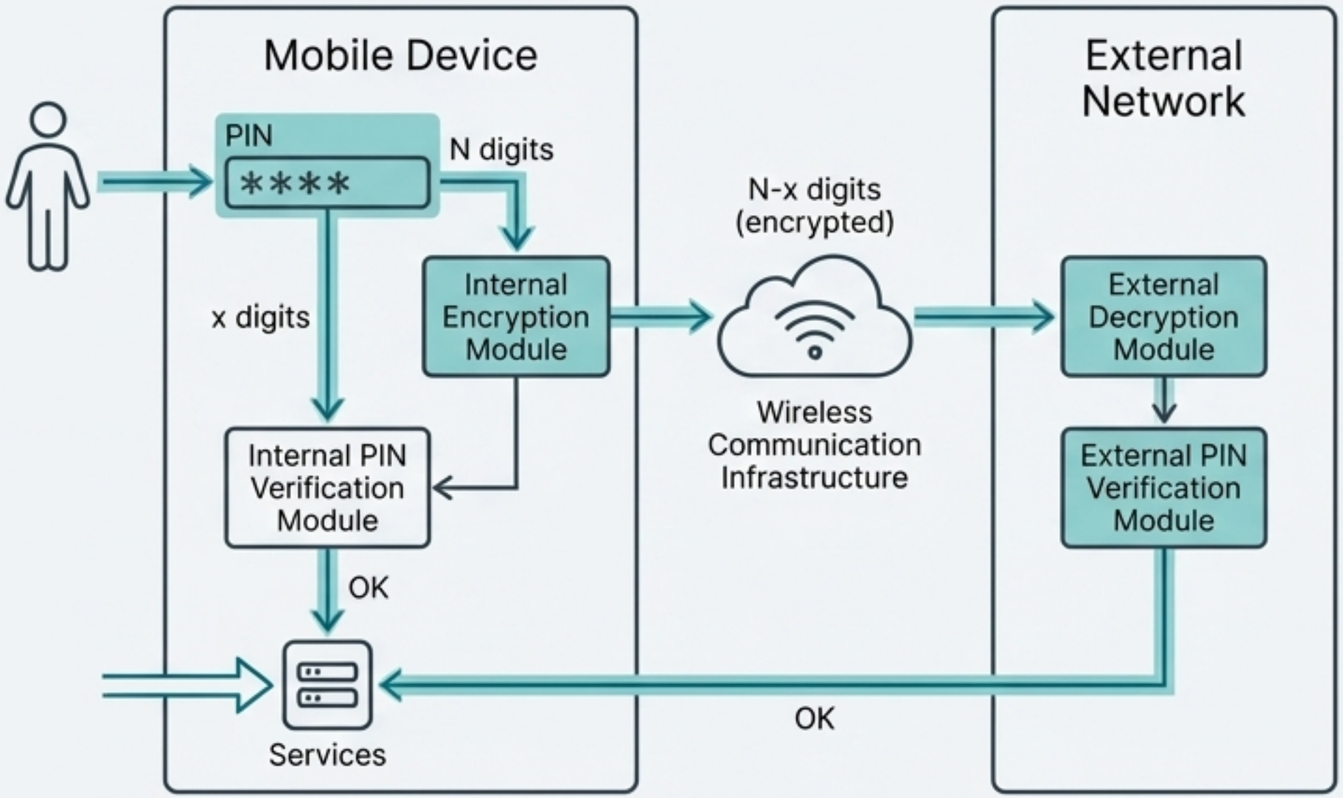
Network-Only. Removes the PIN from the device but creates a new risk: interception of the PIN in transit.

Scheme 3: The Distributed Scheme



Proposed Solution. The best of both worlds. An attacker must compromise two independent systems (device and network) to uncover the full PIN.

How the Distributed Scheme Achieves Dual-Factor Verification



1. **PIN Entry**
   User enters the full N-digit PIN into the mobile device.
2. **Internal Verification**
   The device's Internal Module verifies the first `x` digits of the PIN.
3. **Encrypted Transmission**
   The device encrypts the remaining `N-x` digits and sends them to the External Network for verification.
4. **External Verification**
   The External Module decrypts and verifies the `N-x` digits.
5. **Dual Confirmation**
   Access is granted *only if* the device receives a positive 'OK' from its internal check AND an encrypted 'OK' response from the external network.

> Key Insight: "Discovering the whole PIN requires digging and/or guessing two times independent of each other. The probability of this procedure to succeed is essentially [the] product of the probabilities of digging/guessing."

Quantifying the Risk: The Attacker's Probabilistic Hurdles

To evaluate the security benefit, we model the probability of an attacker succeeding. The total risk is a combination of several independent probabilities.

P_o 

Observation Risk

The probability of uncovering the entire PIN by observing the user (e.g., 'shoulder surfing"). This risk exists regardless of the storage scheme.

P_d 

Device Risk

The probability of a thief uncovering the `x` digits stored on the mobile device after it has been stolen.

P_n 

Network Risk

The probability of uncovering the `N-x` digits stored on the network, either through interception or by compromising the external server.

3×10^{-k}

Guessing Risk

The probability of correctly guessing a `k`-digit portion of the PIN within three attempts.

The Total Risk is a Product of Independent Vulnerabilities, Not a Sum

Attacker succeeds by simple observation.

Attacker compromises *both* the device and the network.

Attacker compromises the network and guesses the device device part.

$$P_f(P_0, P_d, P_n, N, x) = P_0 + (1 - P_0) \times$$

$$[P_d \cdot P_n + 3 \cdot P_n \cdot (1 - P_d) \cdot 10^{-x} + 3 \cdot P_d \cdot (1 - P_n) \cdot 10^{x-N} + 3 \cdot (1 - P_d) \cdot (1 - P_n) \cdot 10^{-N}]$$

Attacker compromises *both* the device and the network.

Attacker compromises the network and guesses the device part.

Attacker compromises the device and guesses the network part.

Attacker compromises neither and must guess the entire PIN.

Key Assumption: We assume that P_0, P_d, and P_n are independent of each other and of the length of the PIN.

The Optimal PIN Split is a Function of Relative Security

$$x_{\text{optimal}} = \frac{N}{2} + \frac{1}{2} \times \log_{10}\left[\frac{P_n \times (1 - P_d)}{P_d \times (1 - P_n)}\right]$$

`x` is the number of digits stored on the device that minimizes total risk.

Translating Math to Strategy

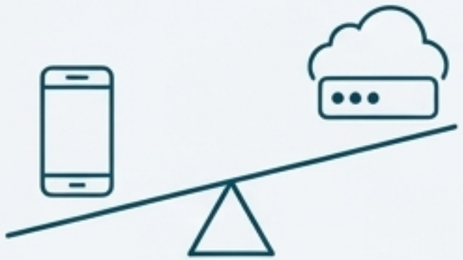
If Device and Network are Equally Secure ($P_d \approx P_n$)

The optimal split is "half-half" ($x \approx N/2$). For a 4-digit PIN, this is 2 digits on the device, 2 on the network.

If the Network is More Secure ($P_n < P_d$)

The logarithm is negative, so the optimal `x` is less than `N/2. More digits should be stored on the more secure network.

If the Device is More Secure ($P_d < P_n$)



The logarithm is positive, so the optimal `x` is greater than `N/2. More digits should be stored on the more secure device.

Rule of Thumb: Each magnitude of difference in `$c = P_n/P_d$` causes one digit to be moved from one place to another.

Measuring the Improvement: Defining the Security "Benefit"

Step 1: Establish the Baseline (Pbasic)

This is the risk of the current, device-only storage scheme (x=N).

$$P_{basic} = P_0 + (1 - P_0) \times [\, P_d + (1 - P_d) \times 3 \times 10^{-N} \,]$$

This formula represents the risk of observation, plus the risk of cracking the device, plus the risk of guessing if cracking fails.

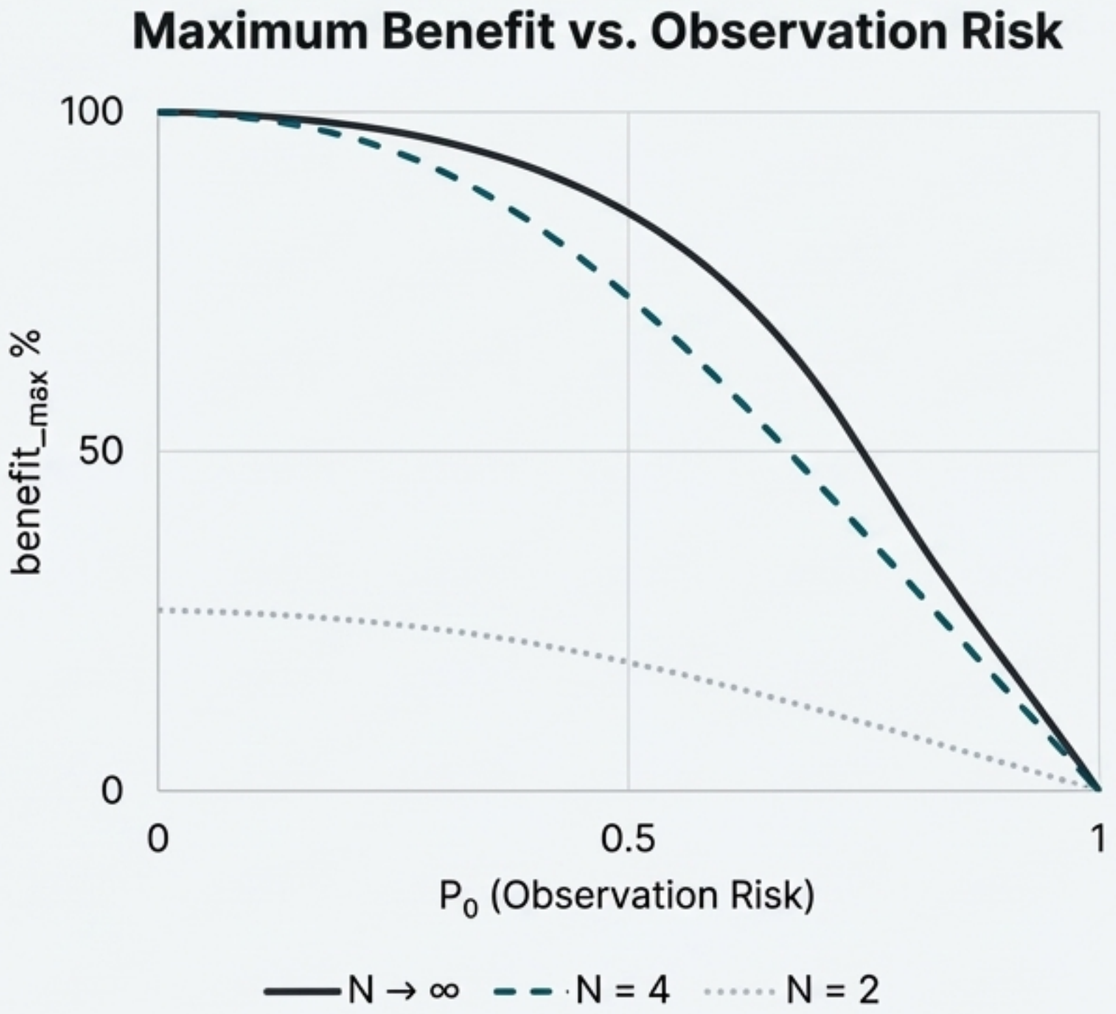
Step 2: Calculate the Benefit

The benefit measures the percentage reduction in risk achieved by the distributed scheme compared to the baseline.

$$\text{benefit} = \frac{P_{basic} - P_f}{P_{basic}} \times 100\%$$

Benefit = (Risk_Old - Risk_New) / Risk_Old

The Distributed Scheme Can Improve Security by Over 1000%



- **High Potential Gain**: For a 4-digit PIN where the device and network are equally secure ($c=1$), the maximum benefit is **90.86%** (an 11x improvement in security), assuming observation risk is negligible.
- **Resilience**: Even with a significant observation risk of $P_0 = 0.1$, a benefit of ~**45%** is achievable if $P_d = 0.1$.
- **The Decisive Factor**: The benefit is primarily driven by the ratio of P_d / P_0. A large security gain is achievable only if it is significantly easier to dig the PIN from the device than to get it through observation ($P_d > P_0$).
  - If P_d and P_0 are of the same magnitude, benefit is ~50%.
  - If P_d is 10x P_0, benefit is ~90%.

Key Takeaways for Maximizing Security

Distribution is Provably Superior: The distributed scheme is mathematically more secure than storing the PIN entirely on the device, especially when the risk of device compromise (Pd) is high.

Relative Security Dictates the Split: The optimal distribution of PIN digits is not arbitrary; it depends directly on the relative security of the device versus the network ($c = Pn/Pd$). A 'half-half' split is a robust default when this ratio is unknown.

Risk Cannot Be Eliminated, But It Can Be Minimized: The scheme's ultimate security is limited by the probability of observation (P_0) and pure guessing. The primary benefit is in reducing the risk from a stolen device down to this fundamental floor.

A Surgical Solution for a Systemic Vulnerability

The Problem

Storing PINs entirely on mobile devices is a fundamental architectural flaw, a “cosmetic” solution that fails against sophisticated threats.

The Solution

Distributing the PIN is a “surgical” fix. By requiring two independent systems for verification, it makes compromising the user’s identity exponentially more difficult for an attacker.

By separating the key from the lock, we create a system of distributed trust. This isn’t just a better way to store a PIN; it’s a more secure foundation for the future of mobile commerce.