TrustBound

Access exists only while trust exists.

Presence-bound access control · Zero Trust for the physical world

TrustBound makes access to critical systems exist **only while the right person is physically in the right room, on the right device — right now.** A stolen password, a stolen laptop, or a remotely hacked machine grant nothing, because trust is re-proven continuously and access renews only while presence holds.

THE PROBLEM

- ✕ Stolen credentials are the #1 cause of breaches — the login looks legitimate.
- ✕ A stolen or lost laptop keeps working anywhere.
- ✕ A remotely compromised device passes every check while an attacker sits inside.
- ✕ Sessions live for hours after the user has left.

THE SOLUTION

- ✓ Binds user + device + device health + location + physical presence.
- ✓ Access is a stream of ~10-second keys, renewed only while you stay.
- ✓ Critical actions require a physical human touch — impossible remotely.
- ✓ Least-privilege keys scoped to one resource, one action, short TTL.

HOW IT WORKS

GPS right building → **UWB beacons** right room → **Device chip** right laptop → **Human touch** you are here → **Key ~10s** access on

WHO NEEDS IT

Banks & fintech · Data centers · Critical infrastructure · Defense & government · R&D / IP · Healthcare

BUILT ON STANDARDS

`NIST SP 800-207` · `DoD Zero Trust` · `TCG TPM 2.0` · `IEEE 802.15.4z` · `PQC-ready`

WHY NOW

The network perimeter is gone, remote work is everywhere, and stolen access drives most breaches. Zero Trust is now mandated by NIST and the U.S. DoD — TrustBound is its **physical extension**: verifiable presence as a continuous factor of trust.

Concept by cybersecurity students at **Igor Sikorsky KPI** · team LeetSh4d0ws **leetsh4d0ws@gmail.com** · leetsh4d0ws.org/trustbound
— seeking pilots & partners