

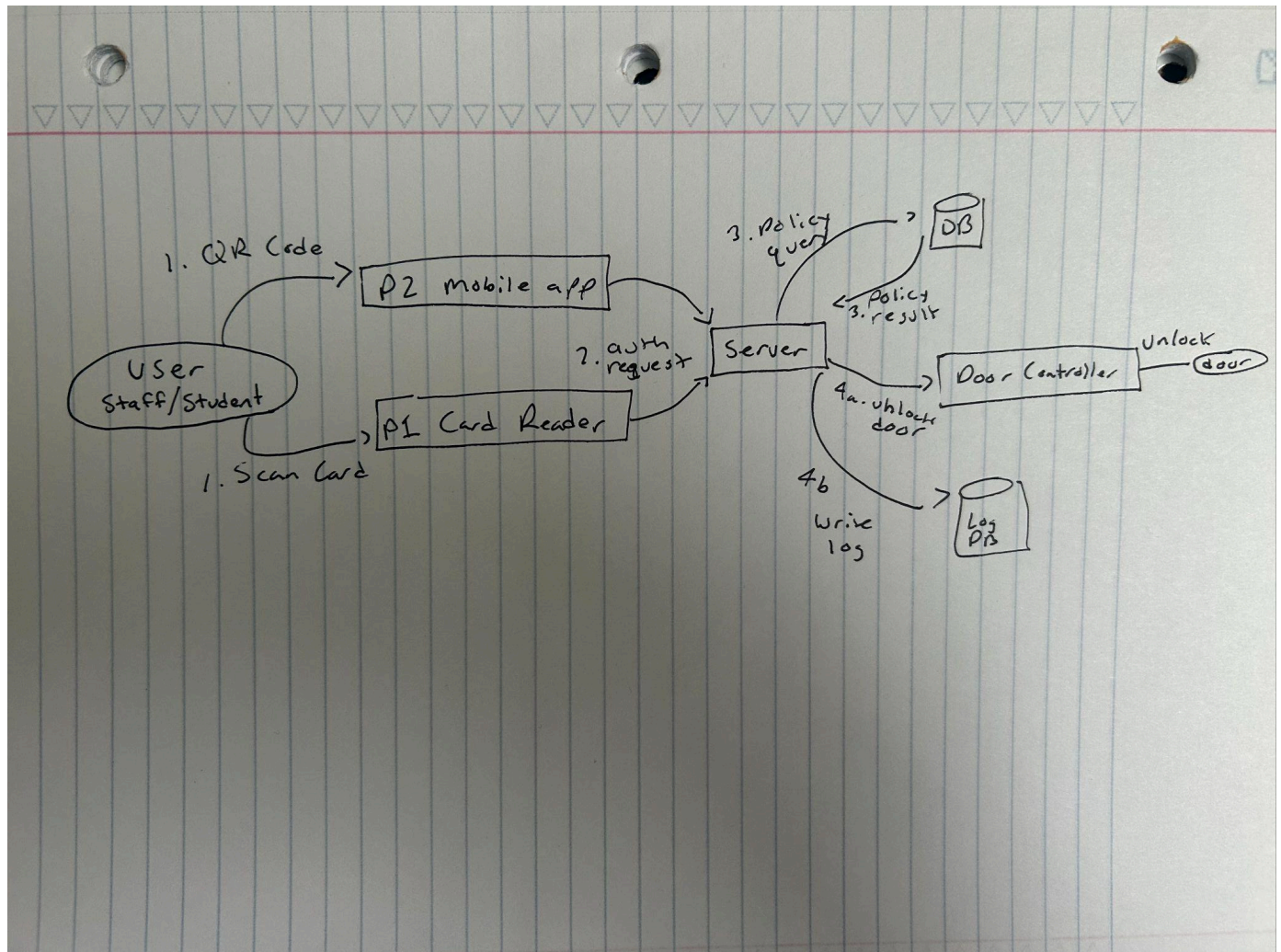
Scope: University campus access control for restricted areas (labs, server rooms, faculty offices).

Components: Card readers, mobile app, backend access control server, cloud database, IoT door controllers.

Flow: credential scan -> reader send auth to server -> server check policy against cloud
-> if authorized, door unlock and event logged

Critical Assets:

1. User credentials (card ID, QR tokens)
 - a. If cloned or stolen, attacker gains physical entry as a legitimate user
2. Access policy data (cloud DB)
 - a. Tampering would allow unauthorized access or locks out staff
3. Access event logs
 - a. Required for incident investigation and non-repudiation. Ensure timestamps are valid
4. Backend access control server
 - a. Compromise here would give an attacker access to all doors
5. IoT door controllers
 - a. Direct manipulation bypasses all upstream checks
6. Communication Channels
 - a. Interception or injection enables replay and spoofed unlocks
7. Mobile app QR generation
 - a. Flawed app would let attackers forge valid QR codes or re-use others QR codes



STRIDE Threat Identifications

T1. Card Reader

STRIDE - Spoofing

Attacker clones an RFID card and authenticates as a legitimate user

T2. Card Reader

STRIDE - Tampering

Physical tampering / skimmer attached to reader to harvest credentials

T3. Mobile App

STRIDE - Spoofing

Screenshot or replay of a QR code to impersonate a user

T4. Mobile App

STRIDE - Information Disclosure

Credentials stored unencrypted on device, extracted from lost/hacked phone

T5. Backend Server

- STRIDE - Elevation of privilege
Injection or auth-bypass flaw lets an attacker gain admin control of the access system
- T6. Backend Server
STRIDE - Denial of Service
DoS attack takes the server down and leaves no door usable
- T7. Cloud Database
STRIDE - Tampering
Unauthorized modification of access policies grants attacker access or revokes staff access
- T8. Cloud Database
STRIDE - Information Disclosure
Breach exposes access logs and would provide movement patterns of all staff and students
- T9. Backend
STRIDE - Repudiation
Attacker deletes or alters log entries (User denies having entered somewhere)
- T10. IoT Door Controller
STRIDE - Tampering
Command injection or malicious firmware causes controller to unlock on demand
- T11. IoT Door Controller
STRIDE - Denial of Service
RF jamming or network flooding disables the controller, leaving the door locked.
- T12. Communication Channel
STRIDE - Information Disclosure
MITM sniffing of communication between reader and server captures credentials in transit

DREAD Quantitative Risk

Rank	ID	Threat	D	R	E	A	Di	Risk	Level
1	T7	Policy tampering in Cloud DB	9	7	6	9	7	7.6	High
2	T5	Server privilege escalation	9	6	6	10	6	7.4	High

3	T10		8	8	6	6	7	7.0	High
4	T1		7	9	7	5	6	6.8	Medium
5	T6		5	7	5	8	7	6.4	Medium
6	T3		6	6	5	6	4	6.2	Medium
7	T12		6	5	4	7	4	5.4	Medium
8	T8		5	6	4	3	6	5.2	Medium
9	T2		4	7	5	3	5	4.8	Medium
10	T11		5	5	4	4	4	4.8	Medium
11	T4		5	5	4	4	4	4.4	Medium
12	T9		4	4	3	5	3	3.8	Low

Defense Plan

ID	Threat	Mitigation Strategy	MITRE Mitigation(s)
T7	Policy tampering	Least-privilege DB accounts, strict write permissions, continuous audit of policy changes	M1026 Privileged Account Management; M1022 Restrict File and Directory Permissions; M1047 Audit
T5	Server EoP	Patch management, input validation/exploit hardening, separate admin accounts with MFA	M1051 Update Software; M1050 Exploit Protection; M1026 Privileged Account Management

T10	Controller injection	Isolate IoT/OT network from campus LAN; verify signed firmware at boot	M1030 Network Segmentation; M1046 Boot Integrity; M1051 Update Software
T1	Card cloning	Require second factor (PIN/app confirmation) for high-security rooms; disable lost cards promptly	M1032 Multi-factor Authentication; M1018 User Account Management
T6	Backend DoS	Rate-limiting and traffic filtering at network edge; redundant server instances	M1037 Filter Network Traffic; M1031 Network Intrusion Prevention
T3	QR replay	Short-lived, single-use signed QR tokens; device-bound MFA	M1032 Multi-factor Authentication; M1054 Software Configuration
T12	MITM sniffing	TLS/mutual authentication on all reader-server-DB links	M1041 Encrypt Sensitive Information; M1031 Network Intrusion Prevention
T8	Log disclosure	Encrypt logs at rest, restrict access, monitor exfiltration	M1041 Encrypt Sensitive Information; M1057 Data Loss Prevention
T2	Reader tampering	Tamper-evident enclosures and alerts; restrict unauthorized hardware	M1034 Limit Hardware Installation (plus physical security controls, outside ATT&CK scope)
T11	Controller DoS	Segment and filter IoT network; define fail-secure behavior for critical doors	M1030 Network Segmentation; M1037 Filter Network Traffic

T4	App credential storage	Encrypt tokens on device (secure enclave/keystore); enforce credential policies	M1041 Encrypt Sensitive Information; M1027 Password Policies
T9	Repudiation	Ship logs in real time to append-only remote storage; regular audit review	M1029 Remote Data Storage; M1047 Audit

Conclusion

The system's risk concentrates in centralized components, like the cloud policy database and backend server, and the weakly protected IoT edge. The defense plan prioritizes privileged access control and auditing for the data tier, patching and exploit protection for the server, and network segmentation with boot integrity for door controllers, with multi-factor authentication and channel encryption to neutralize credential spoofing and interception.