

ACKNOWLEDGEMENTS

This thesis is the culmination of a reflection that would not have been possible without the support and guidance of many folks.

My deepest gratitude goes to my supervisor, Joëlle Bitton, for her invaluable insights, patience, and encouragement throughout this process. I could not have been assigned a better tutor.

I am profoundly thankful to all the participants and colleagues who generously shared their time and experiences for the field observations, surveys, discussions and interviews. Your stories and insights form the empirical heart of this research.

To my friends, especially Sander and Emma: thank you for your sincere support, for your incredible insights, and for giving me constructive criticism.

And finally, to my mother, Mulki ALI: thank you for supporting me throughout this entire process, and continuing to believe in me more than I believe in myself.

ABSTRACT

This thesis examines the act of logging in as a cultural and design practice that defines how people gain access, are recognized, and take part in digital systems. It approaches authentication as a site of negotiation between user and machine, drawing from interface theory, anthropology, and design history to trace its evolution. This trajectory reveals how login processes inherit older logics of verification and control while masking them under convenience. As authentication becomes externalized to devices and identity providers, users lose awareness of the systems that validate them. Through historical analysis, user studies and speculative prototypes, the research explores how “the login experience” could instead support user experience by making context, friction, and user participation central to the experience of recognition online.

TABLE OF CONTENTS

ACKNOWLEDGEMENTS	2
ABSTRACT	4
GLOSSARY	8
INTRODUCTION	12
MOTIVATION	17
BEGINNINGS OF LOGINS	25
First Ideas of Authentication	26
Tokens and Seals...?	28
Watchwords and Speech...!	30
Authentication is Social...	32
Bertillonage and Fingerprinting	34
Corbató and the Invention of Passwords	38
Socio-Technical Fragilities	40
From Passwords to Platforms	42
The Biometric Turn	46
A Reflection on the Design of Security	48
PROBLEMATIC: THE CONTEMPORARY CONDITION OF LOGIN	53
Interfaces and Sites of Production	54
Toward a Situated Design of Security	56

GLOSSARY

Because this research moves between computing, design, and philosophy, several terms require clarification. These definitions explain their words as I understand and use them throughout this thesis. They are not meant as universal truths, rather as working interpretations that situate the vocabulary of this research within the cultural and technical history of login.

Authentication is the process through which a system verifies a user's claim to identity, typically by testing a credential. It includes all processes through which an identity or ownership of an account are verified.

Identification is the first act of naming oneself before a system. It signals presence ("this is me") but not yet recognition. Identification precedes authentication, but together they form the process of entry.

Login, interpreted as "Connexion" in french, is the moment of passage into a digital environment, a process by which a user enters an authentication sequence to be recognised by a platform, device, or service. For me, "login" implies relation: a first exchange between human and system, a gesture closer to connexion than to verification. It is different from the act of authentication, due to the fact that this term only includes human-computer interactions. In that sense, this memoir is HCI research.

The externalisation of login describes the process through which authentication leaves its native platform and becomes distributed across other infrastructures. Through authenticator apps, passkeys, Single Sign-On systems, or biometric devices, recognition migrates toward third parties who guarantee trust on the platform's behalf. In this displacement, the act of entry becomes dependent on external institutions and technologies.

Liminality refers to the state of being in-between, neither fully inside nor outside. Borrowed from anthropological theory, it marks the threshold moment when users are suspended between access and denial, or self and system. Login inhabits this liminal zone, where recognition has not yet been granted but the gesture has already begun.

Alienation, or *aliénation*, describes the user's estrangement from the means and meanings of recognition. It appears when the ability to authenticate, and thus to appear before a system, belongs more to infrastructures that mediate on users' behalf, than to the people being identified themselves. Alienation manifests as frustration, opacity, and doubt about ownership; the unsettling question of whether one's account, data, or identity still belong to oneself. It is a source of frustration.

Trust, or "confiance" as I understand it in french, defines the dynamic relation of belief between user and platform. Both technical and affective, it can be engineered through interface design, reinforced through repetition, or betrayed through breach. Trust is what allows users to hand over their credentials despite knowing little of where or how they will be processed. It is, in short, the faith that the system will keep its promise.

Opacity names the opposite of transparency. It describes a system whose inner workings, decisions, and data flows remain hidden from the user. Opacity in login demands belief in the system's decisions rather than understanding, shaping interactions through secrecy. In the context of login, it is both a condition of security and a source of alienation or estrangement.

INTRODUCTION

Observe a familiar scene: a person stands before a door. They hold a key and attempt to enter: insert, twist, step through. Yet in our digital present, entry is neither simple nor singular. The key has multiplied. One key unlocks another; a code is sent elsewhere to an inbox or a phone; a fingerprint or face must confirm it; a secondary device must approve. What was once a straightforward threshold now unfolds as a distributed action, enacted across screens, devices, and platforms. This condition, which I call the externalisation of login, forms the first focus of this thesis.

Externalisation describes how authentication has migrated away from the immediate relationship between user and platform. To access one service, users must pass through another (Google Authenticator, Microsoft, Apple, SMS verification, recovery emails, or biometric prompts). Each intermediary extends the act of recognition outward, fragmenting it across corporate infrastructures that claim to simplify while quietly centralising control. The interface no longer belongs entirely to the designer or the user; its language and gestures are dictated by standards imposed from elsewhere.

This memoir begins with a simple question: what would the login experience look like if we designed it differently? To ask this is to challenge a fundamental pillar of digital life. We are taught that frustration is the necessary price of safety, and that opacity is a feature of security. Worse yet, users remain frustrated, and are faced with countless more steps to make them “feel more secure”, and yet few of the technologies employed inform users or succeed in enhancing users’ experiences. This relegates additional login steps to another daily chore that erodes patience and, ultimately, care for security itself. Users often make a rational rejection of security advice, when the costs outweigh the perceived benefits (Lazar et al., 2009). Making users care for their security is a step that matters as much as making them secure.

What remains of this act we perform daily, if we reconsider its defined protection? The answer, I propose, is that login reveals something deeper about how we are taught to appear before machines, in how we are trained to submit proof, how we internalise authority, and how we come to believe that friction equals safety.

Building on Alexander Galloway's notion of the interface as an agent of control and Arnold van Gennep's understanding of liminality, this thesis approaches login as a designed threshold that produces both subject and system. It does not simply connect the user to the system, more so that it produces the user, the system, and the world that both inhabit. The login, from this perspective, is a miniature apparatus of governance, defining who may enter, under what terms, and through which gestures of recognition. Following Wendy Hui Kyong Chun, I treat such interfaces as ideological performances that render invisible infrastructures of power into visible acts of participation. The login is therefore a checkpoint and a daily affirmation of faith in unseen systems that promise protection.

This thesis proceeds from three claims:

The login experience is a repetitive practice that, prior to entry, dictates part of users' feelings relating to the platforms they interact with.

The externalisation of login marks a political and aesthetic shift; trust is displaced from individual platforms toward corporate infrastructures, leading to a loss of design independence, as those external infrastructures impose a new design theme platforms struggle to clash with or implement.

Reimagining login requires an approach that questions its inheritances and imagines other modes of authentication, perhaps some that are more interactive or playful. The current login models can be improved upon.

From these claims emerge the guiding questions: What does login teach us about being a user in networked systems? Can login be redesigned as a moment of relation-building between user and platform? Can login have an additional layer of play added to its design?

To address these questions, this research combines theoretical inquiry with design practice. First, it offers a history of authentication, tracing its origins from ancient seals and watchwords to modern biometric and federated systems. Second, it performs critical interface analysis, drawing on semiotics, media theory, user surveys, field research and human-computer interaction to expose how login scripts behaviour and emotion. Third, it develops speculative prototypes, paper or virtual experiments that enact alternative logics of recognition, and tests to see how those first solutions interact with users.

To redesign login is to rethink how we enter the virtual world, a world increasingly organised by credentials, permissions, and proofs of identity. Any reimagining must begin by reclaiming login's lost spaces of relation. The goal is to highlight how secure interactions can feel legible and engaging without endangering safety: to design thresholds that express comprehension and play as part of protection.

My motivation for this research begins with how I, like many users, first experienced them.

MOTIVATION

The act of logging in has become one of the most repeated gestures of digital life. Each day, users identify themselves before machines, providing fragments of data to gain access to the spaces where they work, play, and communicate. These small gestures define the conditions under which people are recognized by their systems.

This project asks how such moments might be redesigned to create new relationships between users and platforms: ones that are proportional, contextual, and humane rather than standardized (and in worse cases, extractive of data, as some users worry about).

As two-factor authentication and verification apps appeared, access turned from invitation to obligation. CAPTCHAs cemented this change with a phrase both banal and profound:

“Prove you are human.”

This peculiar question hinted at a much greater problem. Is the wording correct? It seems a bit of a big ask to prove that I am a human. Is pattern recognition truly the sole thing that defines humans? Can I really only be identified through that?

Trivial in isolation, these questions revealed an emerging pattern. Many people seem to have experienced a fear of losing their accounts during recovery, the stress of Multi-Factor Authentication, and the struggles that come with changing and remembering passwords. For security’s sake, login needed to be complicated, and for security’s sake, human comfort was set aside. Some companies, like Google, publicly aim for a ‘passwordless future,’ pairing devices to a private key for a simpler and more secure sign-in (Google Safety & Security, 2023). But is getting rid of the password the sole solution? Bringing the login outside of its platform and making it dependent on devices creates more dependencies in other infrastructures.

Furthermore, this pursuit of frictionless, universal security often contradicts established guidelines, such as those from the National Institute of Standards and Technology (2024),

which emphasize that digital identity solutions must balance assurance levels with usability. The historical logic of using bodily metrics for identification, rooted in discriminatory practices like anthropometry, finds its echo in modern biometrics. These systems are not neutral; well-documented evidence shows they often fail on darker skin, meaning the very act of login can become a site of exclusion for some users. Adding to that material exclusion from people who lack the means to acquire a device with network access... The command to “prove you are human” then takes on a different, more charged meaning.

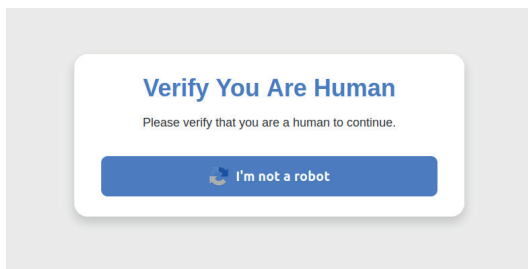
The issue is also not that security remains at the forefront, but that its language has been universalized: one corporate “design grammar” applied to every context, from banking to gaming. Anthropology and media theory help articulate this condition.

The notion of the threshold has long been associated with transformation. In *Les Rites de Passage* (1909), anthropologist Arnold van Gennep described thresholds as structured moments of transition that separate one social state from another. Victor Turner, writing in *The Ritual Process* (1969), expanded this idea through his concept of liminality: a temporary suspension of norms where identities are redefined.

In the digital era, media theorists such as Alexander R. Galloway (*The Interface Effect*, 2012) and Wendy Hui Kyong Chun (*Programmed Visions*, 2011) (who are great sources for me) shift this discussion from physical or social boundaries to computational ones. For Galloway, the interface is a site of protocol and control; for Chun, habitual interaction naturalizes that control into everyday behavior.

However, my approach is as constructive as it is critical. The role of designers in authentication is critical. It is important to create new design philosophies, relations and methods for the login process. Authentication is one of the most consequential interactions we have with today’s online platforms and devices, and should thus be situated in its context. A civic portal may justifiably demand identification through biometric data; a forum or game may not require such personal data. The same philosophy should not govern both.

Fig. 1 – “Verify You Are Human”
reCAPTCHA interface



Interviews with practitioners reinforced this view: one IT worker observed that identification processes (and their severity/complexity) expand whenever justification can be made. In a nutshell, the excuse of security becomes a slippery slope that creates a myriad of ways to “extract personal data” from users, as some put it during interviews. The same IT specialist suggested that “a good login should confirm ownership, not necessarily identity,” distinguishing transferable possession away from intrusive disclosures of the one’s private information.

My motivation is both analytical and propositional: to show how authentication has evolved into a universal checkpoint system, and to explore design alternatives that restore proportionality and meaningful reciprocity between users and platforms. The goal is not to sentimentalize login or aestheticize frustration, but to develop a framework: define context first, then design the relation of access it deserves.

Ultimately, this thesis speaks to two audiences. For theorists, it demonstrates how everyday interactions reproduce systems of recognition and exclusion. For designers, it provides tools to rethink authentication as a deliberate, situated, and reciprocal act.