Romantic Breakups as a Lens for Industrial Cybersecurity:
Cross-Domain Insights for Access Control

Team F, CompSci 261b

Caseysimone Ballestas
Bob Tianqi Wei
Subin Lee
Moritz Rietschel

RQ: **What gaps and differences in access control practices emerge from comparing digital disentanglement narratives in romantic breakups and industrial cybersecurity, and how can these insights improve industrial access protocols?**

Introduction

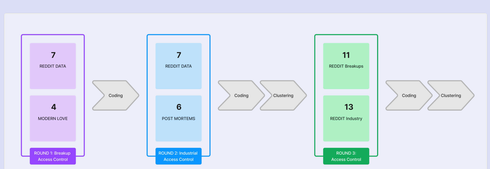
Industrial cybersecurity faces an urgent challenge: 30% of cyber breaches now occur through valid account misuse, representing a 70% increase in just one year [1]. Traditional technical solutions fail to address the more 'human' elements of access control, leading to significant financial losses. This research proposes looking at the problem through a new lens: examining industrial access control through the lens of romantic breakups —where complex digital disentanglement and access revocation also occurs, but under specifically emotional circumstances.

[1] IBM Security. (2024). X-Force threat intelligence index 2024. https://www.ibm.com/reports/threat-intelligence

Method

We used a **comparative grounded theory** approach to examine the processes of digital disentanglement across two contexts: *romantic access control* and *industrial access control*. This approach allowed us to iteratively develop theory while comparing patterns between these domains.

- **INDUSTRIAL ACCESS**
  - Official Post Mortem Reports
  - Reddit Posts
- **RELATIONSHIP ACCESS**
  - NYT's *Modern Love* Essays
  - Reddit Posts



Analysis Process

- Open and axial coding to develop core categories and identify shared and divergent themes
- Manual (re/)clustering of emergent patterns within each context
- Cross-context comparison

Super Cluster	Themes	Quote	Clusters Breakup	Description	Alignment?	Description	Clusters Industry	Quote
SYSTEM DESIGN including CREDENTIALS MANAGEMENT	Access Management				x	badge-based tracking systems and associated risks, such as misuse and manipulation.	**Physical Access and Spatial Layouts**	*"they are actively tracking ID card swipes (building access) to monitor if employees are coming in 2x days a week."*
		"I noticed today my ex has her location still shared with me. We both agreed to no contact last week to help us move on and until I have no romantic hopes left. Do I break no contact to tell her?"	**Decision-Making Moments in Access Changes**	moments of decision and contemplation regarding changes to access and boundaries.	x			
		"I just got out of an abusive relationship, and when I knew my ex would be out of the house yesterday, I went there to get some of my kids' belongings from their room."	**Coordinated Access Management**	intentional coordination in managing or sharing access rights, with strategic and mutual considerations.	x			
		"I looked at the list of devices that were currently logged in and I saw my own two devices, plus his ipad. I immediately deleted the device and changed my password."	**Technical Concerns in Access Systems**	technical issues and uncertainties in access control tools and systems.	x			
		"I'm still concerned about him because he is not that strong mentally and he was really devastated with us ending. In a way, this location is my way of checking if he's safe or if ever he needs help I can go to him immediately."	**Privacy and Location Sharing Decisions**	Deals with dilemmas in privacy and location sharing post-breakup.	x			
	Access Revoked	*"After 4 months post-breakup and 3 months post-NC, I finally did it. Emotional detachment."*	**Digital Separation and Access Termination**	milestones and struggles in disentangling shared digital access post-breakup.	x			
		"Anyway, I returned the key he gave me to his house. I grabbed some of my things and asked for my key back."	**Resolving Physical Access Permissions**	Covers challenges in managing physical access items like keys post-breakup.	x			
	Unauthorized Access and Response		**Access Boundary Violations**	deliberate attempts to breach access boundaries, often involving surveillance and unauthorized technical interventions.	✔	specific exploits' organizational or regional impacts.	**Exploits' Service Disruptions**	*"Between Thursday, 14 July 2022 21:57 US/Pacific and Friday, 15 July 12:40 US/Pacific, GCS customers may have experienced elevated latency, delays, issues importing, exporting or querying data from GCS buckets, and HTTP 500 errors in the Google Cloud regions of us-east1, southamerica-west1, and us-central2, and for buckets located in us-central1, us-east1, and nam4."*
					x	breach events from service failures to resolution, including attack methods.	**Lifecycle of Service Disruptions**	*"Google Cloud Networking experienced reduced capacity for lower priority traffic such as batch, streaming and transfer operations from 19:38 US/Pacific on Thursday, 14 July 2022, through 15:02 US/Pacific on Friday, 15 July 2022. High-priority user-facing traffic was not affected. This service disruption resulted from an issue encountered during a combination of repair work and a routine network software upgrade rollout. Due to the nature of the disruption and resilience capabilities of Google Cloud products, the impacted regions and individual impact windows varied substantially. To our customers whose businesses were impacted during this disruption, we sincerely apologize. This is not the level of quality and reliability we strive to offer you, and Service Disruption, Impact on we are taking immediate steps to improve the platform's availability. "*
					x	organizational impacts of ransomware and system-wide compromises.	**Comprehensive System Compromises**	*"My corporation has been completely shut down. Hackers have taken over our network."*
					x	privacy breaches, data exposure, and remediation efforts.	**Data Exposure and Privacy Breaches**	*"With the help of a viewer, we have discovered a major breach of privacy at a hardware vendor whereupon DN was able to download customer personal information, addresses, phone numbers, and also business-to-business invoices & orders."*
					x	incident tracking, response planning, and crisis management for operational security.	**Incident Documentation and Crisis Response**	*"Where we got lucky We were able to gather a list of affected Azure Active Directory accounts and their email addresses by searching for the "You've been removed from the "trivago N.V." organization" email on our Microsoft Exchange server. We also gathered a list of de-provisioned people from the Azure GitHub Enterprise Application integration from the Azure Active Directory log. GitHub automatically restores team and repository permissions and roles. The GitHub user account we use for syncing users between Azure Active Directory and GitHub was still part of the organization, had the owner role, and we could log in and restore organization administrative access for previous GitHub admins. External contributors haven't been affected because they are not required to log in via Single Sign-On."*
CONTINUOUS CONSIDERATIONS	Active Monitoring and System Upkeep	*"seemed to know things that I didn't remember telling him. But I thought I was just paranoid, surely there was some other explanation."*	**Persistent Monitoring and Surveillance**	motivations and methods of persistent monitoring across platforms.	✔	monitoring access, unauthorized behaviors.	**Access Monitoring**	*"My company is tracking badge swipes: how to request my data"*
		"Checking hisand out that he went several times to her house while we were dating, without telling me."	**Discovery of Concealed Activities**	uncovering hidden access activities, infidelities, and deceptive patterns.				
					x	technical improvements, such as debugging, network isolation, and monitoring.	**Technical Infrastructure Resilience**	*"Improve dashboards that help debugging global- and domain-level control failures and configuration status."*
	Rules and Norms	*"He is not going to make that easy because he claims we were common law married (this is shaky and not likely to hold up in court, but it will allow him to jerk me around for a while and stay in my home rent-free, which is pretty much his goal in life)."*	**Rules and Norms Governing Access Control**	formal and cultural rules that shape decisions on access control and blocking.	✔	dynamics between policies, informal behaviors, and compliance within organizational and legal frameworks.	**Policy and Compliance Dynamics**	*"And I make a point of badging in more than once when I'm in. So lazy counts of the numbers of badge-ins don't flag me as a problem. This part requires a bit of malicious compliance by the department As. "*
	Socio-Emotional Impacts				x	vulnerabilities caused by insufficient training and risky behaviors in high-privilege contexts.	**Security Weaknesses and Training Gaps**	*"You're given minimal training. It is expected to be security and fire watch, forgotten about when it comes to anything to with safety and training. I worked at a plant that literally everyone there had to have at least minimal fire fighting training. Had to wear FR clothing to be past the gates and be certified in how to use an SCBA. While we were never trained how to ID any chemicals if they were leaking, forced to wear flammable polyester uniforms in the plant and got no training."*
		"Do you delete pictures of your ex when it's over?"	**Managing Digital Memories**	dilemmas and decisions about preserving or deleting digital memories.	x			
		"He broke up with me cultural reasons and that he 'lost the spark.'"	**Relationship Termination Contexts**	breakup or separation events that drive changes in access rights or boundaries.	x			
		"It sent me spinning and ng ALL the progress I've made."	**Emotional Responses and Access Changes**	emotional triggers to access-related behaviors, including regrets and reactive blocking.	x			
			Privacy Violations and Emotional Impact	emotional distress caused by privacy breaches, especially when unaddressed.	x			
		"I was blindsided and left alone after a five year relationship."	**Shared Resources and Relationship Investments**	complications from shared assets and relationship-related investments.	x			

GOAL: Derive novel insights for industrial access control system design by analyzing digital asset management during romantic breakups.

Findings

Gaps and Alignments:
Despite differing contexts, we found evidence of shared features in how access control is perceived and enacted on nearly all thematic levels. This alignment suggests that fundamental principles of access control transcend domains.

Differences:
The themes did not frequently align on a one-to-one basis at the domain-specific clustering level. This divergence may indicate:

- how people discuss these issues in public forums, may be influenced by emotional, technical, or cultural factors.
- either there is a cultural avoidance of discussing *access management* and *access revocation* in the industry remembering, or this is an under evaluated area of access control (possibly because of threat of legal recourse looming larger in industry than breakups)

Implications for Industrial Access Design:
Insights from emotional and relational contexts could inform the design of more human-centered and adaptable industrial access control systems, addressing both technical and interpersonal dimensions.

Next Steps

Translating gaps and alignments into design heuristics for industrial access control, focusing on themes that were less common in industrial access control data: *access management*, *access revocation*, and *socio-emotional impacts*.