When Security Becomes a Burden

Understanding and Dealing with Security Policy Fatigue

Dr. Anatoli Kalysch

June 27th, 2025

2nd Semester DIS
HAW Ansbach

whoami

- Science
  - Associated Postdoc @ FAU (Focus: Mobile Security, IT-Forensics, Reverse Engineering)
  - Lecturer (Focus: Mobile Application Security, Cyber Security)
  - Conference reviewer (Focus: Mobile Security, Malware Analysis, Reverse Engineering)
- Industry
  - Penetration tester (Focus: Mobile & Backend Pentesting for Fintech & Insurance)
  - Co-Founder @ TALOS Insights GbR (Focus: NLP, Serverless, IP & Competitive Intelligence)
  - Senior Information Security Officer & deputy @ CSO Taurus SA (Focus: GRC, Incident Response & TPRM)
  - Chief Information Security Officer @ DB Connect GmbH (Focus: GRC, TPRM & Vulnerability Research)

Security Policy Fatigue

01 **Takeaways**

What is important today?

02 **Motivation**

Information overload by design?

03 **Introduction**

What is security fatigue (SF) and what are the causes?

04 **Tailoring Information**

But to what context? Roles, organizations, and individuals

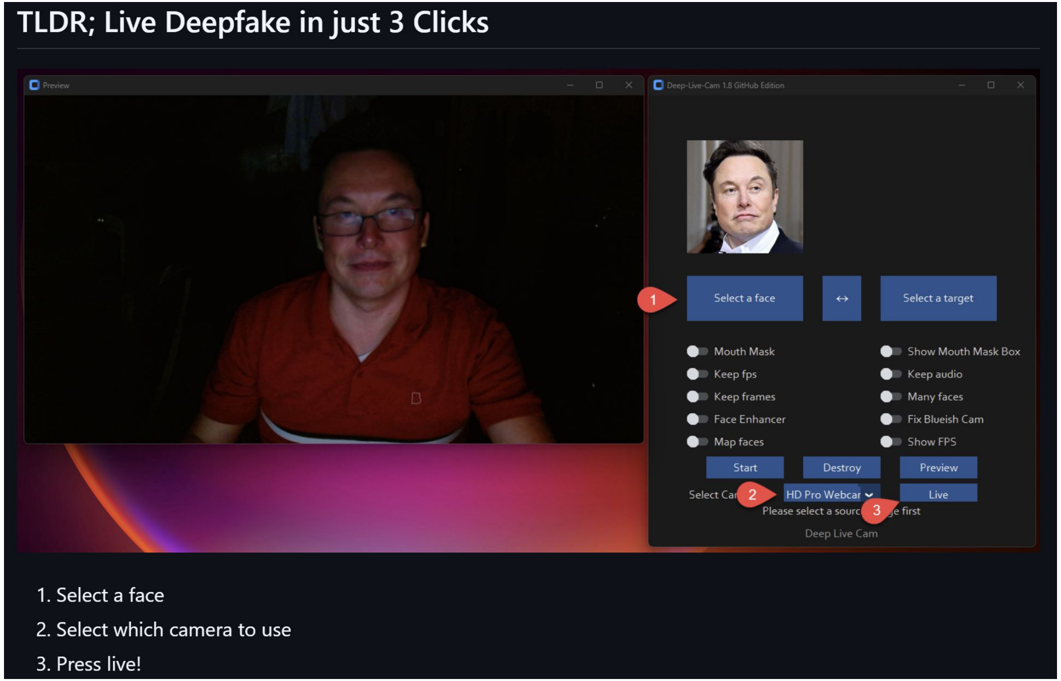
05 **Discussion**

Open questions

Best-Case takeaways

- What is (information) security fatigue
  - What are the causes and symptoms?
  - What does it lead to?
- Understand the broader context of security organizations
  - Why is SF (probably) going to stick around with us for the time being?
  - If we can't completely resolve it, can we alleviate it?
- Security landscape is currently **shifting**

Best-Case takeaways



TLDR; Live Deepfake in just 3 Clicks

1. Select a face
2. Select which camera to use
3. Press live!

Taken from https://github.com/hacksider/Deep-Live-Cam

What is the scope of today’s security & privacy requirements?

Framework	Scope
ISO 27001:2022	More than 40 requirements in ch. 4-10, and 93 controls in annex A.
NIST CSF / NIST SP 800-53	CSF: 5 Functions, more than 100 subcategories; SP 800-53: 20 Control families, over 1k controls
Selected EU requirements	DORA: Over 70 requirements across all Articles; NIS2: [7]
GDPR	Requirements outlined in 99 Articles and all necessary TOMs.
BSI-IT-Grundschutz	More than 100 ‘Bausteine’ with 5 - 15 requirements each.

Quellen: [1] - [7]

A match made in heaven: layer 8 and cyber security

- How much of actual knowledge is arriving where the ‘grunt work’ is happening?
  - Ever skipped a mandatory password reset?
  - Ever been tailgated?
  - Ever read the security policies of a company you worked / did an internship with?
- “Einführung in die IT-Sicherheit” introduced the Human in the loop in cyber security
  - But how does the human know what’s expected?
  - And more importantly, do humans in different departments understand the same things?
- Security policy fatigue is exactly this, “a socio-emotional state in which an individual becomes tired and disillusioned with security policy requirements”. [9]

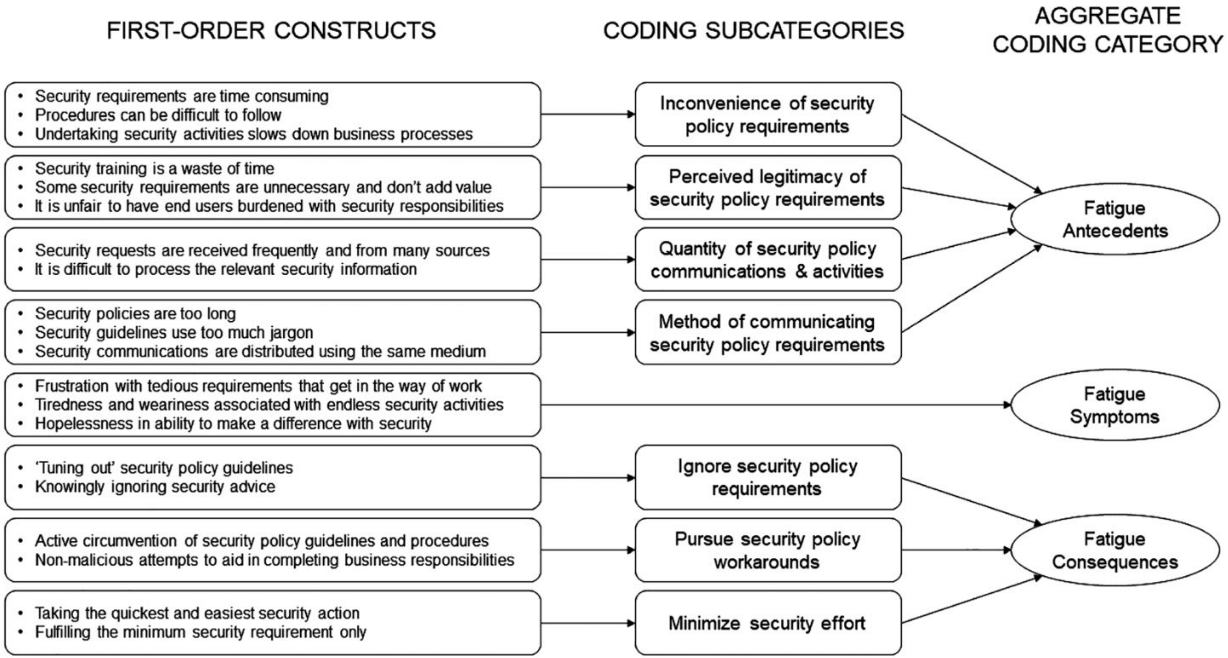
Quellen: [9], [13]

Psychological bias - Different kinds of fatigue

- Decision Fatigue [9]
    - The more decisions you make in a day the worse they get [15]
- Information Overload & Habituation [9, 14]
    - Cognitive overload leads to habitual clicking [14]
- Alert Overload [9, 12]
    - XDR / AV pop-ups [14]
    - Phishing mail detection / External sender notifications
- Friction cost of security [12, 14]
    - MFA, esp. bad FRR

Quellen: [9, 12, 14, 15]

Psychological bias - Different kinds of fatigue



FIRST-ORDER CONSTRUCTS

CODING SUBCATEGORIES

AGGREGATE CODING CATEGORY

- Security requirements are time consuming
- Procedures can be difficult to follow
- Undertaking security activities slows down business processes

→ Inconvenience of security policy requirements → Fatigue Antecedents

- Security training is a waste of time
- Some security requirements are unnecessary and don't add value
- It is unfair to have end users burdened with security responsibilities

→ Perceived legitimacy of security policy requirements → Fatigue Antecedents

- Security requests are received frequently and from many sources
- It is difficult to process the relevant security information

→ Quantity of security policy communications & activities → Fatigue Antecedents

- Security policies are too long
- Security guidelines use too much jargon
- Security communications are distributed using the same medium

→ Method of communicating security policy requirements → Fatigue Antecedents

- Frustration with tedious requirements that get in the way of work
- Tiredness and weariness associated with endless security activities
- Hopelessness in ability to make a difference with security

→ Fatigue Symptoms

- 'Tuning out' security policy guidelines
- Knowingly ignoring security advice

→ Ignore security policy requirements → Fatigue Consequences

- Active circumvention of security policy guidelines and procedures
- Non-malicious attempts to aid in completing business responsibilities

→ Pursue security policy workarounds → Fatigue Consequences

- Taking the quickest and easiest security action
- Fulfilling the minimum security requirement only

→ Minimize security effort → Fatigue Consequences

Quellen: [9]

Are we doing security wrong?

- Fast-paced development of attacks & defenses
- Fast-paced development of the regulatory landscape (see slide 6)
- Fast-paced development of the company’s own risk perception
- Fast-paced development of the workforce makeup [15]
- … contrast that with our policy design speed and awareness trainings

Quellen: [15, 17, 18]

Not all is lost - but communication must be tailored!

- Automation [19]
  - AI [19], Micro-learning and mobile-first approaches [15]

- Stakeholder communication
  - Role-based adaptive learning [20] -> tailor your content
  - Foster resilience [18] -> adapt to emotional load of the role
  - Risk profiles and exposure [16] -> monitor risk levels

- Simplify Policies with Built-in Checks [17]

Quellen: [16 - 20]

THANK YOU!

Questions? Feedback?

anatoli@kalysch.com

Literatur

[1] ISO/IEC. ISO/IEC 27001:2022 — Information security, cybersecurity and privacy protection — Information security management systems — Requirements. International Organization for Standardization, Geneva, 2022.

[2] National Institute of Standards and Technology. Security and Privacy Controls for Information Systems and Organizations. NIST Special Publication 800-53 Rev. 5, U.S. Department of Commerce, Gaithersburg, MD, 2020.

[3] National Institute of Standards and Technology. Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. NIST, Gaithersburg, MD, 2018.

[4] Center for Internet Security. CIS Controls v8. https://www.cisecurity.org/controls/, 2021.

[5] European Commission. Regulation (EU) 2022/2554 on Digital Operational Resilience for the Financial Sector (DORA). Official Journal of the European Union, Dec. 2022.

[6] European Commission. Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2). Official Journal of the European Union, Dec. 2022.

[7] Bundesamt für Sicherheit in der Informationstechnik. IT-Grundschutz-Kompendium, Edition 2023. BSI, Bonn, 2023.

[8] European Cyber Security Organisation. NIS2 Directive Transposition Tracker. https://ecs-org.eu/activities/nis2-directive-transposition-tracker/, accessed June 25, 2025.

Literatur

[9] A. Cram, D. Proudfoot, and M. D'Arcy. Organizational security policy noncompliance: A behavior modeling perspective. Information Systems Journal, vol. 30, no. 3, pp. 528–562, 2020. https://doi.org/10.1111/isj.12284 .

[10] J. Ophoff and A. Cram. Risk homeostasis and security fatigue: A case study of data specialists. Information and Computer Security, vol. 30, no. 4, pp. 593–611, 2022. https://doi.org/10.1108/ICS-11-2022-0172 .

[11] M. Stanton, K. Stam, and B. Mastrangelo. An Analysis of End User Security Behaviors. Computers & Security, vol. 68, pp. 16–29, 2017. https://doi.org/10.1016/j.cose.2017.03.002 .

[12] J. D'Arcy and P.-L. Teh. Predicting employee information security policy compliance on a daily basis: The interplay of security-related stress, emotions, and neutralization. Information & Management, vol. 56, no. 7, 2019. https://doi.org/10.1016/j.im.2019.02.006 .

[13] S. M. Furnell and K.-L. Thomson. From culture to disobedience: Recognising the varying user acceptance of IT security. Computer Fraud & Security, vol. 2009, no. 2, pp. 5–10, Feb. 2009. https://doi.org/10.1016/S1361-3723(09)70019-1.

[14] Körber, M., Kalysch, A., Massonne, W., & Benenson, Z. (2022, June). Usability of Antivirus Tools in a Threat Detection Scenario. In IFIP International Conference on ICT Systems Security and Privacy Protection (pp. 306-322). Cham: Springer International Publishing https://link.springer.com/chapter/10.1007/978-3-031-06975-8_18 .

[15] T. Aoun, S. F. Dabbous, and J. Makhoul. “Investigating Security Fatigue: The Role of Digital Natives in Cybersecurity Compliance,” Sage Open, vol. 11, no. 3, 2021. https://doi.org/10.1177/21582440211000049 .

[16] J. A. Jacobsen. “Exploring the Relationship Between Cybersecurity Overload and Employee Well-being: A Mixed Methods Study,” Massey University Research Bank, 2020. https://hdl.handle.net/10.26021/9846502e-9e1d-42bb-8efc-c317659e1ddd .

Literatur

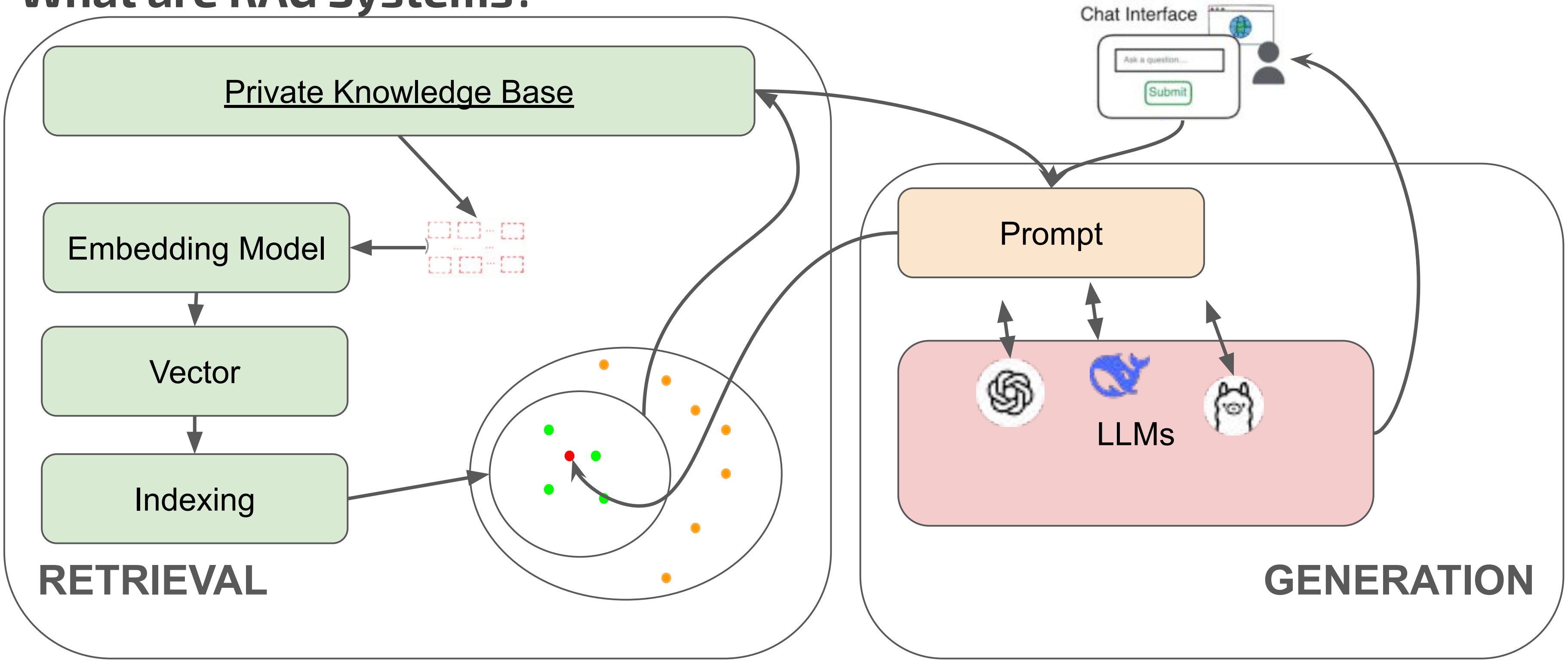
[17] L. Kirchner and R. Schreck. “Designing Fatigue-Resistant Security Policies,” in Proceedings of the 2023 ACM Conference on Computer and Communications Security (CCS), Adelaide, Australia, pp. 512–526, 2023. https://doi.org/10.1145/3627043.3659569 .

[18] M. McIlwraith and E. Freeman. “Psychological Perspectives on Security Compliance: Managing Fatigue and Stress,” Journal of Health Psychology, vol. 24, no. 6, pp. 789–802, 2019. https://doi.org/10.1177/1359105318763510 .

[19] F. H. Smith and G. Patel. “Automated Security Awareness to Combat Human Fatigue,” 2016 IEEE Symposium on Technologies for Homeland Security (HST), pp. 1–6. https://doi.org/10.1109/THS.2016.7579112 .

[20] S. Wagner, J. Ritz, and B. Müller. “Adaptive Security Training: Balancing Education and Overload,” in *Cybersecurity Education and Technology: Methods and Practices*, Springer, pp. 235–252, 2021. https://doi.org/10.1007/978-3-030-50309-3_15 .

What are RAG Systems?


Private Knowledge Base
Embedding Model
Vector
Indexing
RETRIEVAL
Chat Interface
Ask a question...
Submit
Prompt
LLMs
GENERATION