



The weakest link, and other myths
about
the **human in the loop**:
a **socio-technical understanding**
of **security** in critical situations

IFIP Working Group 10.4
Ischia 28 June 2025

Gabriele Lenzini





IFIP TC 11 Working Group 12 - Human Aspects of Information Security and Assurance

TC11: Security and Privacy Protection in Information Processing Systems

- WG 11.2: Pervasive Systems Security
- WG 11.3: Data and Application Security and Privacy
- WG 11.4: Network & Distributed Systems Security
- WG 11.6: Identity Management
- WG 11.7: Information Technology: Misuse and The Law (joint with WG 9.6)
- WG 11.8: Information Security Education
- WG 11.9: Digital Forensics
- WG 11.10: Critical Infrastructure Protection
- WG 11.11: Trust Management
- WG 11.12: **Human** Aspects of Information Security and Assurance

TC 13: Human-Computer Interaction

- WG 13.2: Methodology for User-Centered System Design
- WG 13.5: Human Error, Safety and System Development
- WG 13.6: Human Work Interaction Design
- WG 13.7: Human-Computer Interaction & Visualization
- WG 13.8: Interaction Design and International Development

TC 14: Entertainment Computing

- WG 14.4: Entertainment Games

Background in Formal Methods

Sociotechnical Cybersecurity

Systems that hide design flaws, puzzle users, or fail to implement requirements remain exposed to misuses and cyberattacks.

Research

Partners

SNT
securityandtrust.lu



“A socio-technical system has both human and technical components working together to achieve production tasks, as well as achieving the enabling task of securing that system effectively”

Flechais, I., Riegelsberger, J., & Sasse, M. A. (2005). Divide and Conquer: The Role of Trust and Assurance in the Design of Secure Socio-technical Systems

the exotic fruit in the menu



the exotic fruit in the menu



Belly landing, when aircraft
lands without extending
completely its gears





It's ungood !

Damages the aircraft extensively, with risk of flip over or disintegration.

Jeju airplane disaster, South Korea 2024

Causes and prevention [\[edit \]](#)

Pilot error [\[edit \]](#)

The most common cause of gear-up landings is the pilot simply forgetting to extend the landing gear before touchdown. On any retractable gear aircraft, lowering the landing gear is part of the pilot's landing checklist, which also includes items such as setting the flaps, propeller and mixture controls for landing. Pilots who ritually perform such checklists before landing are less likely to land gear-up. However, some pilots neglect these checklists and perform the tasks by memory, increasing the chances of forgetting to lower the landing gear. Even careful pilots are at risk, because they may be distracted and forget to perform the checklist or be interrupted in the middle of it by other duties such as collision avoidance or another emergency. In the picture shown above, the B-17 Dutchess' Daughter had landed normally, when the copilot inadvertently flipped the landing gear switch to retract. The gear collapsed near the end of the landing roll.^{[\[3\]](#)}



A [C-17 Globemaster](#) after a belly-landing at [Bagram Airfield](#), Afghanistan (2009). The cause of this was later determined to be pilot error.^{[\[1\]](#)[\[2\]](#)}

Causes and prevention [\[edit \]](#)

Pilot error [\[edit \]](#)

landing. Pilots who ritually perform such checklists before landing are less likely to land gear-up. However, some pilots neglect these checklists and perform the tasks by memory, increasing the chances of forgetting to lower the landing gear. Even careful pilots are at risk, because they may be distracted and forget to perform the checklist or be interrupted in the middle of it by other duties such as collision avoidance or another emergency. In the picture shown above, the B-17 Dutchess' Daughter had landed normally, when the copilot inadvertently flipped the landing gear switch to retract. The gear collapsed near the end of the landing roll.^[3]

determined to be pilot error.^{[1][2]}

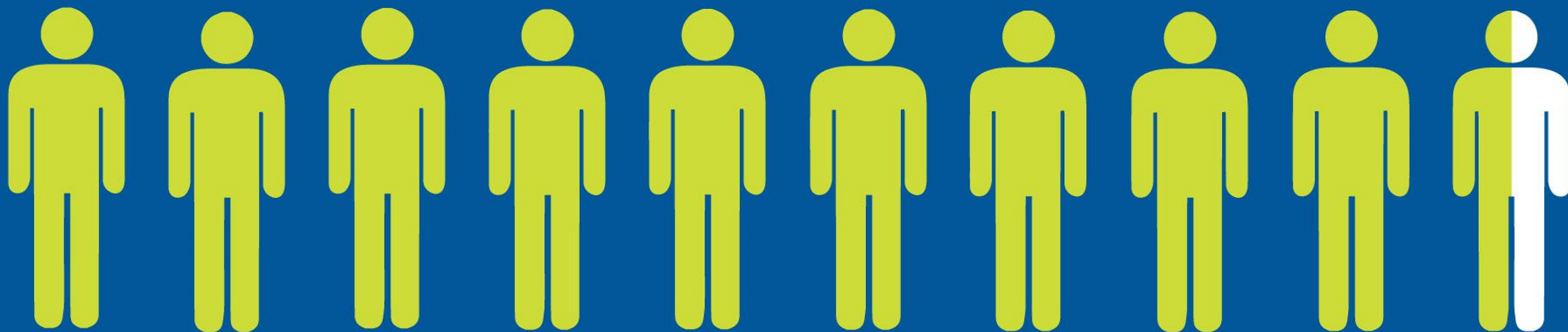
It rings a bell

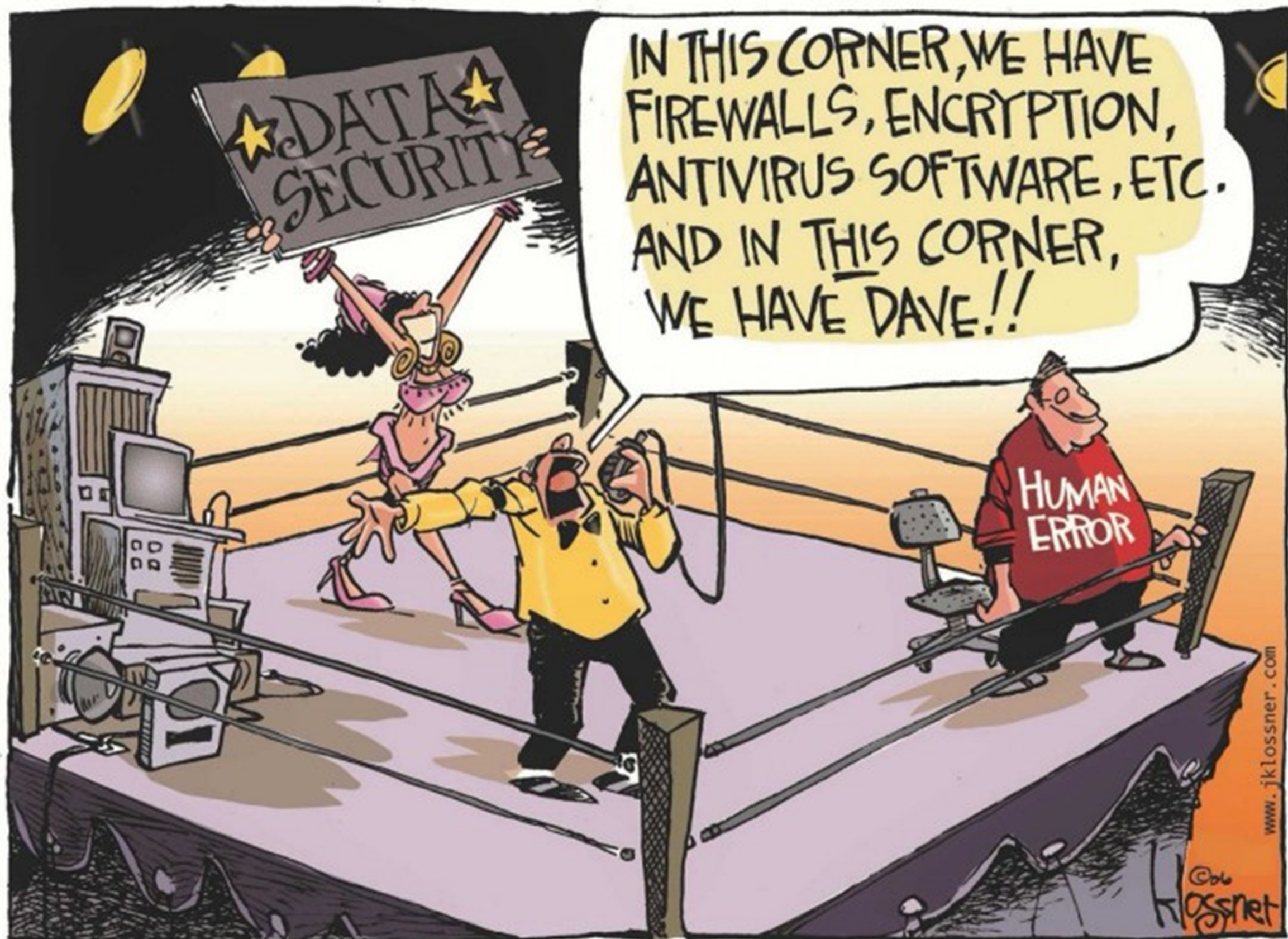


95%

of all successful cyber attacks
is caused by human error

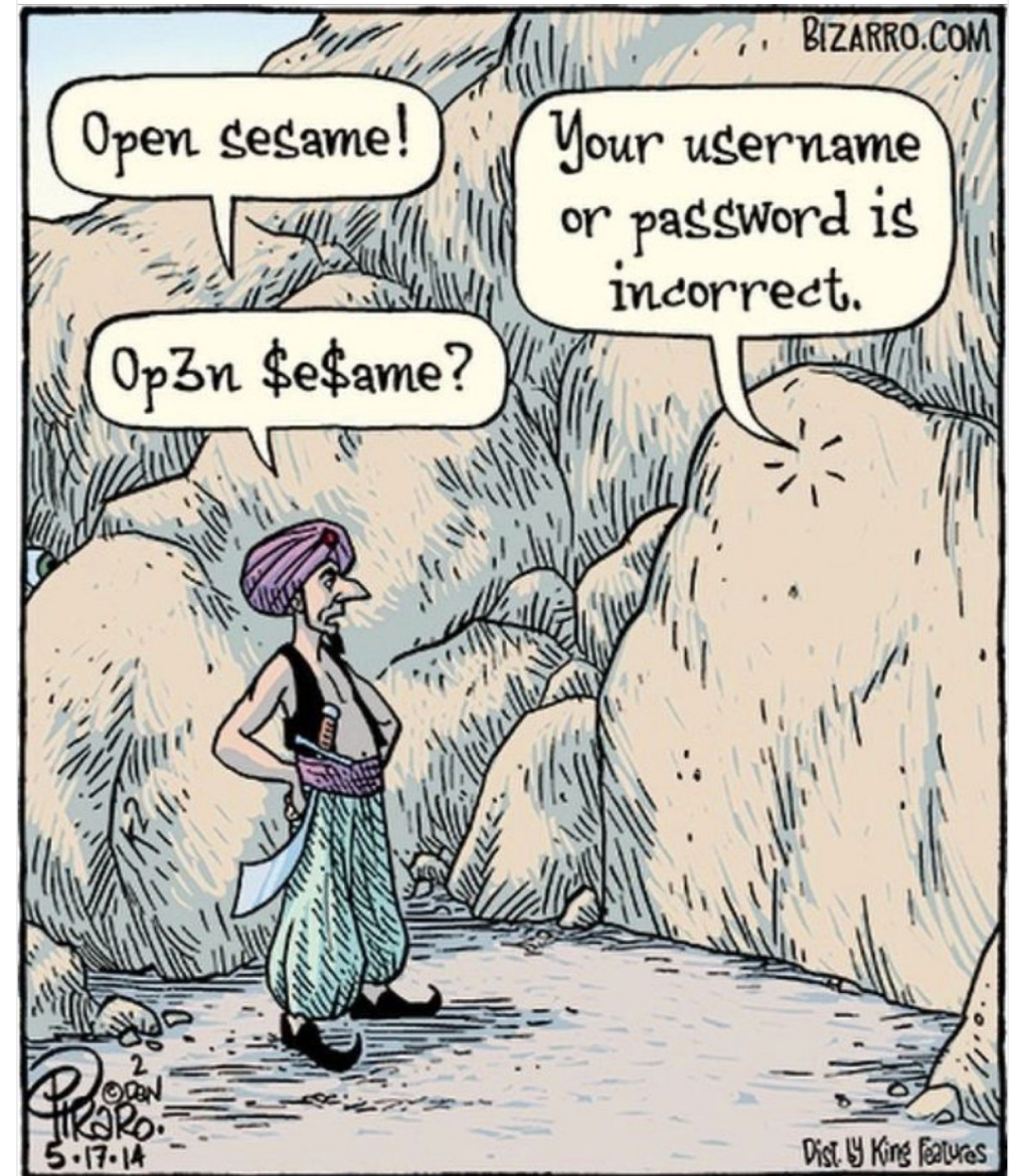
Source: IBM Cyber Security Intelligence Index





.. as with Passwords ..

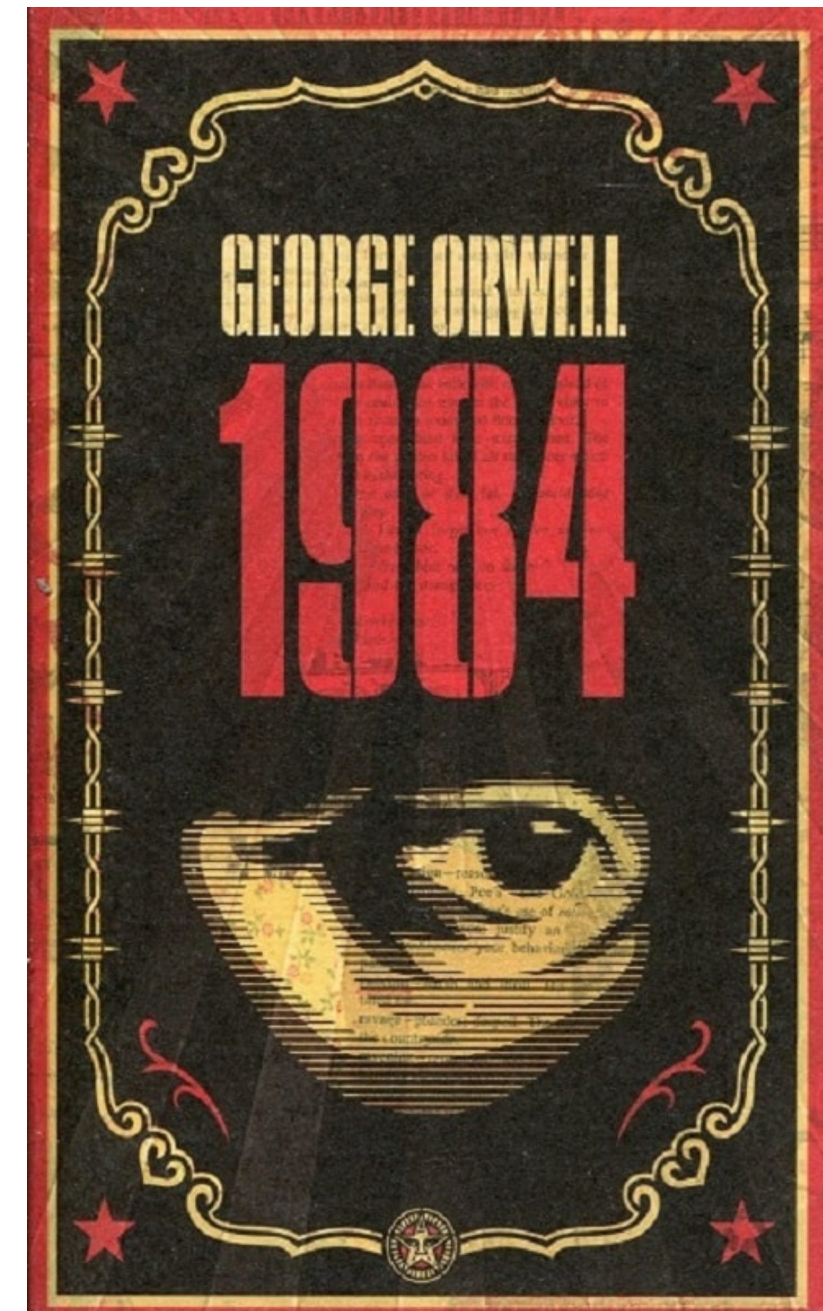
.. people failing to create strong or remembering them



Newspeak

In the end the whole notion of
[goodness and badness] will be covered
by [...] only one word: [good]

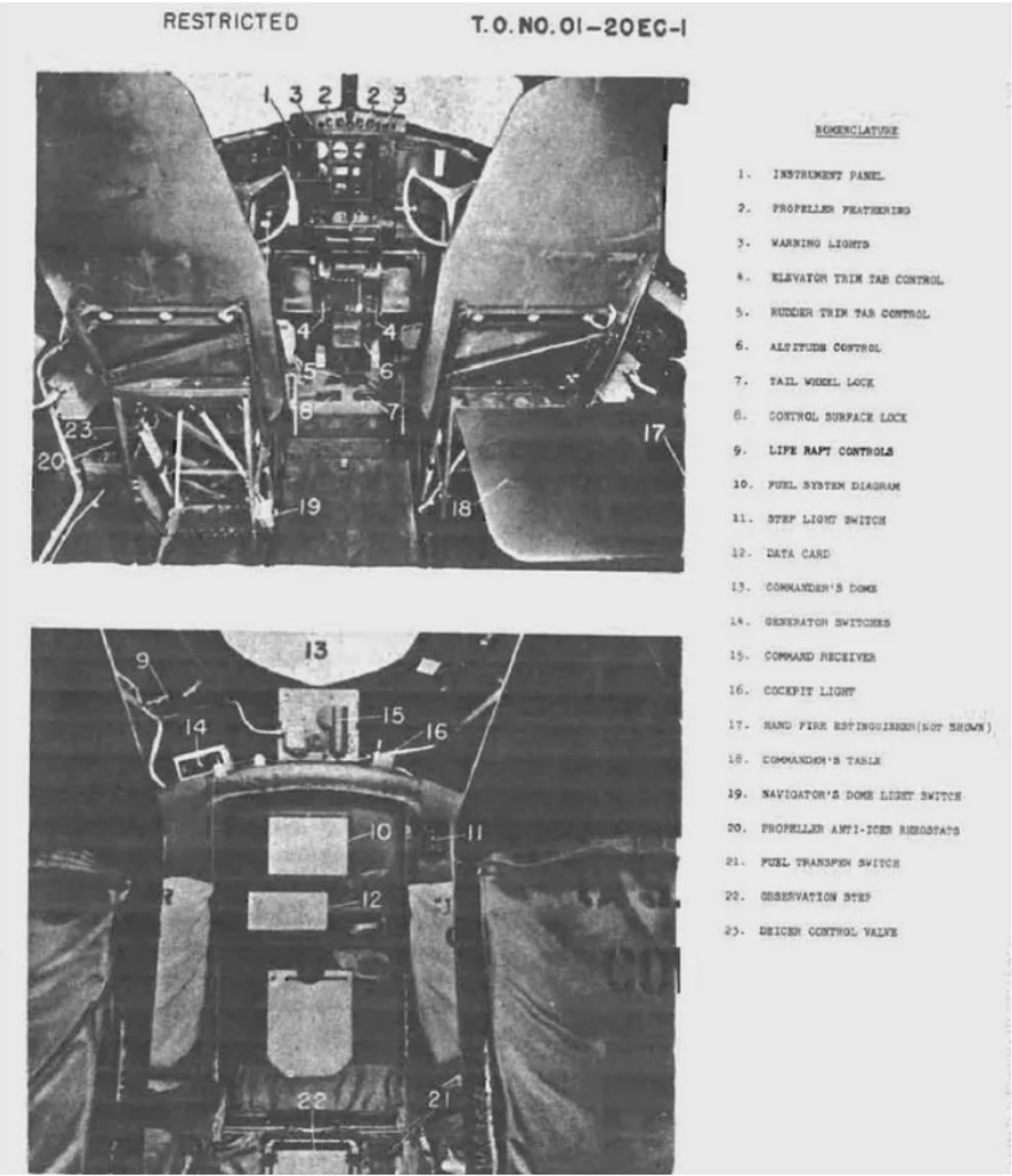
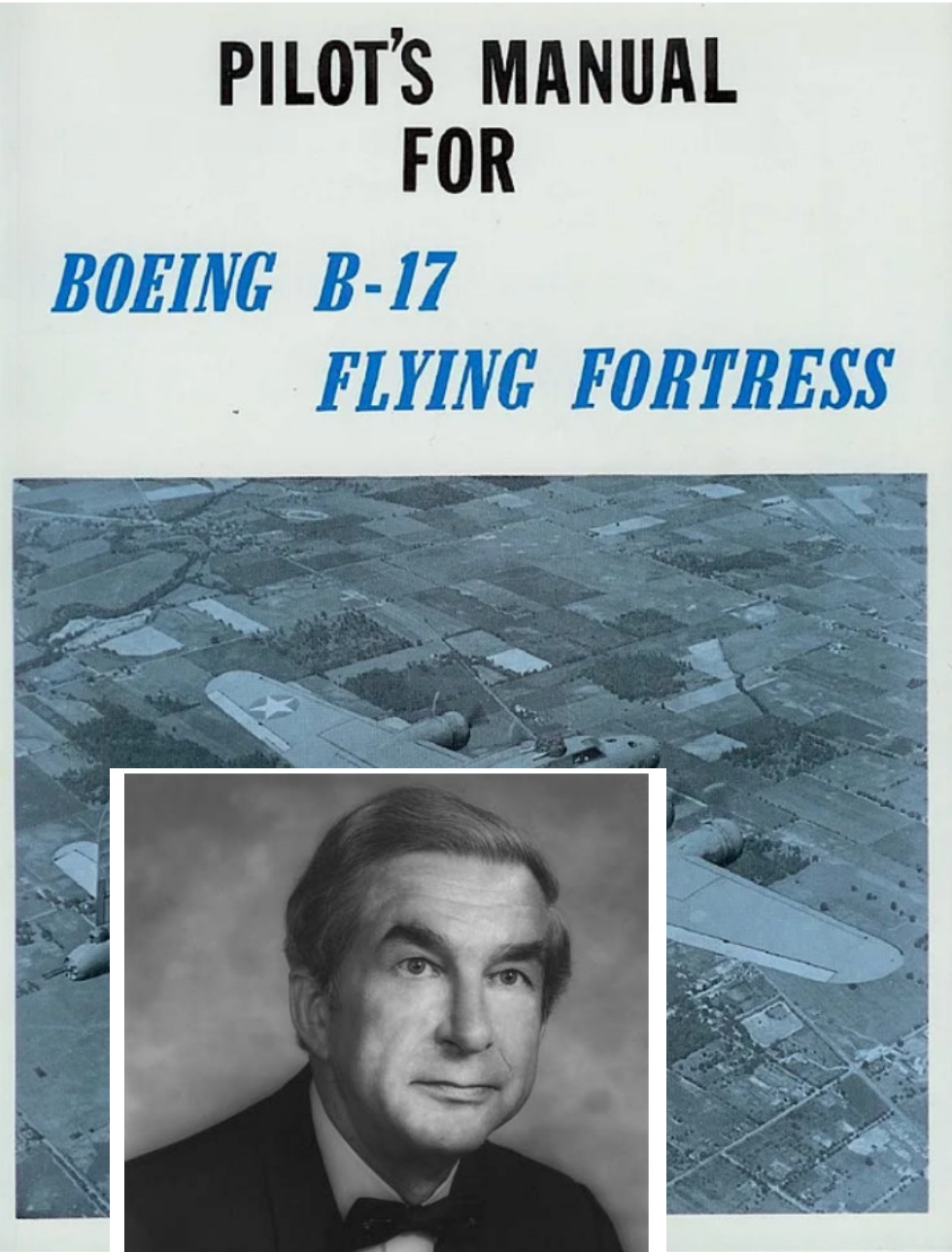
Don't you see the beauty of that, Winston?"



Security Newspeak

In the end the whole notion
of [**security failure**] will be covered
by only one word: [**human error**]

Don't you see the beauty of that, Winston?..."

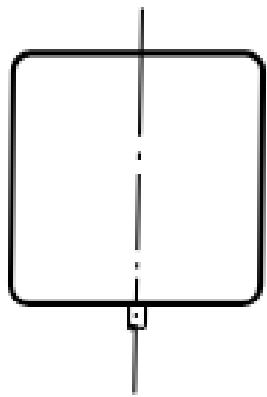


Original cover B-17 Pilot's Manual and complex checklist (courtesy of the AirCorps Library)

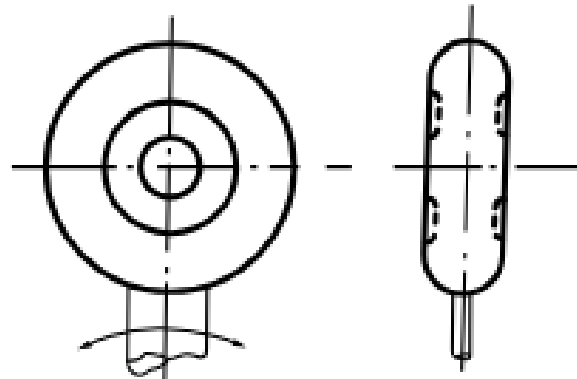
Alphonse Chapanis



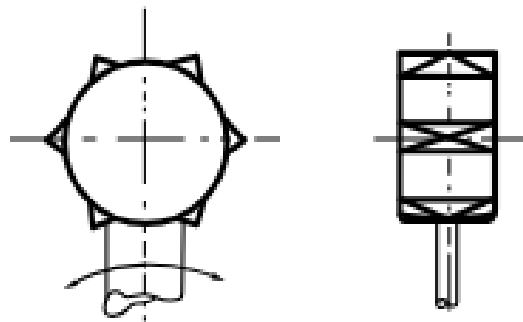
SO CLOSE!



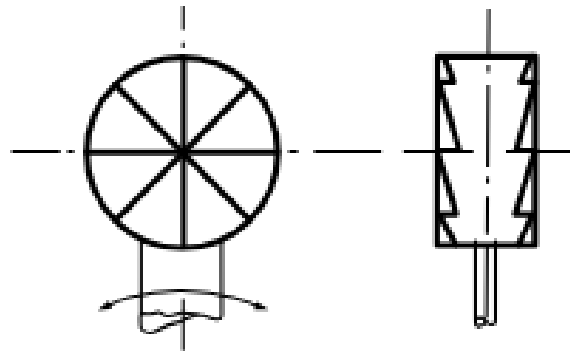
FLAP CONTROL KNOB



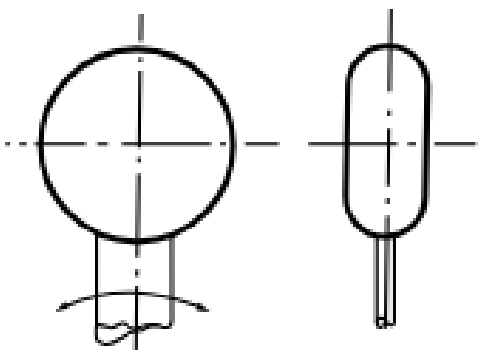
LANDING GEAR CONTROL KNOB



MIXTURE CONTROL KNOB



SUPERCHARGER CONTROL KNOB



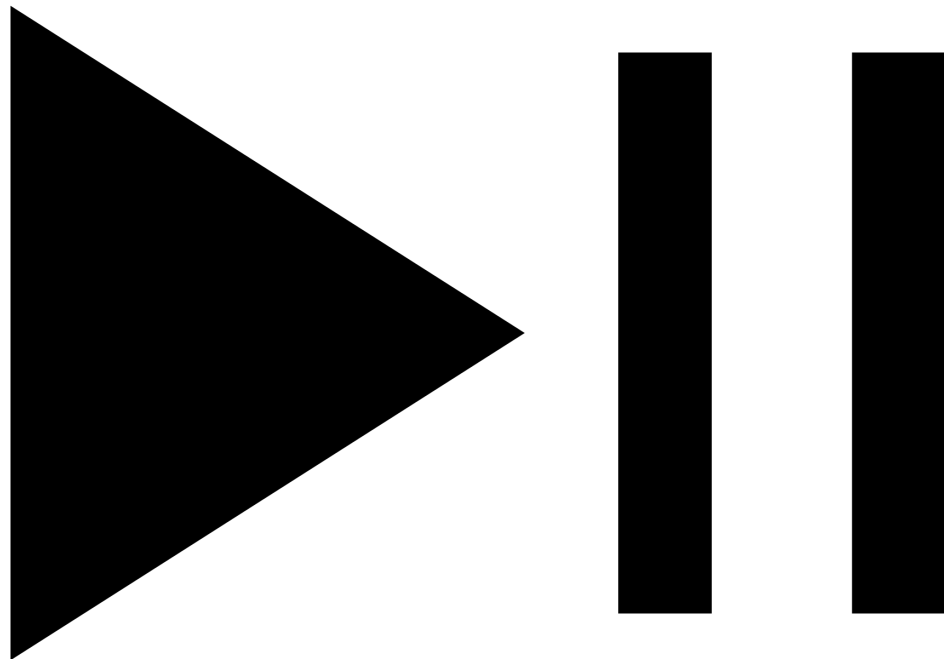
POWER OR THRUST KNOB



PROPELLER CONTROL KNOB



Pause

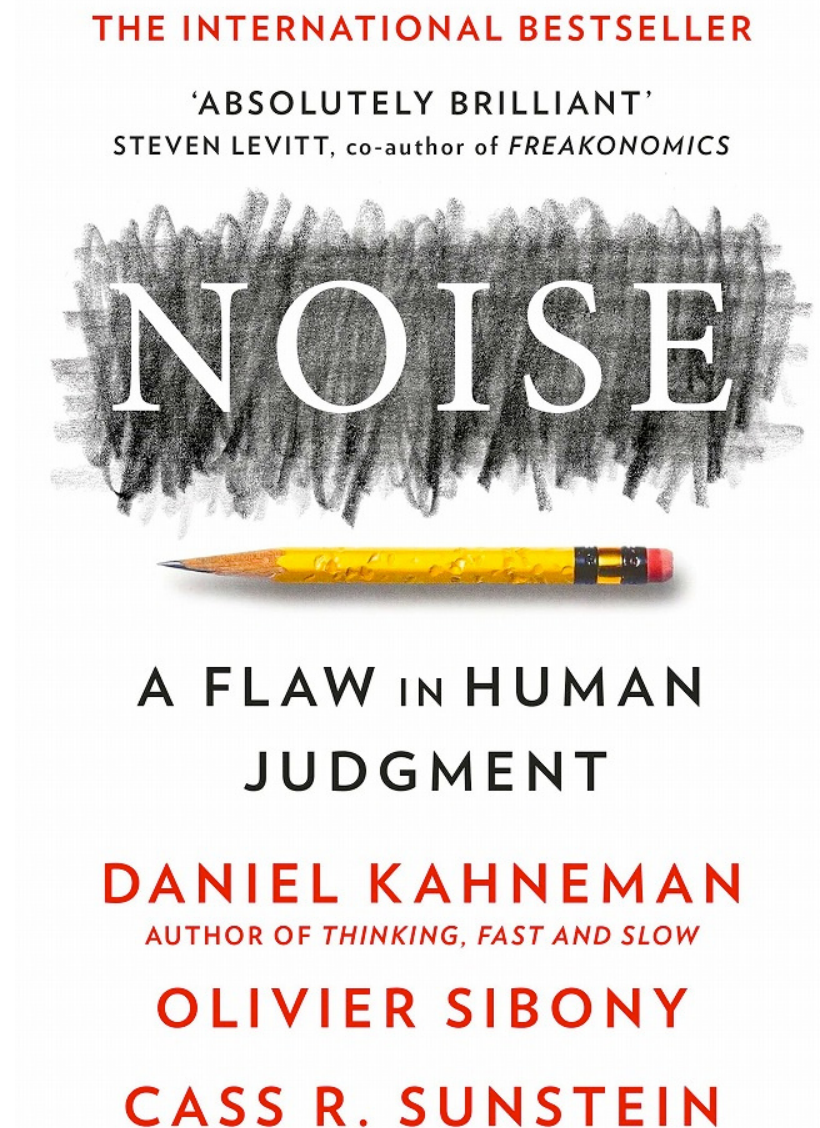


- So what?

Accept the harsh reality

Despite years, users still struggle in basic tasks:

- choose strong passwords
- use security instruments (encryption)
- balance / assess risks
- learn (long lasting) lessons from IS training
- identify phishing (or similar scam)



BY RYAN WEST

THE PSYCHOLOGY OF SECURITY

Why do good users make bad decisions?

“... [the system] must be easy to use and must neither require stress of mind nor the knowledge of a long series of rules...”

AUGUSTE KERCKHOFFS ON THE DESIGN OF CRYPTOGRAPHIC SYSTEMS (*La cryptographie militaire*, 1883)

The importance of the design of security mechanisms has been recognized since Auguste Kerckhoffs published his treatise on cryptography, *La cryptographie militaire*, over a century ago. In the past century, there has been tremendous awareness and research in the field of security mechanisms.

Risk and uncertainty are extremely difficult concepts for people to evaluate. For designers of security systems, it is important to understand how users evaluate and make decisions about security. The most elegant and intuitively designed security systems do not improve security if users ignore warnings, misinterpret instructions, or unintentionally subvert corporate policy. One of the biggest problems in security systems is not just about user in-

ILLUSTRATIONS BY SERGE BLOCH

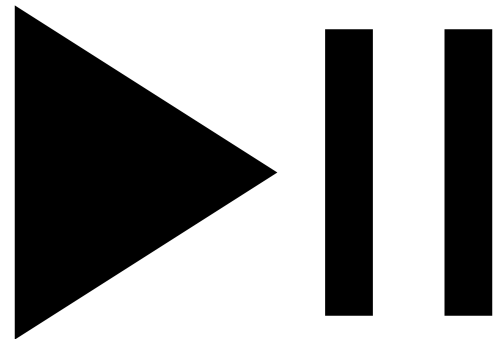


Human-hard tasks in security are also known

People tend to believe they are less vulnerable to risks than others. People also believe they are less likely to be harmed by consumer products compared to others. It stands to reason that any computer user has the preset belief that they are at less risk of a computer vulnerability than others.



Pause



- Shall we ignore humans?
- What to do about it?

Top initial access vectors

IBM X-Force
2025 Threat
Intelligence Index



The top initial access vector observed in 2024 was a tie between exploitation of public facing applications and use of valid account credentials, both representing 30% of X-Force incidence response engagements.

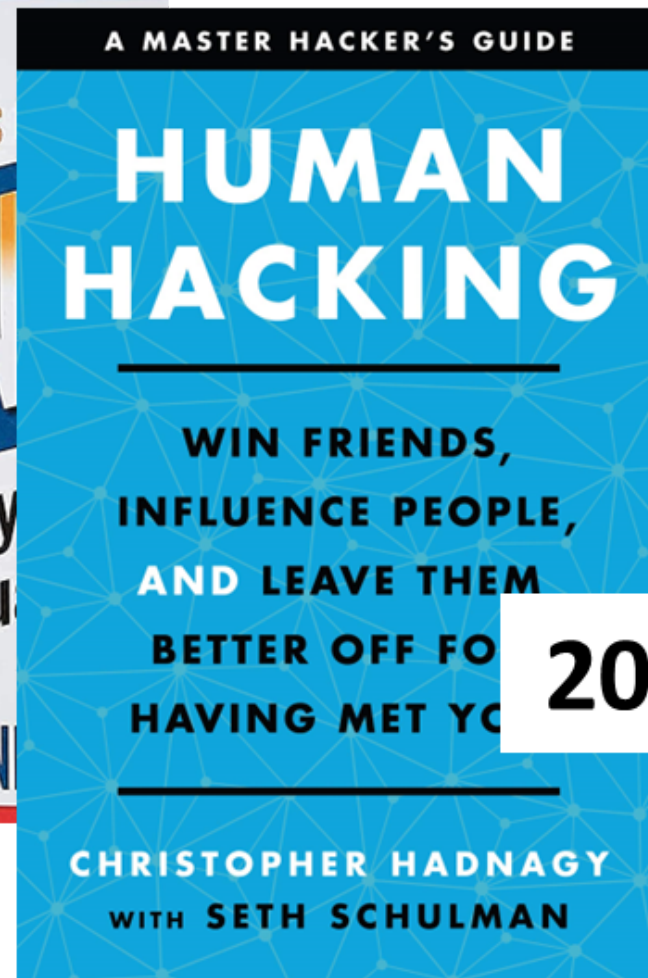
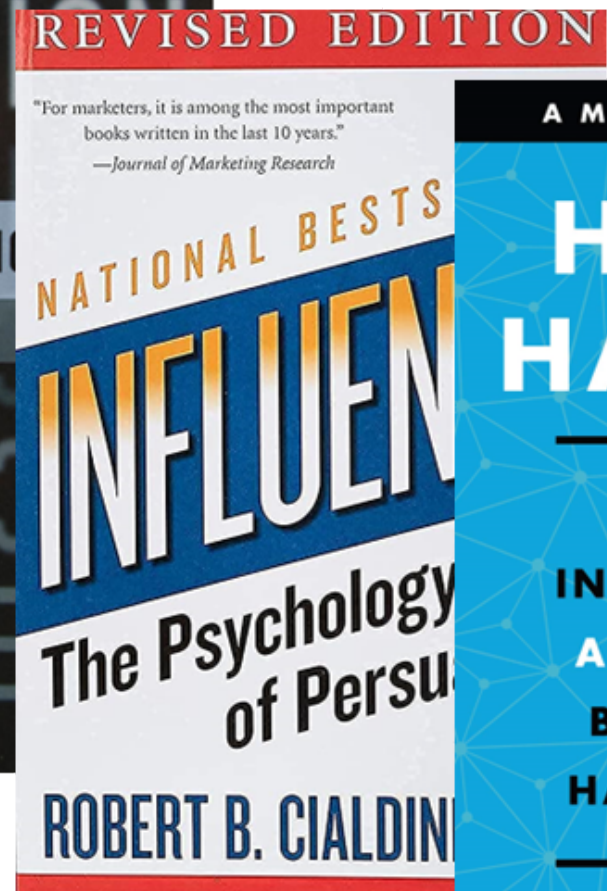
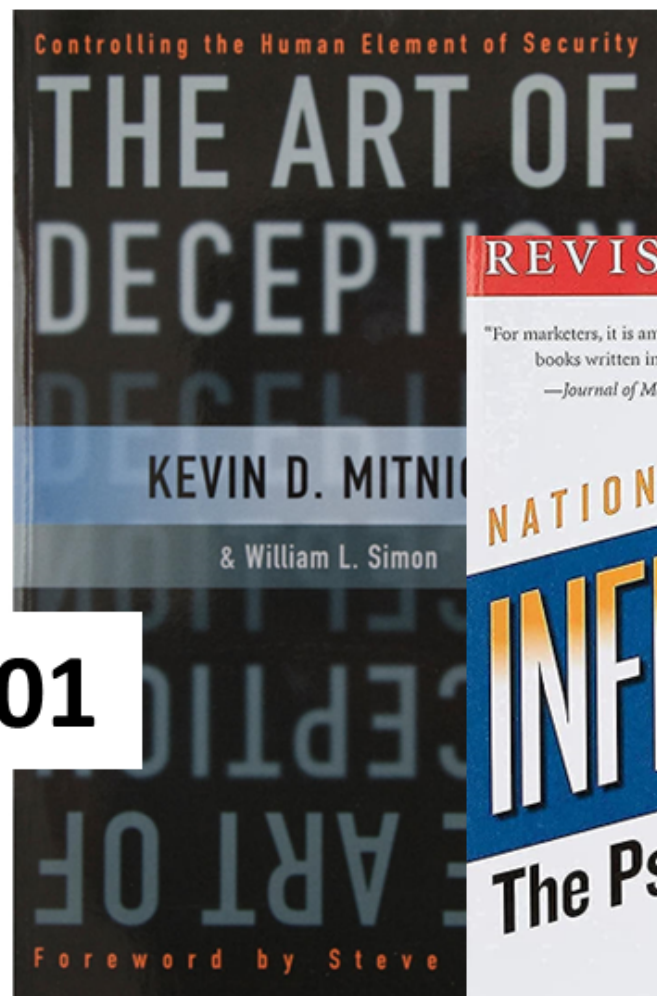
The abuse of valid account credentials is an area we highlighted last year after observing a dramatic rise, continuing the theme of “hackers don’t break in, they log in.” This continues to be a problem and an initial access vector that adversaries are quick to exploit.

Top initial access vectors

This distribution highlights attackers' adaptability and their focus on exploiting vulnerabilities in exposed systems and human error.

The abuse of valid account credentials is an area we highlighted last year after observing a dramatic rise, continuing the theme of "hackers don't break in, they log in." This continues to be a problem and an initial access vector that adversaries are quick to exploit.

2001



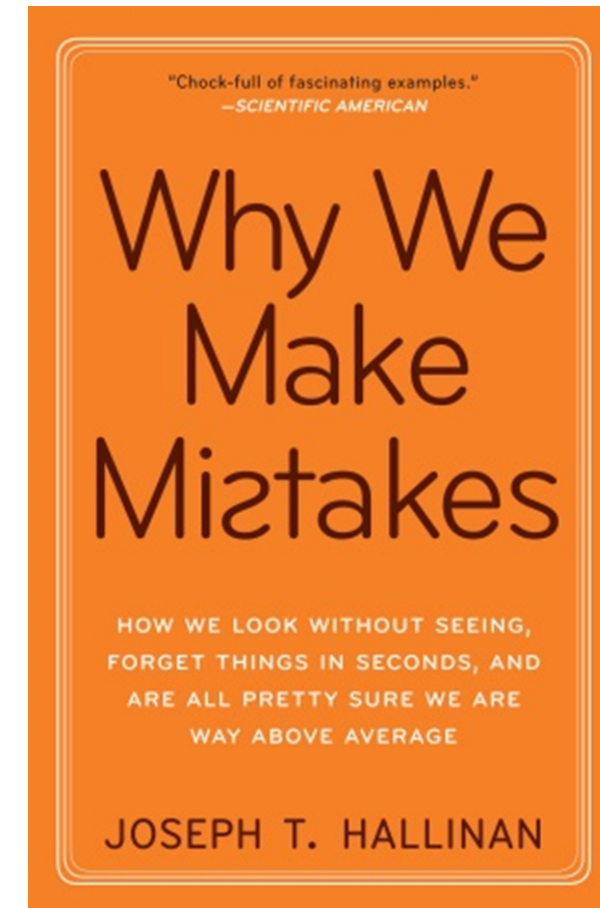
2021



Today



2019



1883



AUGUST KERCKOFFS
(La cryptographie militaire, 1883)

Il est nécessaire que le système soit **d'un usage facile, ne demandant ni tension d'esprit**, ni la connaissance d'une longue série de règles à observer

Early Steps: Usable Security

1975

Human interfaces MUST BE designed for ease of use, so that users routinely apply the protection mechanisms correctly.

To minimize mistakes, **user's mental image of protection MUST match the mechanisms used.**

USERS ARE NOT THE ENEMY

Why users compromise computer security mechanisms and how to take remedial measures.

Confidentiality is an important aspect of computer security. It

depends on authentication mechanisms, such as passwords, to safeguard access to information [9]. Traditionally, authentication procedures are divided into two stages: *identification* (User ID), to identify the user; and *authentication*, to verify that the user is the legitimate owner of the ID. It is the latter stage that requires a secret password. To date, research on password security has focused on designing technical mechanisms to protect

access to systems; the usability of these mechanisms has rarely been investigated. Hitchings [8] and Davis and Price [4] argue that this narrow perspective has produced security mechanisms that are, in practice, less effective than they are generally assumed to be. Since security mechanisms are designed, implemented, applied and breached by people, human factors should be considered in their design. It seems that

currently, hackers pay more attention to the human link in the security chain than security designers do, for example, by using social engineering techniques to obtain passwords.

The key element in password security is the crackability of a password combination. Davies and Ganesan [3] argue that an adversary's ability to crack passwords is greater than usually believed. System-generated passwords are essentially the optimal security approach; however, user-generated passwords are potentially more memorable and thus less likely to be disclosed (because users

do not have to write them down). The U.S. Federal Information Processing Standards [5] suggest several criteria for assuring different levels of password security. *Password composition*, for example, relates the size of a character set from which a password has been chosen to its level of security.

An alphanumeric password is therefore more secure than one composed of letters alone. Short *password*

lifetime—changing passwords frequently—is suggested as reducing the risk associated with undetected compromised passwords. Finally, *password ownership*, in particular individual ownership, is recommended to:

- Increase individual accountability;
- Reduce illicit usage;
- Allow for an establishment of system usage audit trails; and
- Reduce frequent password changes due to group membership fluctuations.

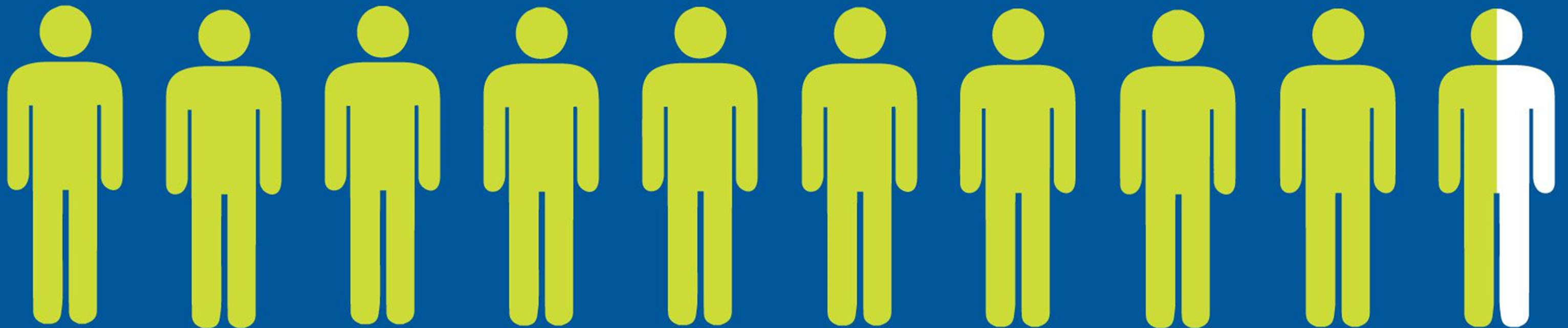
ANNE ADAMS AND
MARTINA ANGELA SASSE

It's not a bug, it's a feature

95%

of all successful cyberattacks are due by
sociotechnical security vulnerabilities

Source: IBM Cyber Security Intelligence Index



Let's start

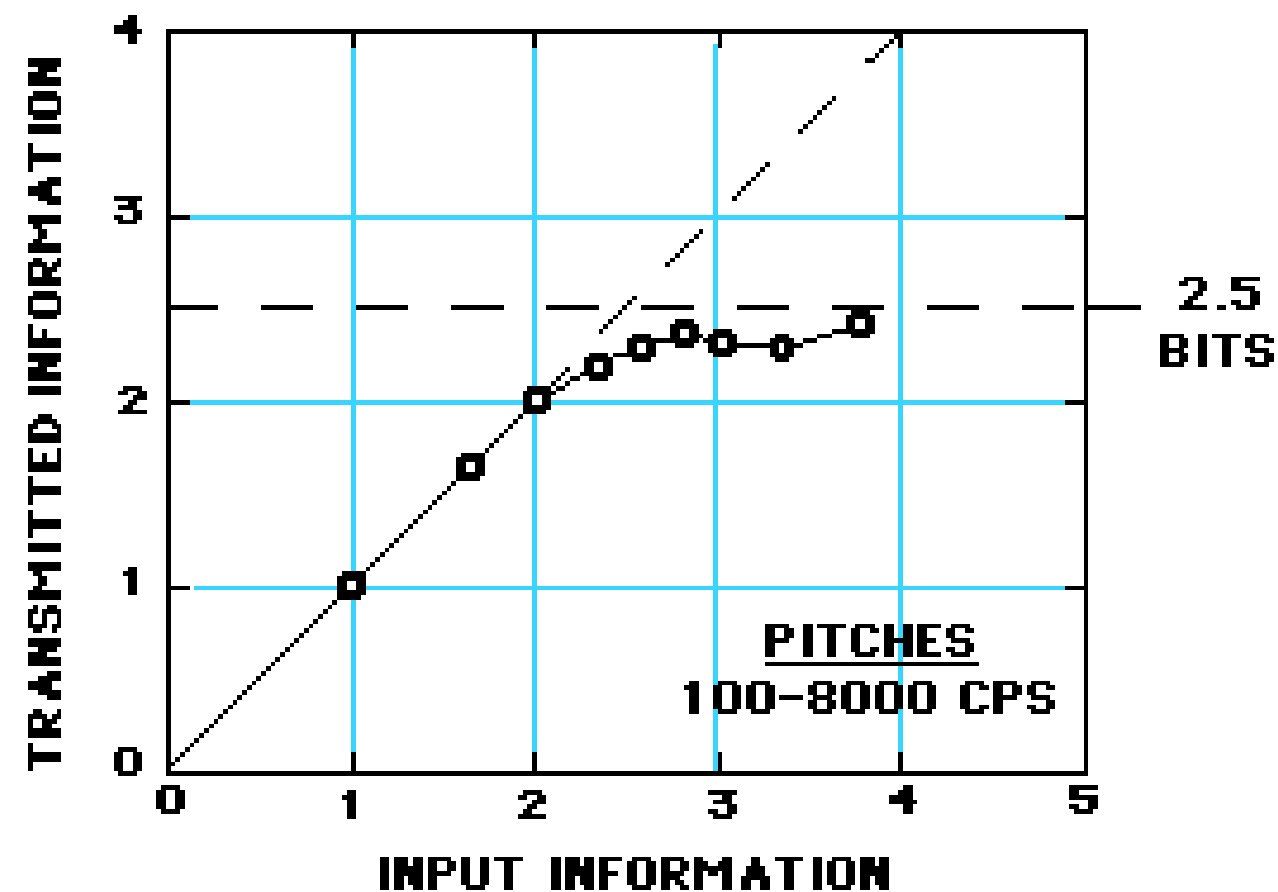
H. A. Miller, The magic number seven, plus or minus two, Psychology Review, 1956

THE PSYCHOLOGICAL REVIEW

THE MAGICAL NUMBER SEVEN, PLUS OR MINUS TWO: SOME LIMITS ON OUR CAPACITY FOR PROCESSING INFORMATION¹

GEORGE A. MILLER

Harvard University



My problem is that I have been persecuted by an integer. For seven years this number has followed me around, has intruded in my most private data, and has assaulted me from the pages of our most public journals. This number assumes a variety of disguises, being sometimes a little larger and sometimes a little smaller than usual, but never changing so much as to be unrecognizable. The persistence with which this number plagues me is far more than a random accident. There is, to quote a famous senator, a design behind it, some pattern governing its appearances. Either there really is something unusual about the number or else I am suffering from delusions of persecution.

I shall begin my case history by telling you about some experiments that tested how accurately people can assign numbers to the magnitudes of various aspects of a stimulus. In the traditional language of psychology these would be called experiments in absolute

judgment. Historical accident, however, has decreed that they should have another name. We now call them experiments on the capacity of people to transmit information. Since these experiments would not have been done without the appearance of information theory on the psychological scene, and since the results are analyzed in terms of the concepts of information theory, I shall have to preface my discussion with a few remarks about this theory.

INFORMATION MEASUREMENT

The "amount of information" is exactly the same concept that we have talked about for years under the name of "variance." The equations are different, but if we hold tight to the idea that anything that increases the variance also increases the amount of information we cannot go far astray.

The advantages of this new way of talking about variance are simple enough. Variance is always stated in terms of the unit of measurement— inches, pounds, volts, etc.—whereas the amount of information is a dimensionless quantity. Since the information in a discrete statistical distribution does not depend upon the unit of measurement, we can extend the concept to situations where we have no metric and we would not ordinarily think of using

¹This paper was first read as an Invited Address before the Eastern Psychological Association in Philadelphia on April 15, 1955. Preparation of the paper was supported by the Harvard Psycho-Acoustic Laboratory under Contract N5ori-76 between Harvard University and the Office of Naval Research, U. S. Navy (Project NR142-201, Report PNR-174). Reproduction for any purpose of the U. S. Government is permitted.

- transience,
- absent-mindedness,
- blocking,
- misattribution,
- suggestibility,
- bias, and
- persistence..

The Seven Sins of Memory

Insights From Psychology and Cognitive Neuroscience

Daniel L. Schacter
Harvard University

Though often reliable, human memory is also fallible. This article examines how and why memory can get us into trouble. It is suggested that memory's misdeeds can be classified into 7 basic "sins": transience, absent-mindedness, blocking, misattribution, suggestibility, bias, and persistence. The first three sins involve different types of forgetting, the next three refer to different

evident when one contemplates what the various forms of memory make possible in our everyday lives: a sense of personal history, knowledge of facts and concepts, and learning of complex skills. Because of memory's importance in everyday life, it is easy to see why Vernon Jordan would be struck by Clinton's "extraordinary memory" and how that ability would enhance Clinton's prospects as a

A Human Complexity Framework?

Maybe Poor Johnny Really Cannot Encrypt – The Case for a Complexity Theory for Usable Security

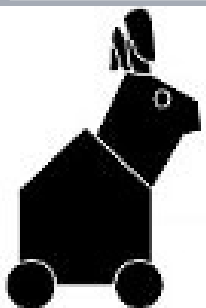
Zinaida Benenson^{*}
Computer Science Department
Friedrich-Alexander-Universität
Erlangen-Nürnberg
zinaida.benenson@fau.de

Gabriele Lenzini
Interdisciplinary Centre for
Security Reliability and Trust
University of Luxembourg
gabriele.lenzini@uni.lu

Daniela Oliveira
Electrical and Computer
Engineering Department
University of Florida
daniela@ece.ufl.edu

Simon Parkin
Department of Computer Science
University College London
s.parkin@ucl.ac.uk

Sven Uebelacker
Security in Distributed
Applications
Hamburg University of Technology
uebelacker@tuhh.de



System,
Users,
UserActions(A),
SecurityEvalToolkit,
UsabilityEvalToolkit

Traces $\subseteq A^*$
InCapacity
OutCapacity
GoalTraces
AttackTraces

Def Secure and Usable

$\text{AttackTraces} = \emptyset \wedge \text{Traces} \subseteq \text{InCapacity}$

Def Insecure and Maybe Usable

$\text{AttackTraces} \neq \emptyset \wedge (\text{Traces} \cap \text{OutCapacity} = \emptyset)$

Human Scale Security Protocol



Toward a Broader View of Security Protocols



Matt Blaze

Blaze, [title], Proc. NSPW 2004

- $P \rightarrow S$: Request bill and present card to S
- $S \rightarrow P$: Calculate bill and run charge with card;
present bill and charge slip to P
- $P \rightarrow S$: Examine bill and charge slip;
if incorrect complain to have bill recalculated and charge invalidated;
if correct sign charge and summon server;
exit
- $S \rightarrow P$: Collect signed charge slip



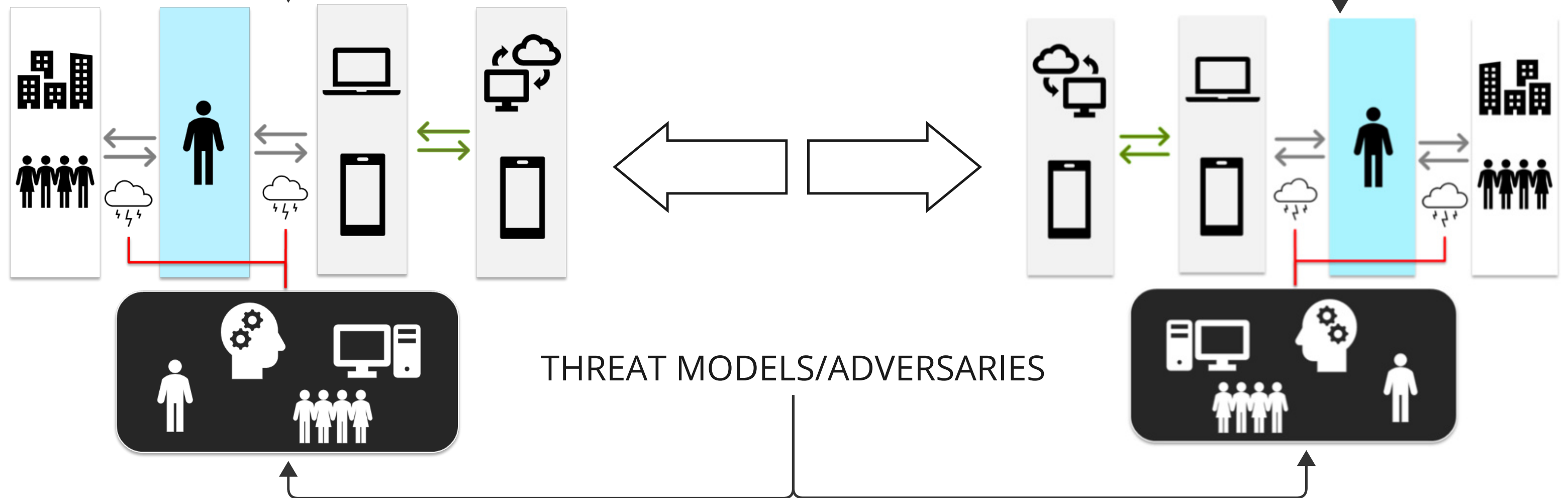
Blaze suggests we should:

- ***Analyze security properties on human scale protocols to understand how they succeed and fail***
- ***Apply tools and techniques of computer security in novel ways to **analyze and improve the security** of human-scale systems.***

(Semi) Formal approaches

Ceremony is an extended network protocol including human beings and objects as nodes in the network

PROTOCOLS / INTERACTIONS



MULTI LAYERED INFORMATION FLOW

Concertina

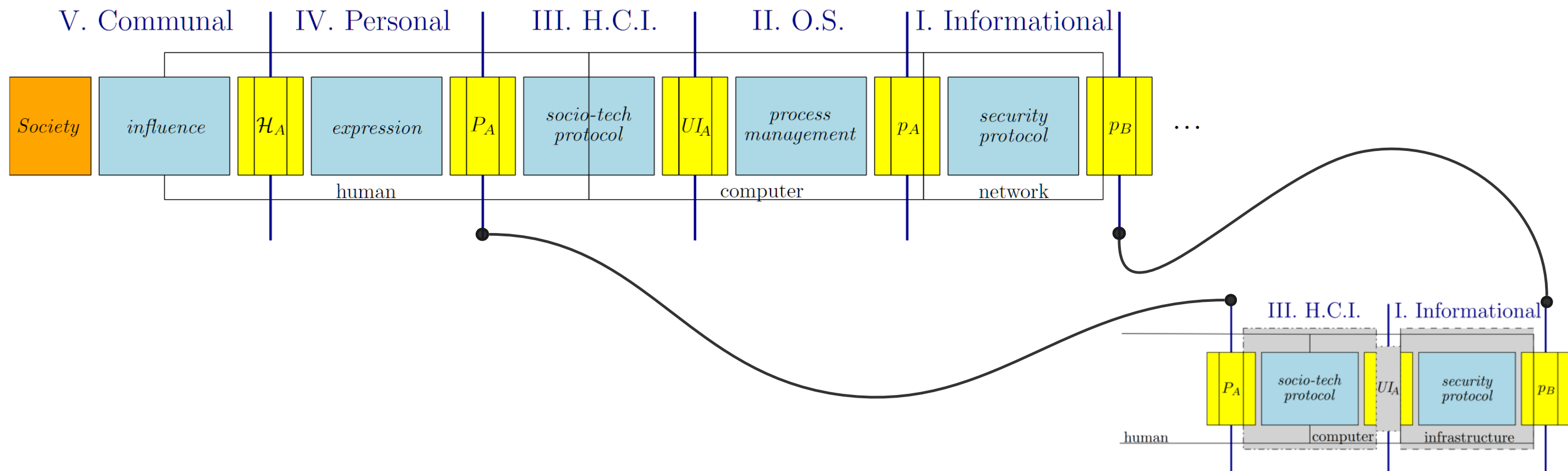
A Socio-Technical Methodology for the Security and Privacy Analysis of Services

Giampaolo Bella
Dipartimento di
Matematica e Informatica
University of Catania, Italy
Email: giamp@dmi.unict.it

Paul Curzon
School of Electronic Engineering
and Computer Science
Queen Mary University of London
Email: p.curzon@qmul.ac.uk

Rosario Giustolisi
Interdisciplinary Centre for
Security Reliability and Trust
University of Luxembourg
Email: rosario.giustolisi@uni.lu

Gabriele Lenzini
Interdisciplinary Centre for
Security Reliability and Trust
University of Luxembourg
Email: gabriele.lenzini@uni.lu



Use Case I

TSL handshake

user/browser(s) interaction

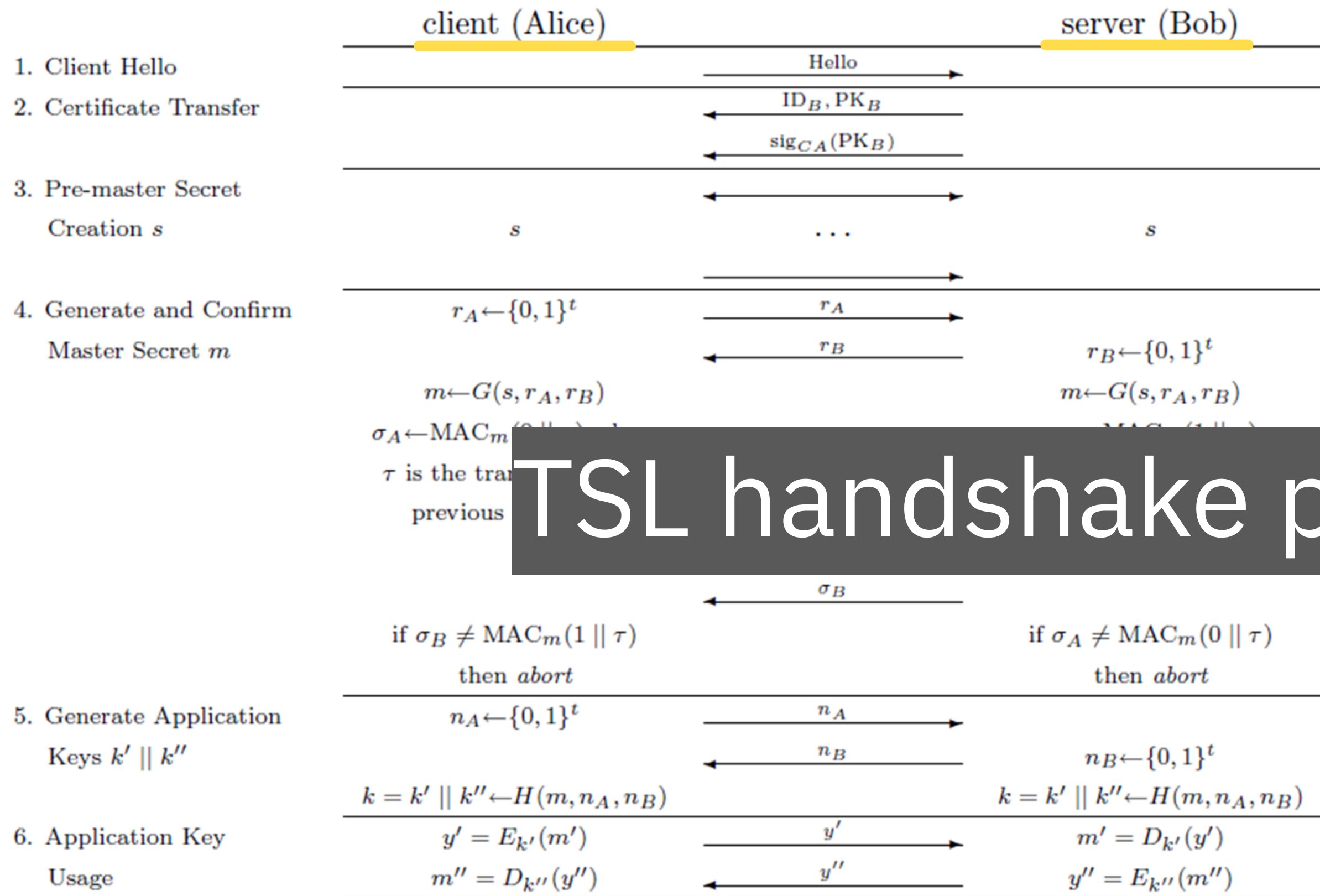
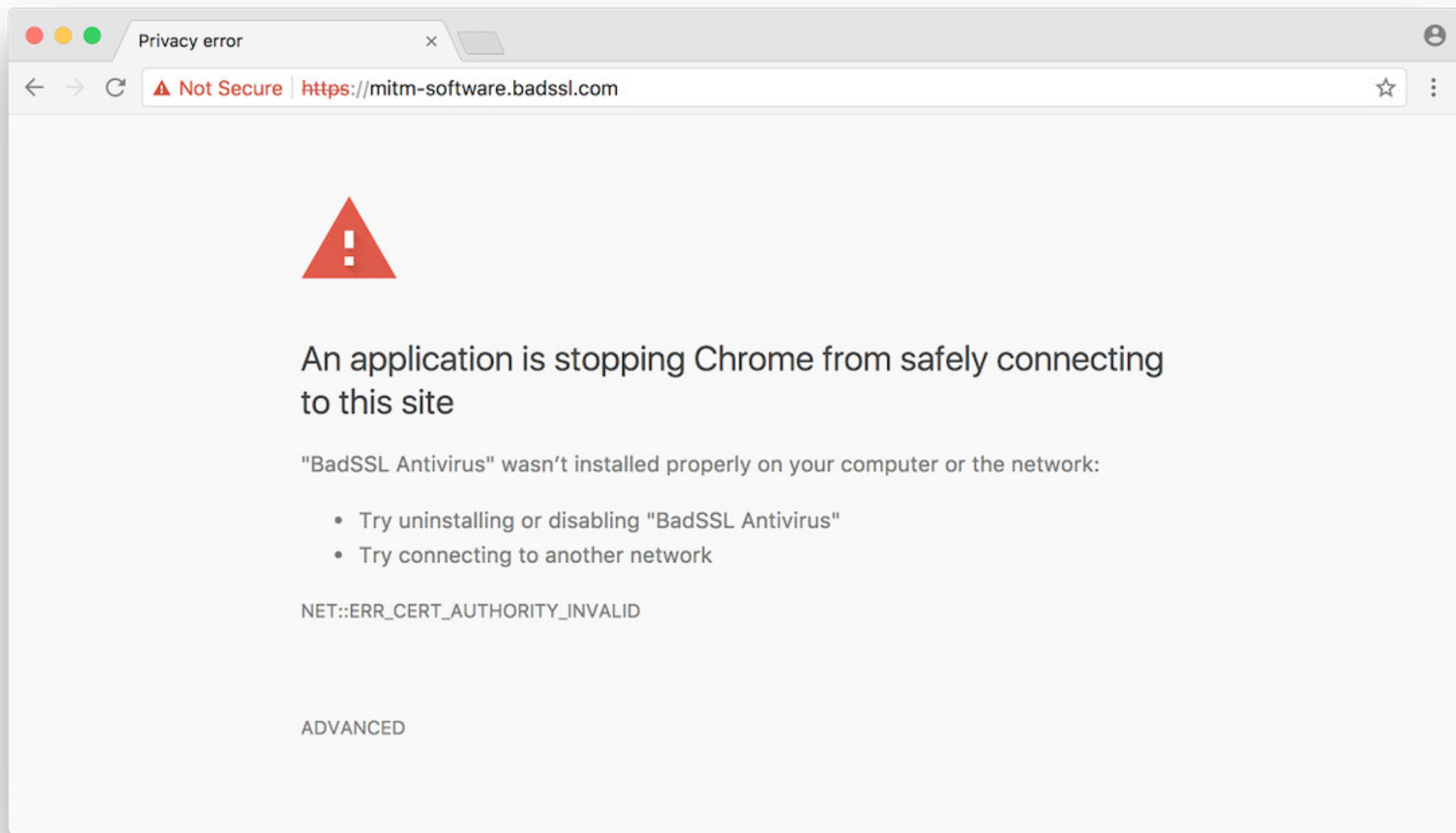


Figure 1: A general TLS like protocol



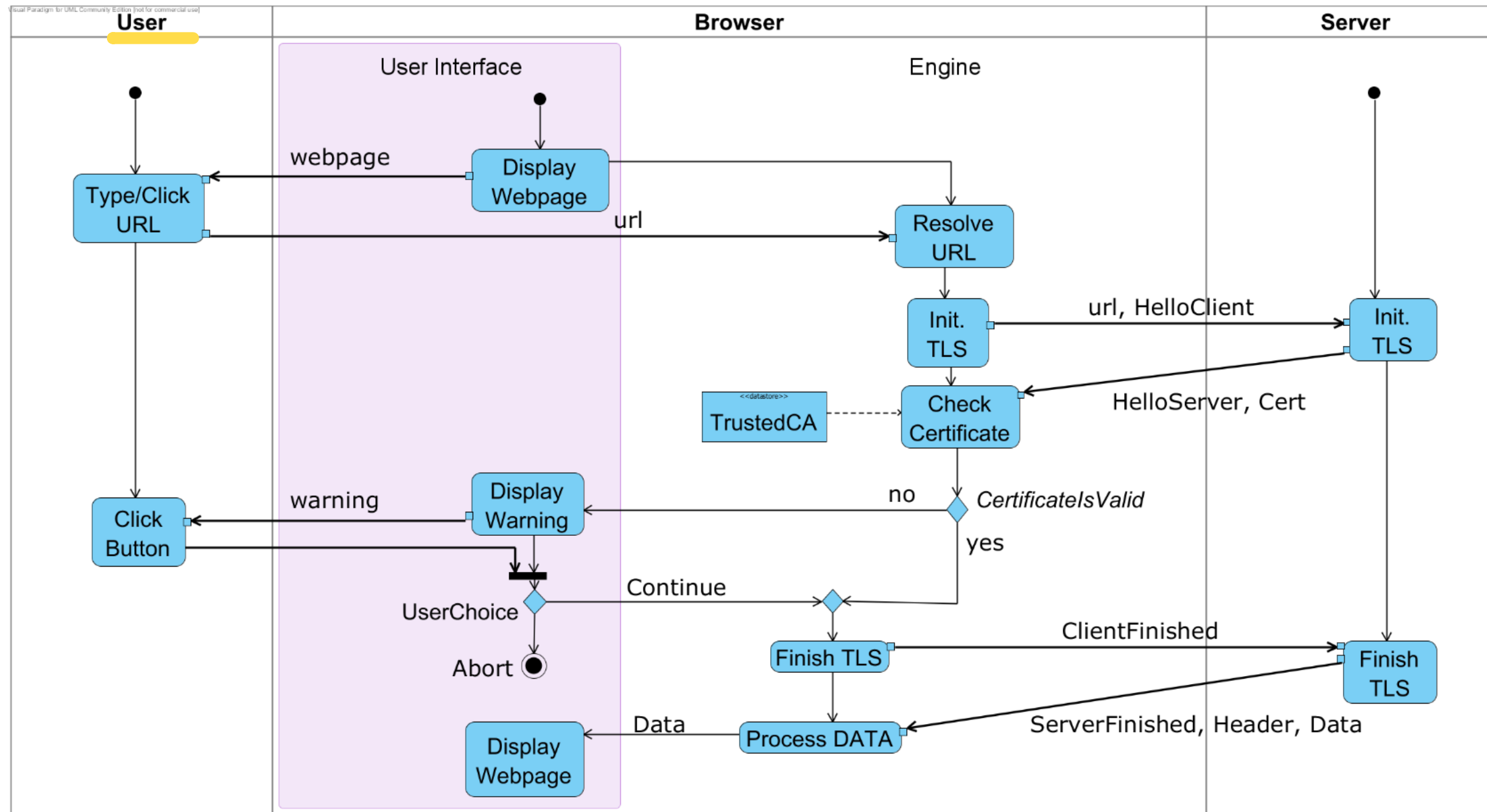
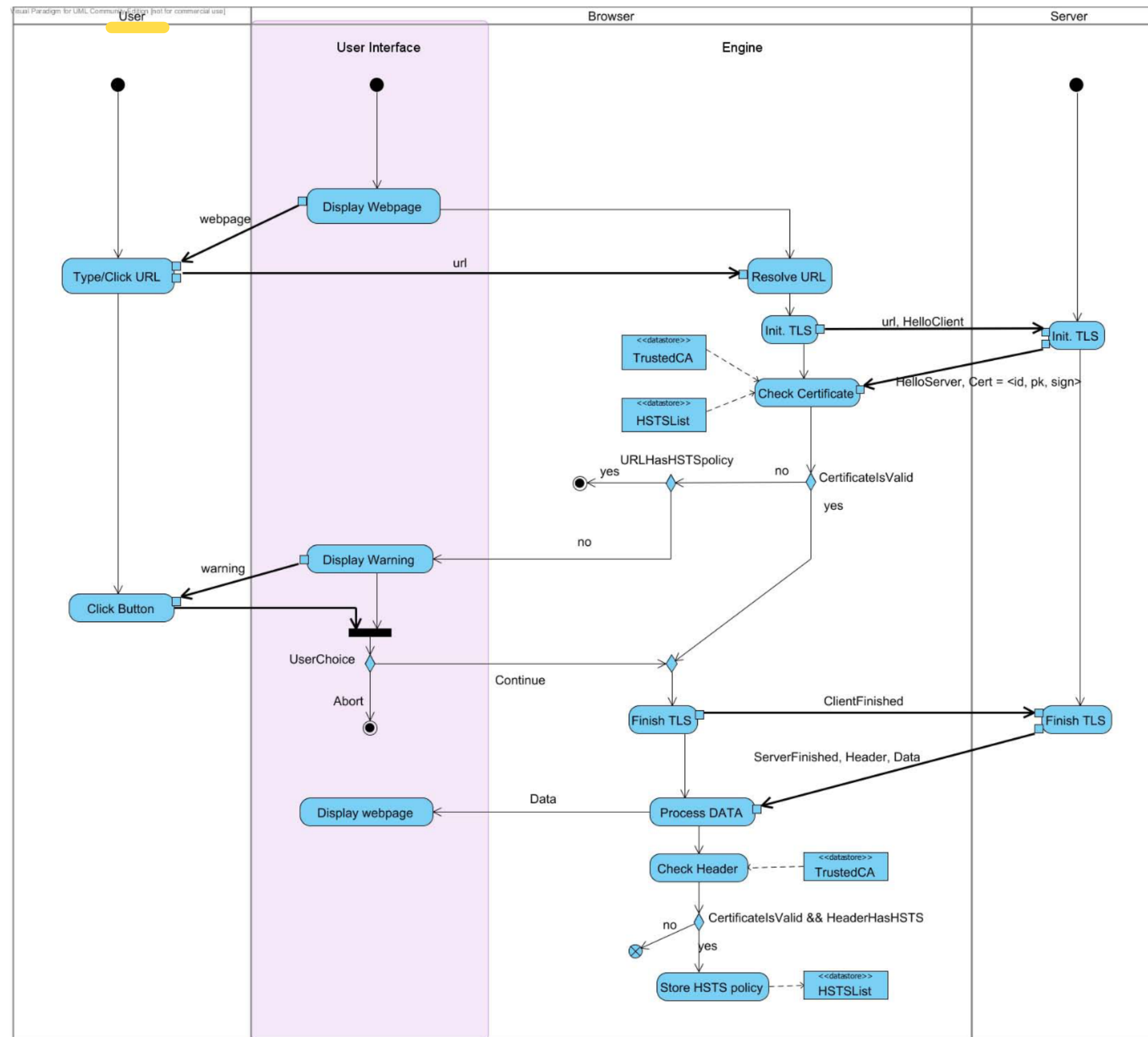


Fig. 2: Activity diagram for certificate validation in Internet Explorer



Property 1 (Warning Users).

*A user whose browser receives an **invalid certificate** on a **TLS** session **is warned about this by the browser BEFORE the browser completes the session***

Property 4 (Learning from Server Certificate History).

*A user who completes a TLS session with a server via a browser receiving an **invalid certificate**, and then completes another session with the same server via the same browser receiving a valid certificate **is warned by the browser about the risk of man-in-the-middle attack***

Property 3 (HSTS [HTTP Strict Transport Security])

*A user who accesses a **server that sends an HSTS header** on a TLS session via a browser that receives a valid certificate **is protected from man-in-the-middle attacks on future sessions** with the same server via the same browser*

Property 2 (Storing Server Certificates).

*A user who stores a certificate that associates an **honest server** to its public key on a TLS session via a browser **is protected from man-in-the-middle attacks on future sessions** with the same server via the same browse*

It is possible to define and analyze these properties formally, using LTL and Proverif

Browser	Property 1	Property 2	Property 3	Property 4
<i>Firefox</i>	×	×	✓	×
<i>Chrome</i>	✓	✓	✓	×
<i>Internet Explorer</i>	✓	✓	×	×
<i>Opera Mini</i>	×	✓	×	×

These are, however, properties of interfaces and the "ceremonies" they offer to users.

X-Men: A Mutation-Based Approach for the Formal Analysis of Security Ceremonies

Diego Sempredoni
Department of Informatics
King's College London
London, UK
diego.sempredoni@kcl.ac.uk

Luca Viganò
Department of Informatics
King's College London
London, UK
luca.vigano@kcl.ac.uk

Abstract—There is an increasing number of cyber-systems (e.g., payment, transportation, voting, critical-infrastructure systems) whose security depends intrinsically on human users. A security ceremony expands a security protocol with everything that is considered out-of-band to it, including, in particular, the mistakes that human users might make when participating actively in the security ceremony. In this paper, we introduce a novel approach for the formal analysis of security ceremonies. Our approach defines mutation rules that model possible behaviors of a human user, and automatically generates mutations in the behavior of the other agents of the ceremony to match the human-induced mutations. This

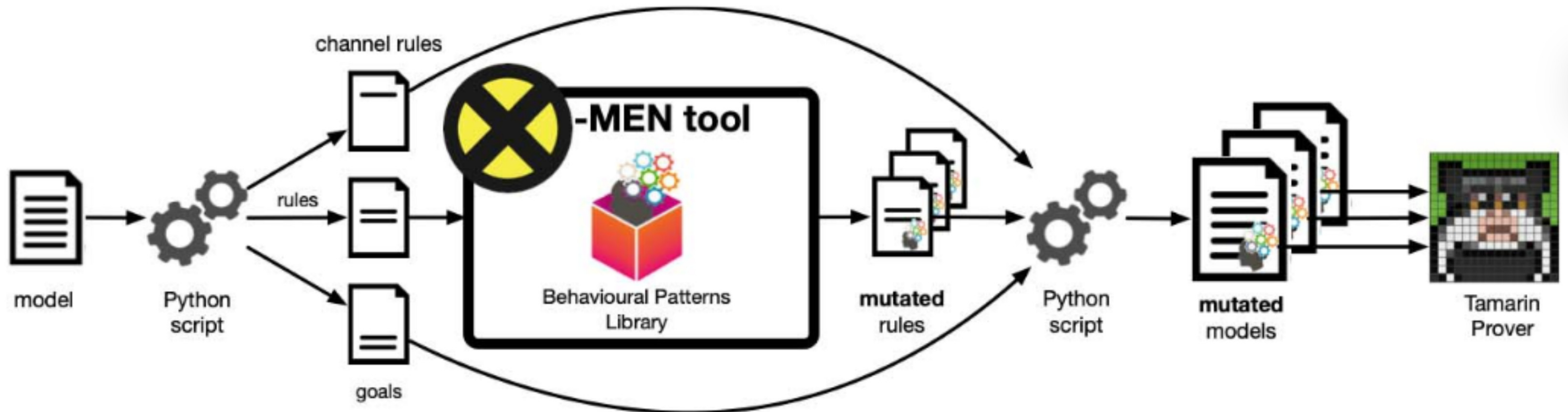
- considering one or more attackers that can carry out whatever actions they are able to in order to attack the protocol, but then
- modeling all other protocols actors (regardless of whether they are computers or human users) as honest processes that behave according to the protocol specification.

When considering security ceremonies, in which humans are first-class actors, it is not enough to take this “black&white” view. It is not enough to model human users as “honest processes” or as attackers, because they are neither. Modeling a person’s behavior is not simple



Users, and user's errors can be modelled (at least in part)

A library that, from a ceremony, generates realistic user's interaction failure modes (e.g., post completion errors).





Transport for London

Watch out for card clash, only touch the card you wish to use on the reader



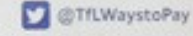
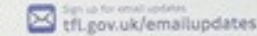
Card clash happens when the card reader detects two or more Oyster, contactless payment or other smartcards. This could lead to the ticket gates not opening or you getting a red light, meaning you haven't paid for your journey.

To avoid card clash only touch the one card you wish to use on the reader.

Contactless payment cards cannot be charged for travel until later this year.

If you have questions or need help, please speak to a member of staff.

For more information visit tfl.gov.uk/oyster



MAYOR OF LONDON



User Identification Procedures with Human Mutations: Formal Analysis and Pilot Study (Extended Version)

Megha Quamara and Luca Viganò

Department of Informatics, King's College London, London, UK

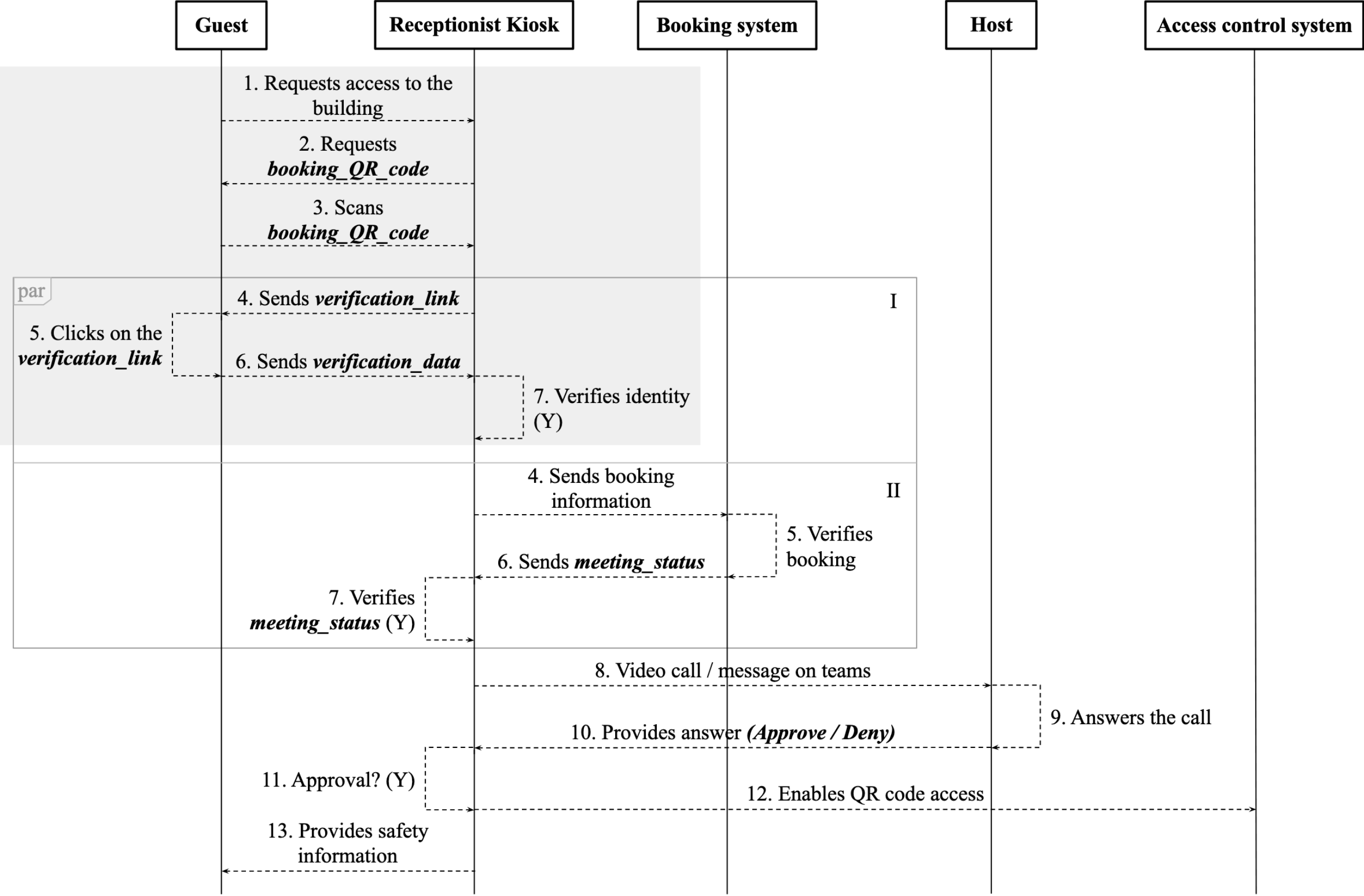
megha.quamara@kcl.ac.uk, luca.vigano@kcl.ac.uk

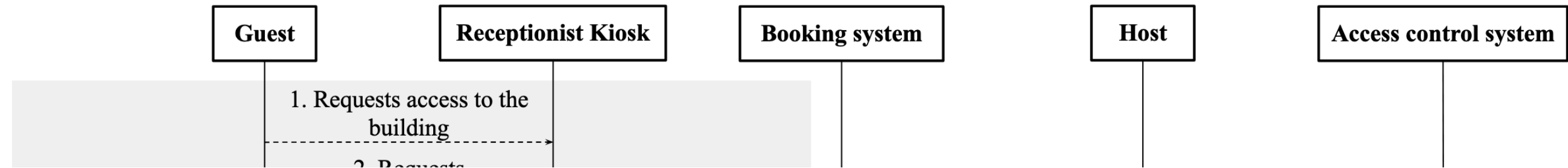
Abstract—User identification procedures, essential to the information security of systems, enable system-user interactions by exchanging data through communication links and interfaces to validate and confirm user authenticity. However, human errors can introduce vulnerabilities that may disrupt the intended identification workflow and thus impact system behavior. Therefore, ensuring the integrity of these procedures requires accounting for such erroneous behaviors. We follow a formal, human-centric approach to analyze user identification procedures by modeling them as security ceremonies and apply proven techniques for automatically analyzing such ceremonies. The approach relies on mutation rules to model potential human errors that deviate from expected interactions during the identification process, and is implemented as the X-Men tool, an extension of the Tamarin prover, which automatically generates models with human mutations and implements matching mutations to other ceremony participants for analysis. As a proof-of-concept, we consider a real-life pilot study involving an AI-driven, virtual receptionist kiosk for authenticating visitors.

Index Terms—User identification, security ceremonies, mutations, formal methods, modeling and analysis

human users who interact with computing systems and exchange messages and data through communication channels, user interfaces, or similar means [4]. This enables us to identify vulnerabilities arising from unexpected or incorrect behavior by human users while interacting with other ceremony participants, such as the system, during the identification process. To this end, we adapt and extend the mutation-based approach presented in [5]. *Mutations* model potential mistakes the human users might make compared to the behavior specified for them in a ceremony. We consider three mutations of [5]—*skip*, *add*, and *replace*—and define an additional mutation, *disorder*, for the actions performed in the ceremony. The approach allows mutations in the behavior of other ceremony participants as a consequence of (and to align with) the human-induced mutations. These mutations propagate throughout the ceremony. This facilitates analyzing the original ceremony specification and its possible mutations, including how the ceremony has been (or could be) implemented. If matching mutations







Quote: *"Our [Vigano's and Quamara's] analysis revealed vulnerabilities arising from human errors, which can affect other agents and disrupt the identification process.*

We aim to extend our mutation model with timing-related mutations, where action execution delays, such as a user scanning an expired QR code or using an outdated verification link .."



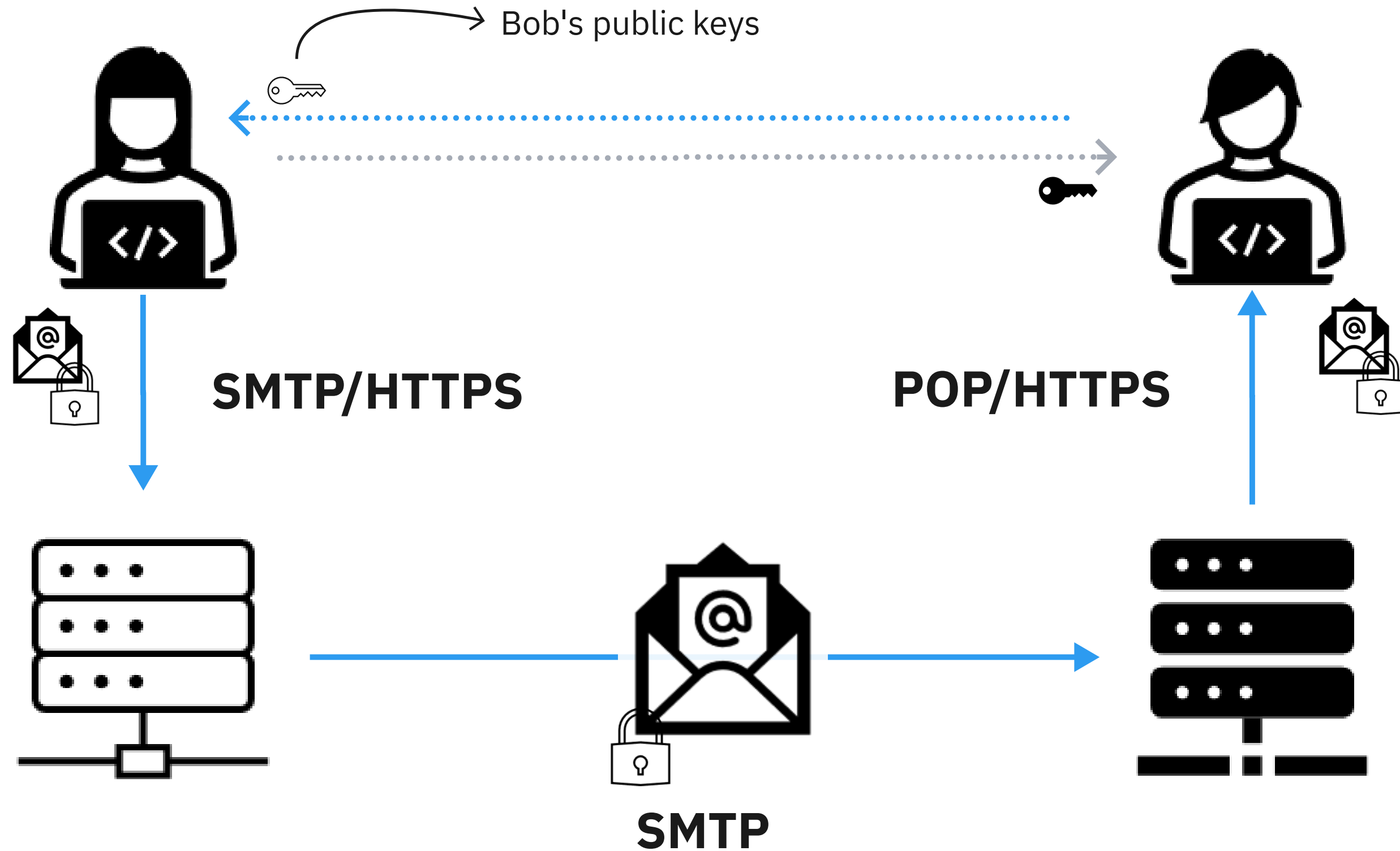


Check the time

Use Case I

Secure communications

end-to-end encryption (decentralized p2p)



Obstacles to the Adoption of Secure Communication Tools

Ruba Abu-Salma
University College London, UK

M. Angela Sasse
University College London, UK

Joseph Bonneau
Stanford University & EFF, USA

Anastasia Danilova
University of Bonn, Germany

Alena Naiakshina
University of Bonn, Germany

Matthew Smith
University of Bonn, Germany

and their perceptions of the tools' security properties. We found that the adoption of secure communication tools is hindered by fragmented user bases and incompatible tools. Furthermore, the vast majority of participants did not understand the essential concept of end-to-end encryption, limiting their motivation to adopt secure tools. We identified a number of incorrect mental models that underpinned participants' beliefs.

Cops see an encryption problem. Spyware makers see an opportunity

Source: <https://www.technologyreview.com/s/614898/cops-see-an-encryption-problem-spyware-makers-see-an-opportunity/>

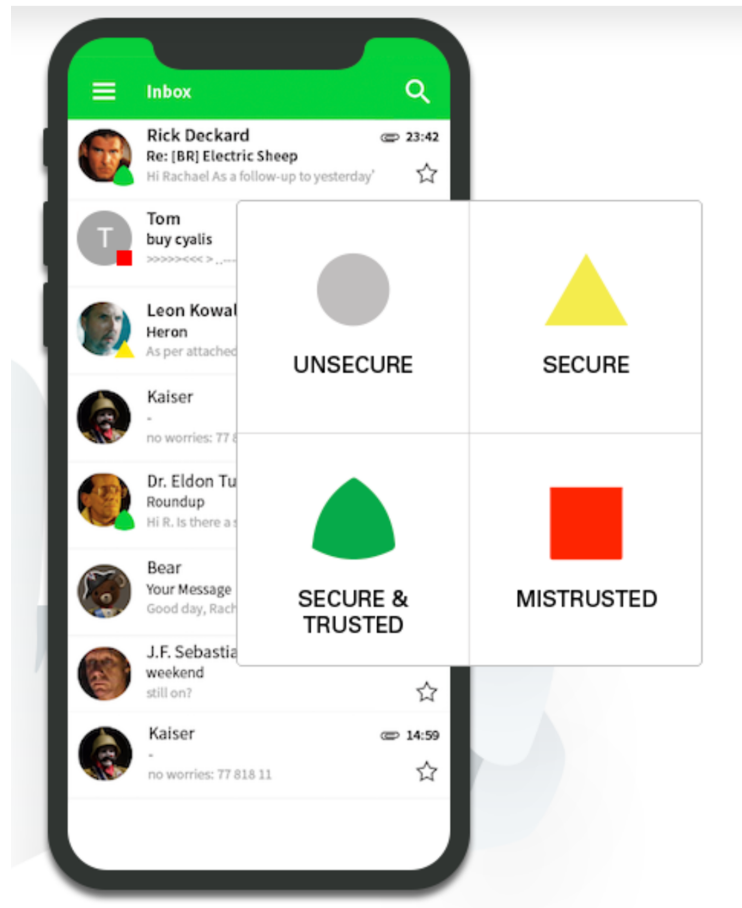
P6-Fi5



P6-Fi5: Intercept data, encryption is not broken .. it is simply rendered unusable

“The device cannot read encrypted data, but instead tries a different tactic to get private information: making encrypted apps glitchy or even totally unusable. It’s a subtle but strong way to push a frustrated target away from a private app and toward a non-encrypted service that can easily be intercepted and eavesdropped on.”





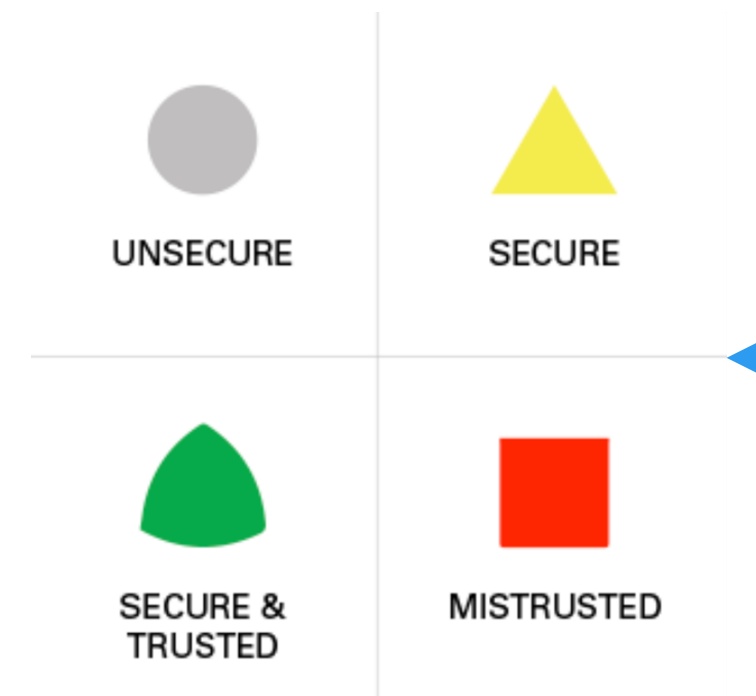
- Automatic Key Generation, Discovery, and Management
- Authentication via Trustwords
- Automatic end-to-end encryption of messages
- *Privacy Rating assigned to a message*

- Do users understand whether their comm are secures?
(a study of prietty easy privacy):


UI Icons (metaphors) mapped from by internal states

Rating code	Rating label
-3	under attack
-2	broken
-1	mistrust
0	undefined
1	cannot decrypt
2	have no key
3	unencrypted
4	unencrypted for some
5	unreliable
6	reliable
7	trusted
8	trusted and anonymized
9	fully anonymous

Rating codes	Color code	Color label
-3 to -1	-1	red
0 to 5	0	no color
6	1	yellow
7 to 9	2	green



We formally checked (in part) the protocols in Proverif

Rating code	Rating label	Color code	Color label	Icon	Rating title	Rating explanation	Rating suggestion
-3	under attack	-1	red		Under Attack	This message is not secure and has been tampered with.	Separately verify the content of this message with your communication partner.

 Reply



 Forward

 Archive

 Junk

 Delete

More ▾

From  Gabriele Lenzini 

Subject **private message**

01/07/2019, 11:08

To  Borce STOJKOVSKI 

Date Mon, 1 Jul 2019 11:08:38 +0200

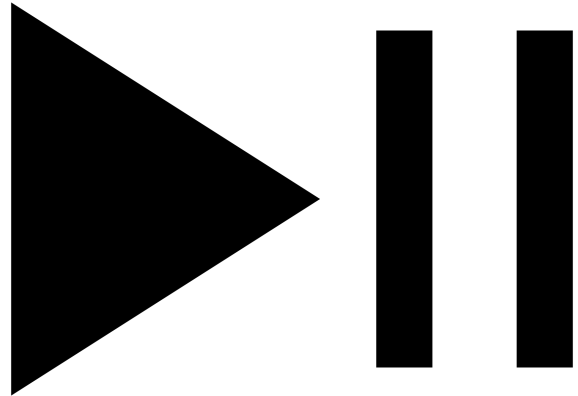
Message ID <01978a928dc3402b9b2826a999beba98@uni.lu> ▾

MIME-Version 1.0

It's me.

Gabriele Lenzini

Pause



- What are relevant properties here?
- Are user's happy to adopt e2e?
- Are user's "sense" **aligned** with .. ?

User/Systems Misalignment: problems

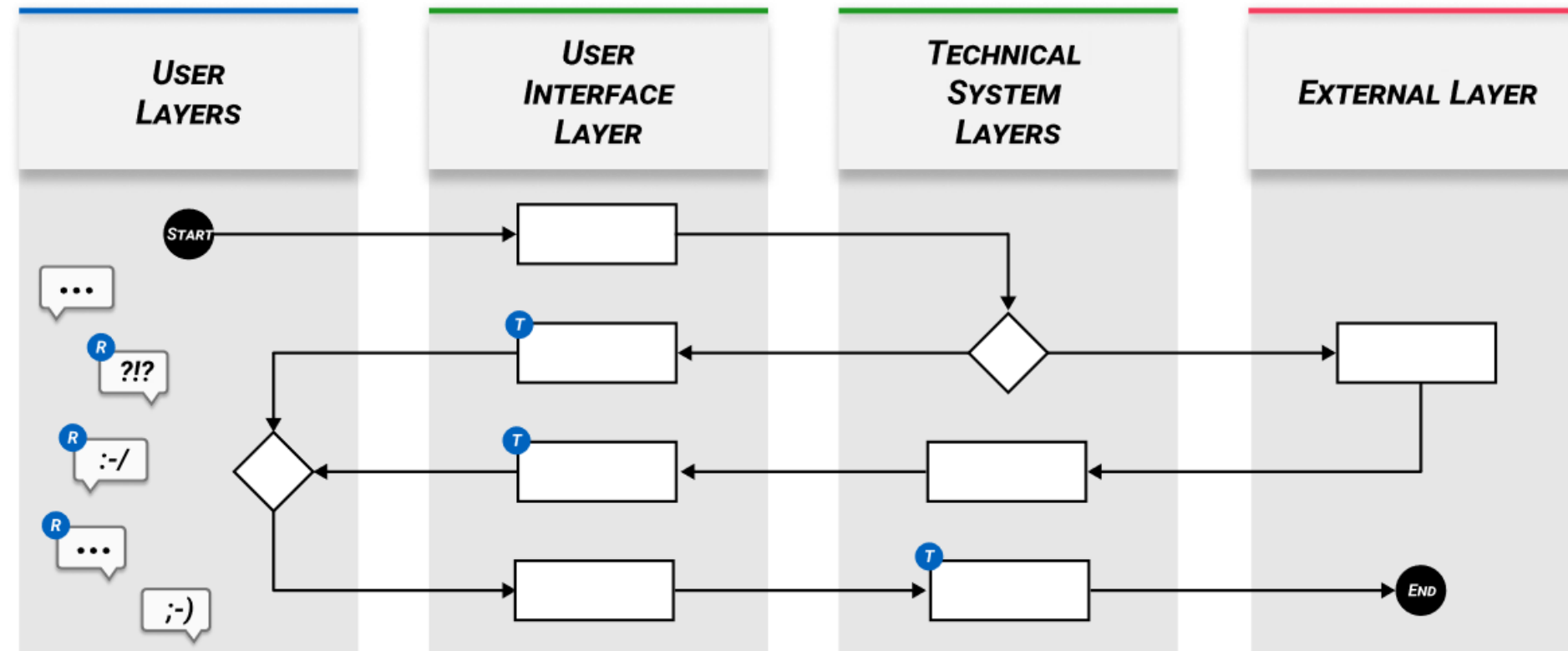
False sense of security: injective certainty where it is technically unjustified.

False sense of insecurity: failing to transmit a justified sense of security

A ceremony with user's emotions

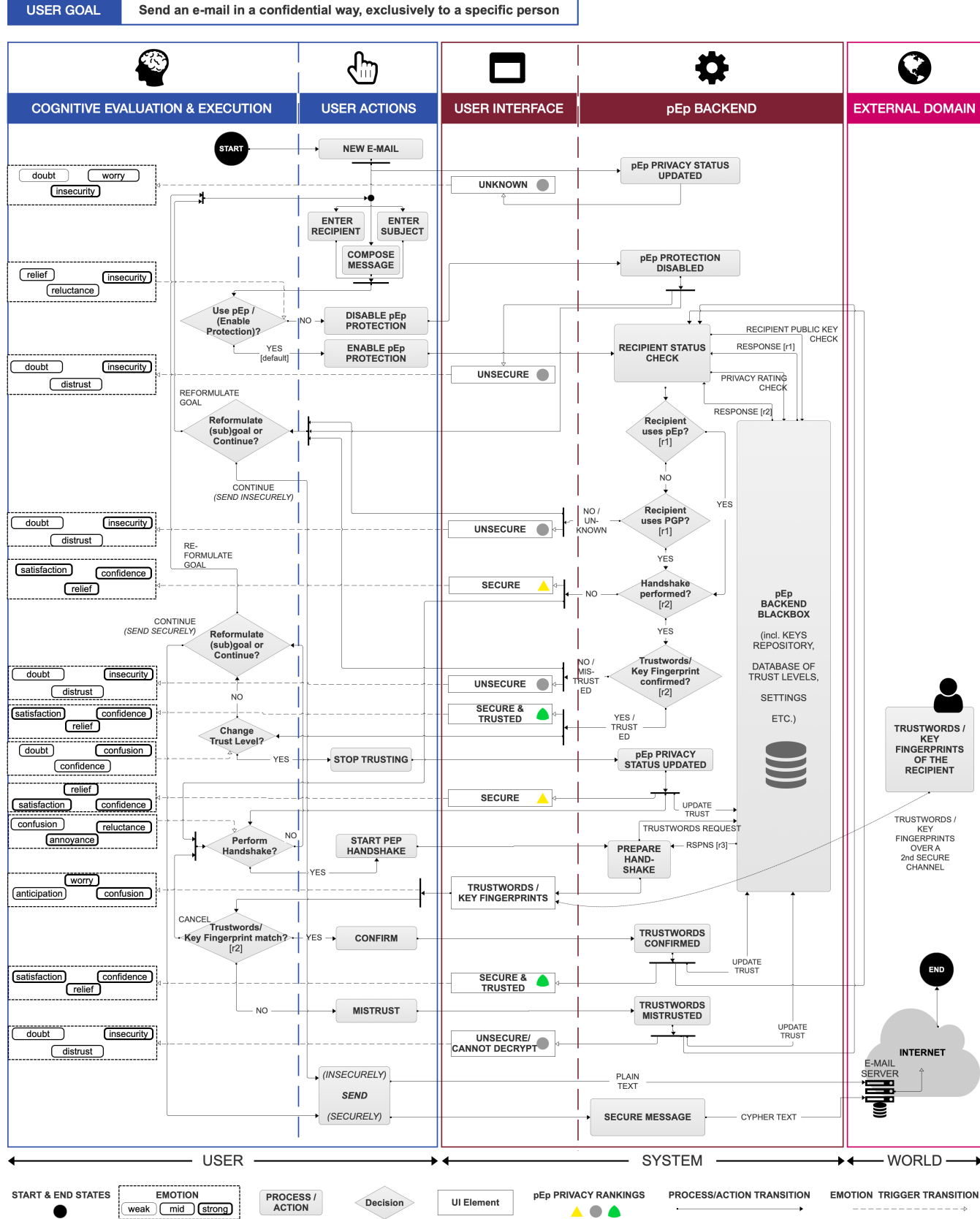
USER	SCENARIO	GOAL	EXPECTATIONS
	<hr/> <hr/> <hr/>	<hr/>	<hr/> <hr/> <hr/>

JOURNEY FLOW



LEGEND

- **START & END STATES**
- **TRANSITION**
- **PROCESS/ACTION**
- ◇ **DECISION**
- 💬 **USER THOUGHT OR EMOTIONAL RESPONSE**
- Ⓣ **TRIGGER THAT MAY LEAD TO AN EMOTIONAL OR BEHAVIORAL REACTION (A RESPONSE ON A VISCERAL, BEHAVIORAL OR REFLECTIVE LEVEL)**
- Ⓡ **REACTION INDUCED BY A TRIGGER THAT MAY IMPACT DECISION MAKING OR ACTIONS TAKEN BY THE USER**



Emotions as states in a Labelled Transition Systems

User and system's states as measurable qualities: emotions and security status

*(e.g., sense of security/confidence **vs** message is encrypted by the other party, no man-in-the-middle attacks)*

They can aligned or misaligned.

OXFORD

ALAN BRYMAN

social research
methods

4th Edition

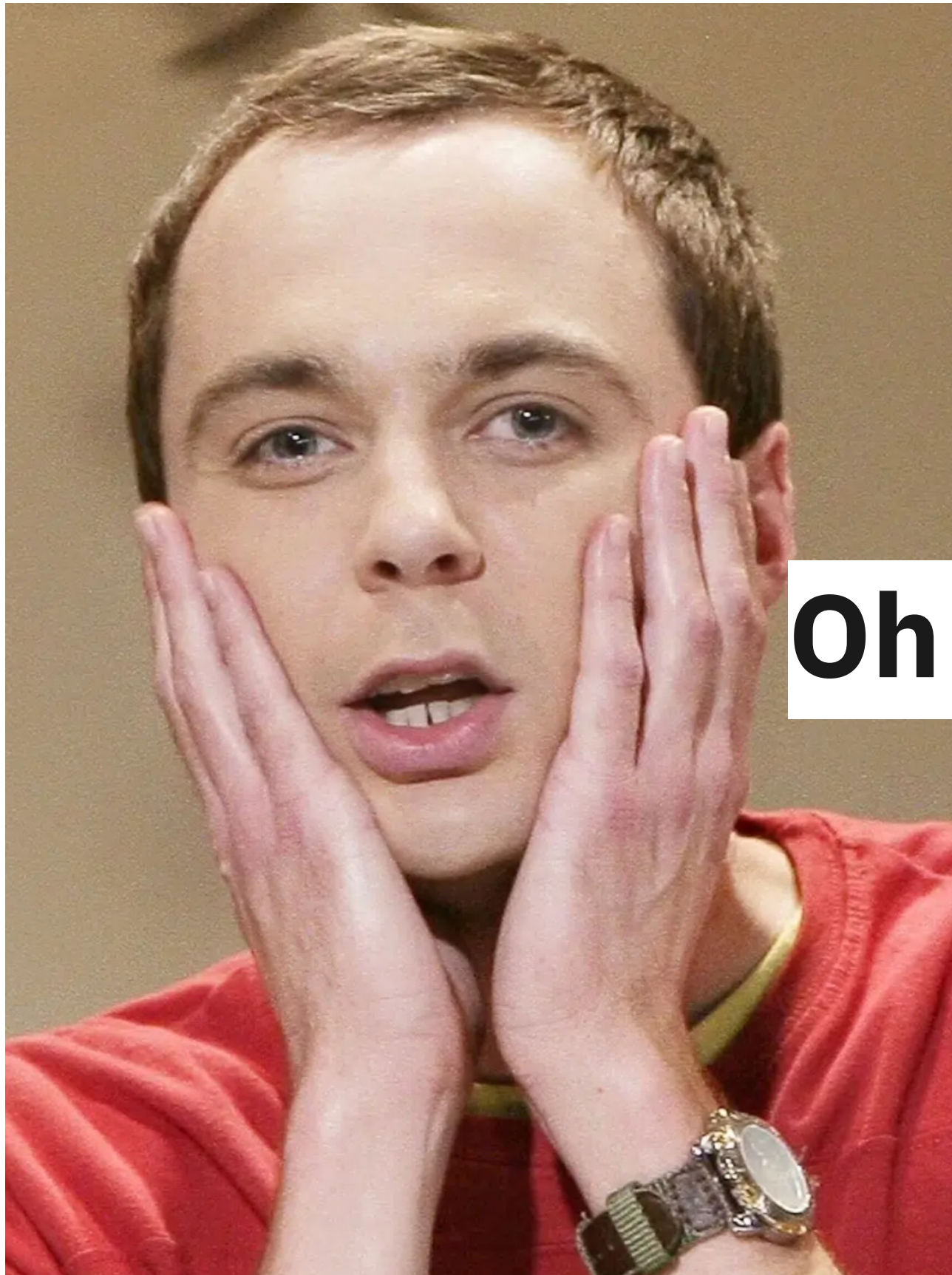


How to assess for user's emotions / mental model?

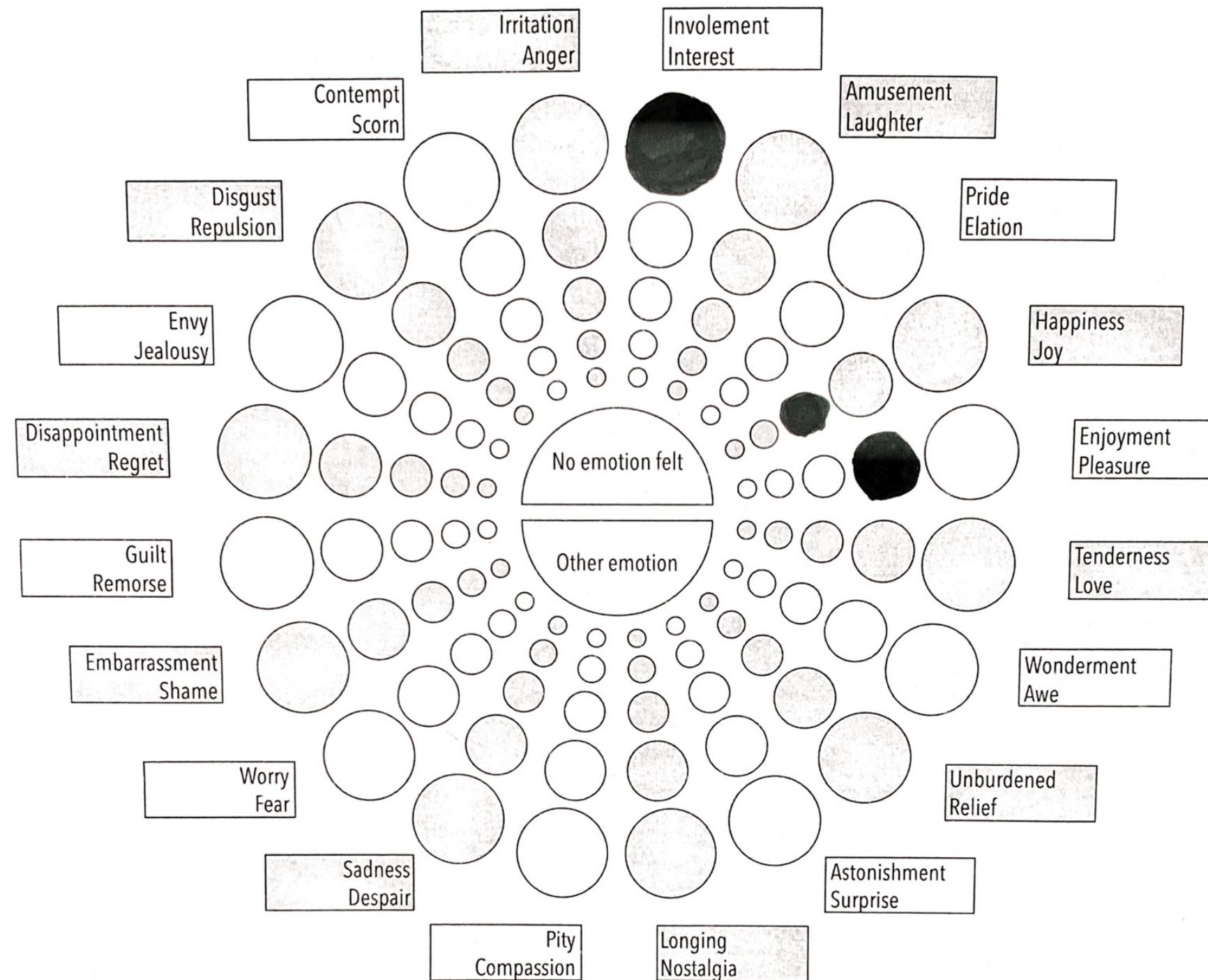


@ online
resource
centre

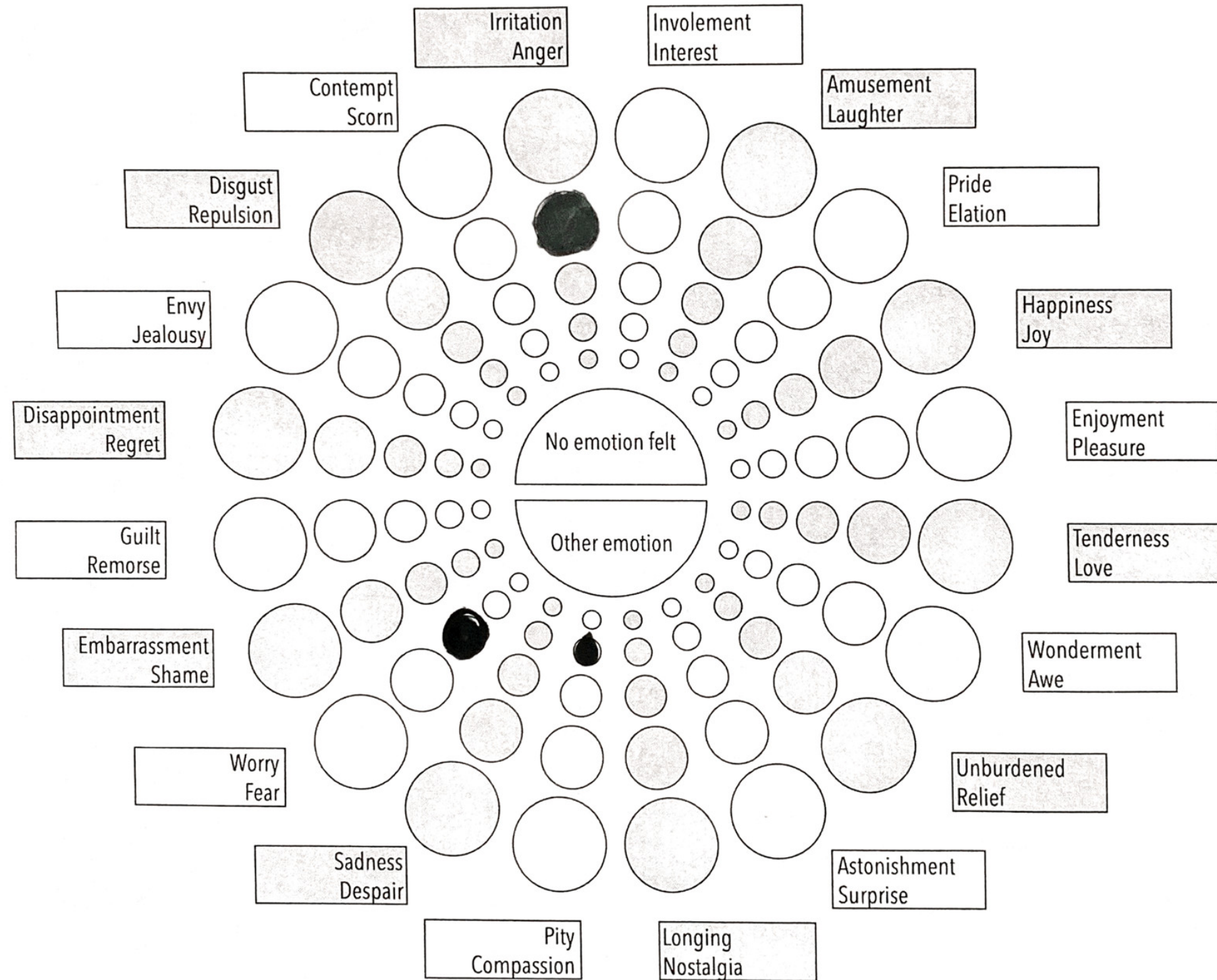
Copyrighted material



Oh no, the (in)humanities



BEFORE installing a secure email app



AFTER installing, or trying to, the app

UX Assessment

Which visual indicator do you associate with the statement:

Unreliable Security



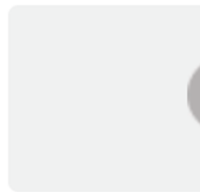
Which visual indicator do you associate with the explanation:

This message does not contain enough information to determine if it is secure.



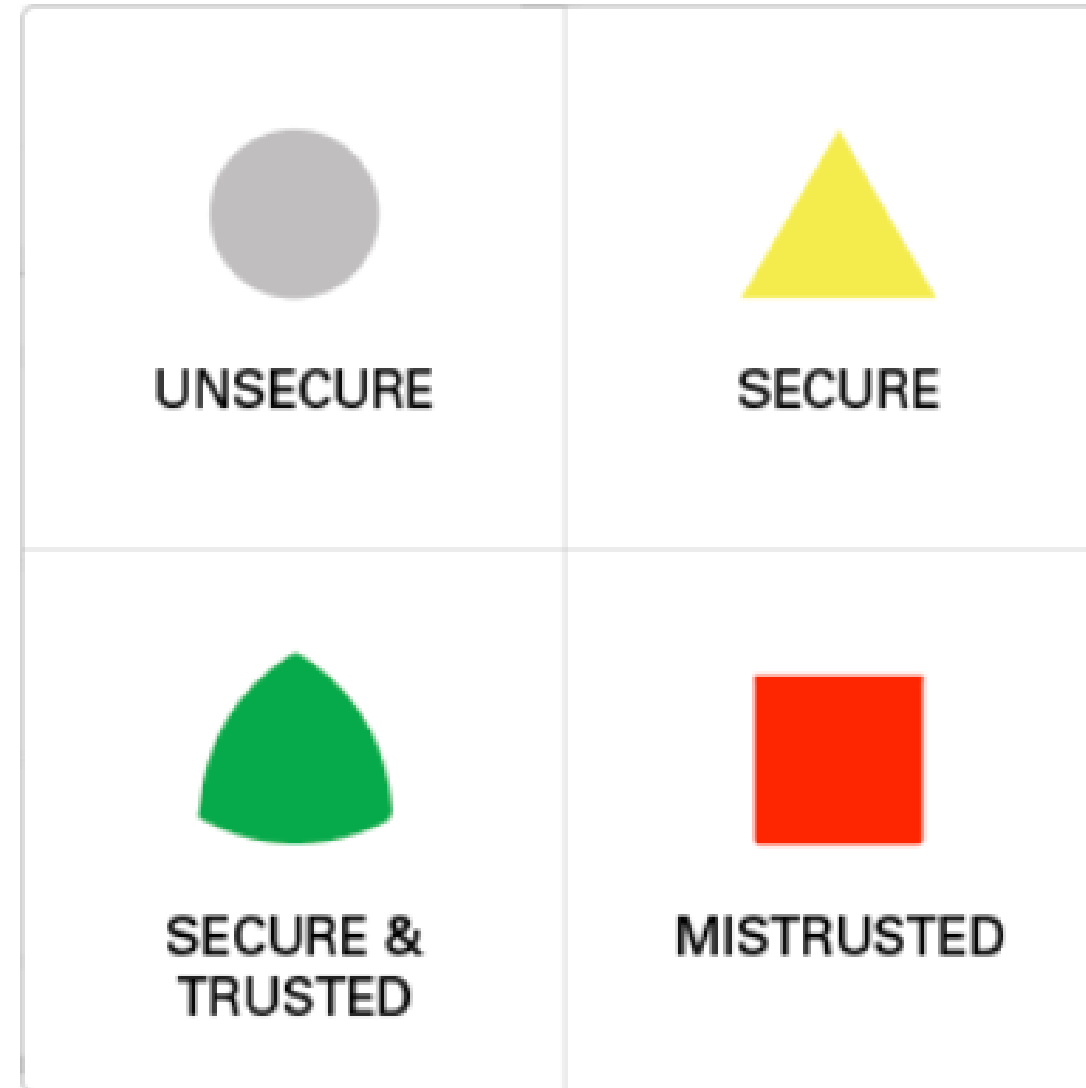
Test

Which visu
Unreliable



MATCH

NO MATCH







































(a) Old version











(b) New version

- ▶ if the icon chosen by the majority of testers is not the same as the one chosen by $p \equiv p$

ITEM		PRIVACY RATING (Statement & Explanation)	PARTICIPANTS' RESPONSES (%)					p≡p's CHOICE	MATCH STRENGTH	RESULT
							Most voted			
RQ1	1	Under Attack	0,0	2,4	<u>76,2</u>	21,4			<u>76 %</u>	MATCH
RQ2	1	This message is not secure and has been tampered with.	0,0	11,5	<u>69,2</u>	19,2			<u>69 %</u>	MATCH
RQ1	2	Broken	2,4	16,7	<u>59,5</u>	21,4			<u>60 %</u>	MATCH
RQ2	2	This message has broken encryption or formatting.	0,0	0,0	<u>38,5</u>	61,5			<u>38 %</u>	NO MATCH
RQ1	3	Mistrusted	2,4	14,3	<u>40,5</u>	42,9			<u>40 %</u>	NO MATCH
RQ2	3	This message has a communication partner that has previously been marked as mistrusted.	3,9	0,0	<u>23,1</u>	73,1			<u>23 %</u>	NO MATCH
RQ1	4	Unknown	0,0	<u>78,6</u>	2,4	19,1			<u>79 %</u>	MATCH
RQ2	4	This message does not contain enough information to determine if it is secure.	3,9	<u>23,1</u>	11,5	61,5			<u>23 %</u>	NO MATCH

RQ1	5	Cannot Decrypt	7,1	<u>28,6</u>	42,9	21,4			<u>29 %</u>	NO MATCH
RQ2	5	This message cannot be decrypted because the key is not available.	0,0	<u>38,5</u>	19,2	42,3			<u>38 %</u>	NO MATCH
RQ1	6	Unsecure	0,0	<u>11,9</u>	69,1	19,1			<u>12 %</u>	NO MATCH
RQ2	6	This message is unsecure.	0,0	<u>7,7</u>	61,5	30,8			<u>8 %</u>	NO MATCH
RQ1	7	Unsecure for Some	2,4	<u>9,5</u>	16,7	71,4			<u>10 %</u>	NO MATCH
RQ2	7	This message is unsecure for some communication partners.	0,0	<u>11,5</u>	19,2	69,2			<u>12 %</u>	NO MATCH
RQ1	8	Unreliable Security	2,4	<u>14,3</u>	26,2	57,1			<u>14 %</u>	NO MATCH
RQ2	8	This message has unreliable protection.	0,0	<u>15,4</u>	19,2	65,4			<u>15 %</u>	NO MATCH

RQ1	9	Secure	90,5	7,1	2,4	<u>0,0</u>			<u>0 %</u>	NO MATCH
RQ2	9	This message is secure but you still need to verify the identity of your communication partner.	0,0	19,2	7,7	<u>73,1</u>			<u>73 %</u>	MATCH
RQ1	10	Secure & Trusted	<u>95,2</u>	4,8	0,0	0,0			<u>95 %</u>	MATCH
RQ2	10	This message is secure and trusted.	<u>100,0</u>	0,0	0,0	0,0			<u>100 %</u>	MATCH

State	Version	#	Count	%	Proportion	95% CI*	Mean	SD	Var
M	Old	1	10	20%	P_{M-1}	0.2 [0.1124, 0.3304]	1.80	.404	.163
	New	2	40	80%	P_{M-2}	0.8 [0.6696, 0.8876]			
	Total:		50	100%		1			
S	Old	1	10	20%	P_{S-1}	0.2 [0.1124, 0.3304]	1.80	.404	.163
	New	2	40	80%	P_{S-2}	0.8 [0.6696, 0.8876]			
	Total:		50	100%		1			
S&T	Old	1	3	6%	P_{ST-1}	0.06 [0.0206, 0.1622]	1.94	.240	.058
	New	2	47	94%	P_{ST-2}	0.94 [0.8378, 0.9794]			
	Total:		50	100%		1			

*CI method: Wilson Score interval

Table 6.5: Study D - Statistics and Frequency Table

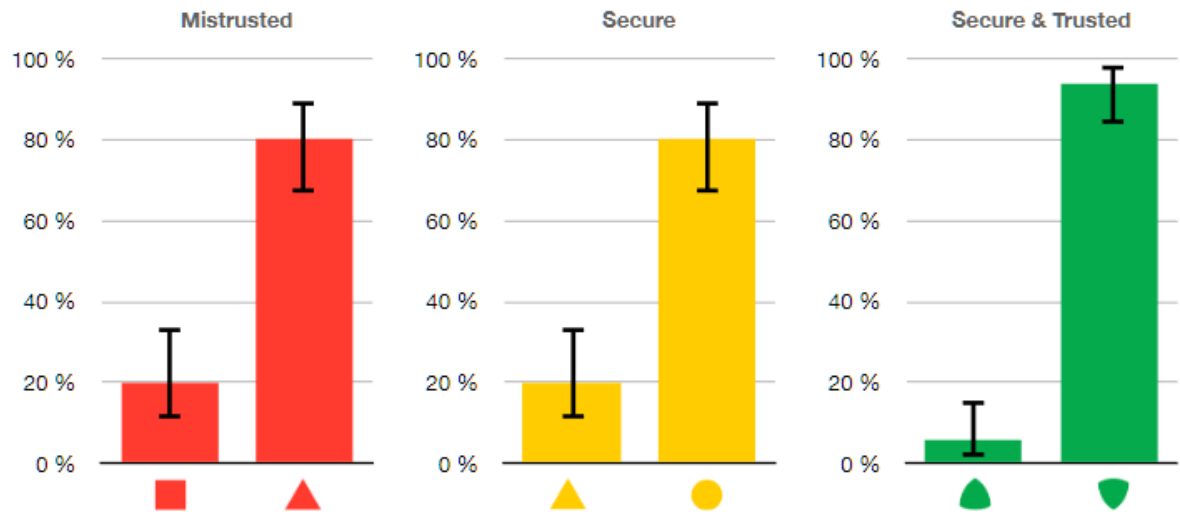


Figure 6.8: Study D - Proportions of frequencies of the two icon versions per privacy state (old vs new)

Question 1

Select the icon that matches best with the text under it?


Mistrusted


Mistrusted

☐ ☐

Question 2

Select the icon that matches best with the text under it?


Secure


Secure

☐ ☐

Question 3


Select the icon that matches best with the text under it?


Secure & Trusted


Secure & Trusted

☐ ☐

Take a look at the following icon and label under it.


Secure & Trusted

Please state whether you agree or disagree with the following statement?

Strongly disagree

Disagree

Somewhat disagree

Neither agree nor disagree

Somewhat agree

Agree

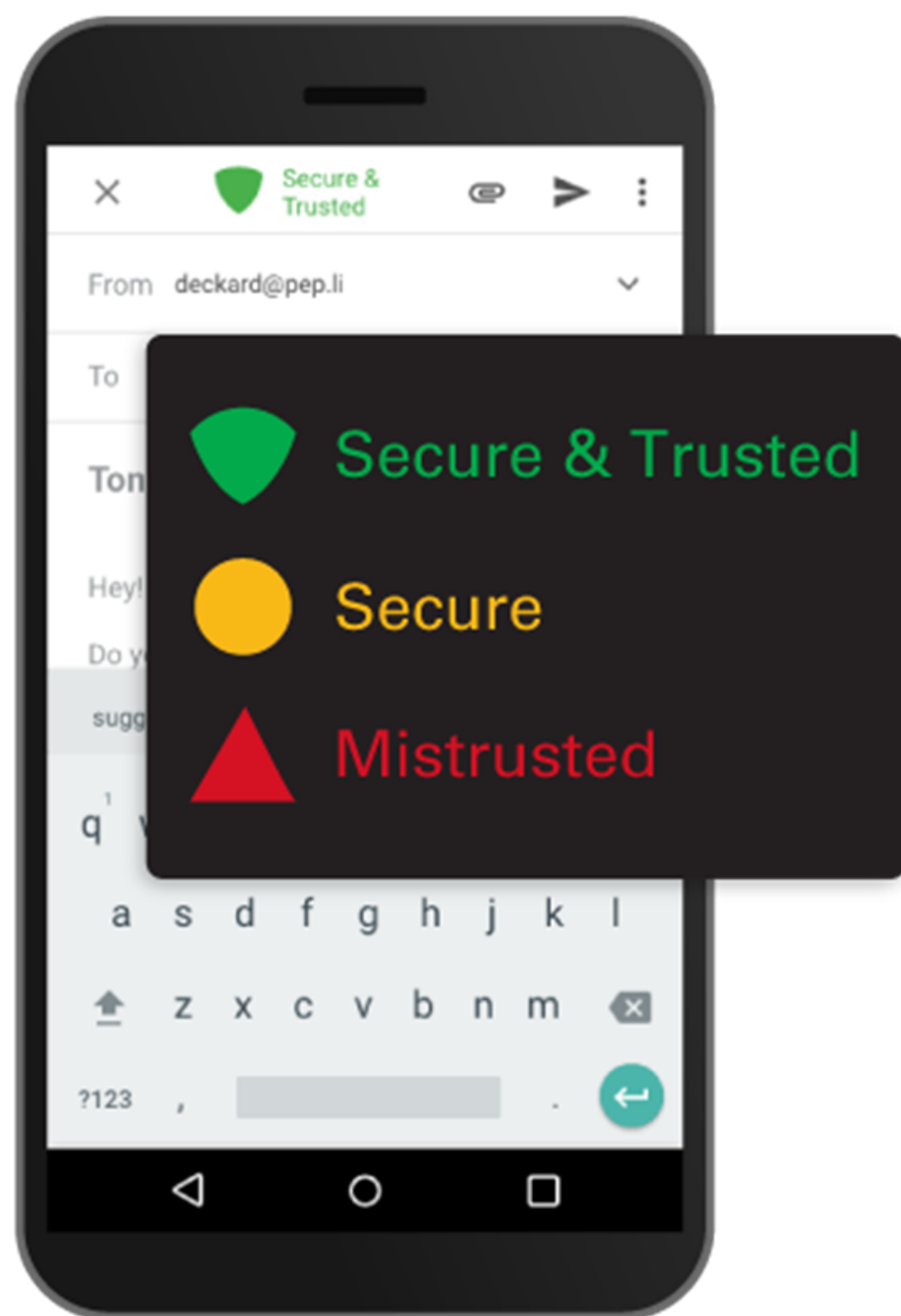
Strongly agree

☐ ☐ ☐ ☐ ☐ ☐ ☐

The icon is a good representation of the text under it.

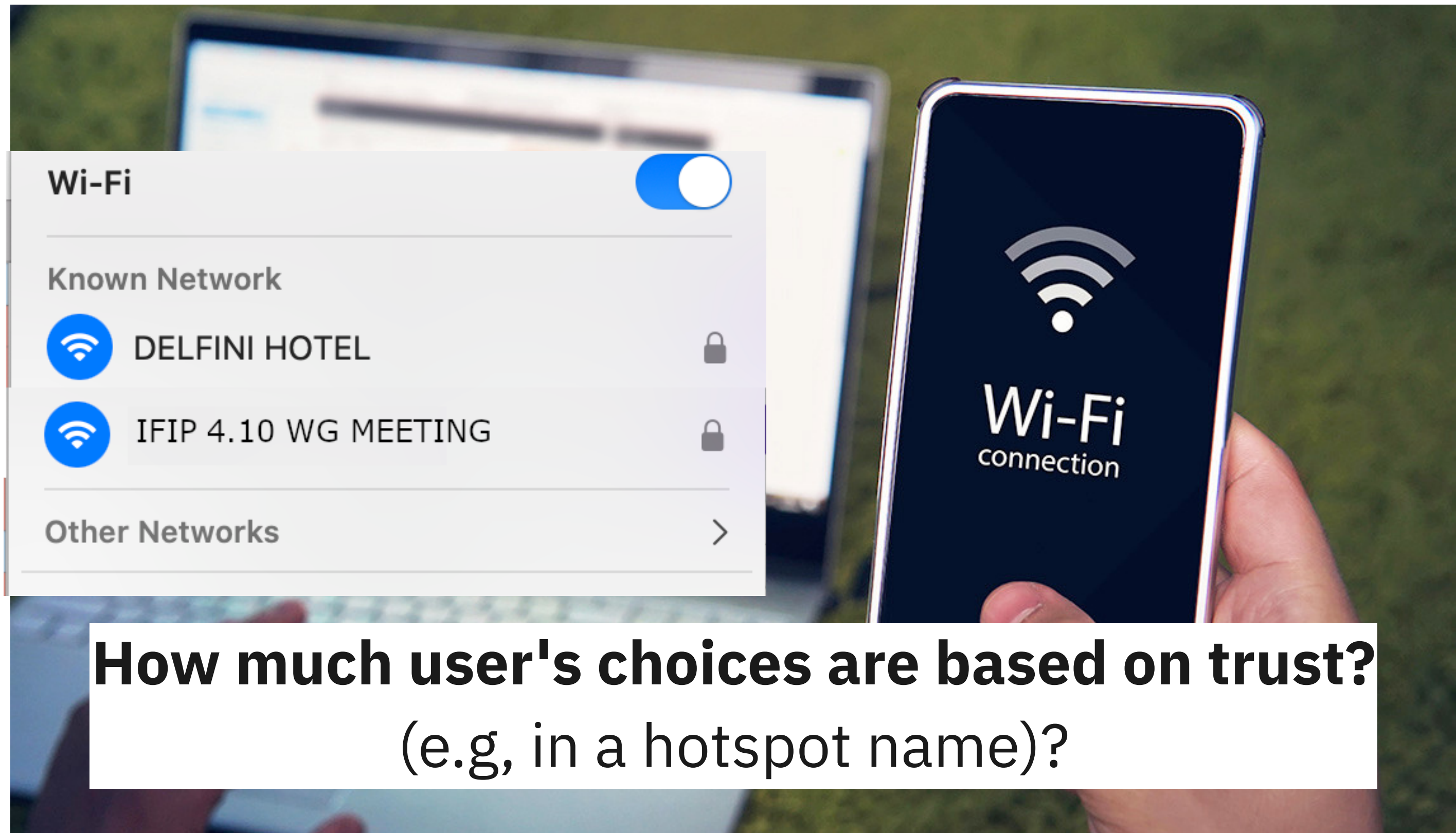
Borce Stojkovski, et al . 2019. Detecting Misalignments between System Security and User Perceptions: A Preliminary Socio-technical Analysis of an E2E email Encryption System. In 2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW).

Borce Stojkovski et al 2021. “I Personally Relate It to the Traffic Light”: A User Study on Security & Privacy Indicators in a Secure Email System Committed to Privacy by Default. In Proceedings of the 36thmAnnual ACM Symposium on Applied Computing (SAC ’21)



Use case III

Trust and the hotspot



How much user's choices are based on trust?
(e.g, in a hotspot name)?

Socio-technical Security Analysis of Wireless Hotspots

Ana Ferreira^{1,2}, Jean-Louis Huynen^{1,2}
Vincent Koenig^{1,2}, and Gabriele Lenzini^{2*}

¹ Institute of Cognitive Science and Assessment - Univ. of Luxembourg

² Interdisciplinary Centre for Security Reliability and Trust - Univ. of Luxembourg

Abstract. We present a socio-technical analysis of security of Hotspot and Hotspot 2.0. The analysis focuses is user-centric, and aim at understanding which user action can compromise security in presence of a attacker. We identify research questions about possible factors that may affect user's security decisions, and propose experiments to answer them.

Keywords: socio-technical security analysis, hotspot ceremonies

Conclusions

Human role in ST systems is not to be ignored but included in

- design
- security analysis

Human behaviour in ST systems can be, at some extend

- modelled/formalized
- studied


Conclusions

Human role in ST systems can be

- part of the solution (how?)
- harmonized with the security goals

ST security requires "interdisciplinarity"

Sign of life out there (NIST2) ..

NIST (National Institute of Standards and Technology) has updated its password guidelines and no longer recommends mandatory, periodic password changes (e.g., every 60–90 days). Instead, NIST now advises that **passwords should only be changed when there is evidence of a security breach or compromise**. This shift is based on the understanding that frequent password changes can lead to weaker, more easily guessed passwords as users often resort to minor variations of their old passwords. 

Thank you



NO SOCIOTECH



Gabriele LENZINI

SnT/University of Luxembourg

gabriele.lenzini@uni.lu



