

The Cybersecurity Planet

Giampaolo Bella

Dipartimento Matematica e Informatica
Università di Catania, Italy

Cyber Security CRC and CSIRO's Data61 joint seminar
15th December 2022

Out of some joint works and innumerable debates with
P.Biondi, L.Coles-Kemp, P.Curzon, S.Esposito, R.Giustolisi,
G.Lenzini, J.E.Martina, D.Micale, K.Renaud, P.Ryan and L.Viganò

Highlights

- Recent teaching
 - cybersecurity, data protection, offensive security
- Recent research
 - automotive, IoT, VPAs, fuzzing, security ceremonies
- Recent events
 - Security Track @ ACM Symposium in Applied Computing (SEC@SAC)
 - Workshop Socio-Technical Aspects in SecuriTy (STAST)
 - International Conference on Security for Information Technology and Communications (SECICT22)
- About
 - <https://www.dmi.unict.it/giamp/>
 - <https://www.linkedin.com/in/giampaolo-bella-a905315a/>

Latest efforts

- Designing and implementing an AUTOSAR-based Basic Software Module for enhanced security

G.Bella, P.Biondi, G.Costantino, I.Matteucci

Elsevier Computer Networks, 1389-1286, 2022. (doi: [10.1016/j.comnet.2022.109377](https://doi.org/10.1016/j.comnet.2022.109377))

- Perceptions of Beauty in Security Ceremonies

G. Bella, J. Ophoff, K. Renaud, D. Sempredoni, L. Viganò

Springer Philosophy & Technology, 35(72), 2022 -- [Link](#)

- Embedded Fuzzing: a Review of Challenges, Tools, and Solutions

M.C.Eisele, M.Maugeri, R-Shriwas, C.Huth, G.Bella

Springer Cybersecurity, 2523-3246, 2022 (doi: [10.1186/s42400-022-00123-y](https://doi.org/10.1186/s42400-022-00123-y))

- Modelling human threats in security ceremonies

G.Bella, R.Giustolisi, C.Schürmann

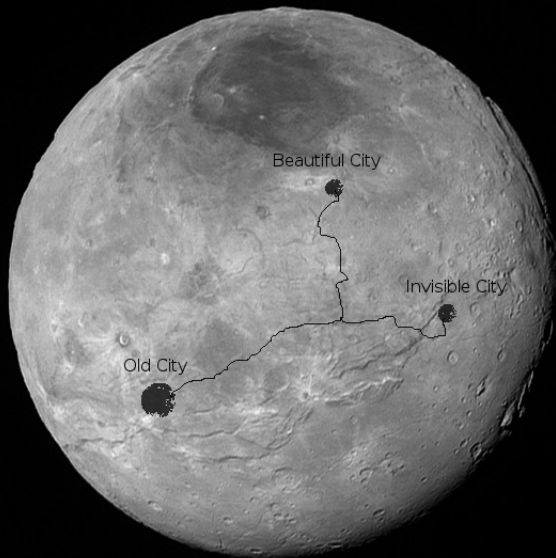
IOS Journal of Computer Security, pp.1-23, 2022. (doi: [10.3233/JCS-210059](https://doi.org/10.3233/JCS-210059)) -- [Link](#)

- Multi-service threats: Attacking and protecting network printers and VoIP phones alike

G.Bella, P.Biondi, S.Bognanni

Elsevier Internet of Things, 2542-6605, 2022. (doi: [10.1016/j.iot.2022.100507](https://doi.org/10.1016/j.iot.2022.100507)) -- [Link](#)

Early pic of Cybersecurity planet



What I found out...

JIC-05-2019-0127_proof 291..307
10-1108_jic-05-2019-0127-corrected.pdf 144%

Out to explore the cyber... 291

- Introduction 291
- The human factor 291
- Security ceremonies 292
- Hypothesis (metha... 292
- Article contribution 292
- Lexical considerati... 293
- Article structure 293
- Democratic city 293
- Dictatorial city 294
- Beautiful city 296
- Invisible city 299
- Discussion 304
- Conclusions 305
- References 306

The current issue and full text archive of this journal is available on Emerald Insight at:
<https://www.emerald.com/insight/1469-1930.htm>

Out to explore the cybersecurity planet

Giampaolo Bella

Dipartimento di Matematica e Informatica, Università di Catania, Catania, Italy

Exploring the cybersecurity planet

291

Received 31 May 2019
Revised 17 October 2019
12 December 2019
19 December 2019
Accepted 19 December 2019

Abstract

Purpose – Security ceremonies still fail despite decades of efforts by researchers and practitioners. Attacks are often a cunning amalgam of exploits for technical systems and of forms of human behaviour. For example, this is the case with the recent news headline of a large-scale attack against Electrum Bitcoin wallets, which manages to spread a malicious update of the wallet app. The author therefore sets out to look at things through a different lens.

Design/methodology/approach – The author makes the (metaphorical) hypothesis that humans arrived on Earth along with security ceremonies from a very far planet, the Cybersecurity planet. The author's hypothesis continues, in that studying (by huge telescopes) the surface of Cybersecurity in combination with the logical projection on that surface of what happens on Earth is beneficial for us earthlings.

Findings – The author has spotted four cities so far on the remote planet. *Democratic City* features security ceremonies that allow humans to follow personal paths of practice and, for example, make errors or be driven by emotions. By contrast, security ceremonies in *Dictatorial City* compel to comply, hence humans here behave like programmed automata. Security ceremonies in *Beautiful City* are so beautiful that humans just love to follow them precisely. *Invisible City* has security ceremonies that are not perceivable, hence humans feel like they never encounter any. Incidentally, the words “democratic” and “dictatorial” are used without any political connotation.

Originality/value – A key argument the author shall develop is that all cities but Democratic City address the human factor, albeit in different ways. In the light of these findings, the author will also discuss security ceremonies of our planet, such as WhatsApp Web login and flight boarding, and explore room for improving them based upon the current understanding of Cybersecurity.

Keywords Computer security, Computer privacy, Socio-technical security

Paper type Research paper

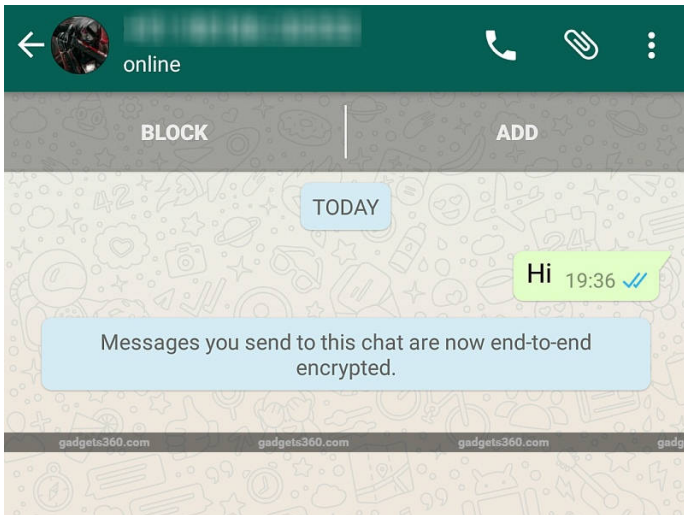
<https://arxiv.org/abs/2112.12790>

Agenda





- Hypotheses (metaphorical?)
- Known cities and neighbouring areas
 - 1 Democratic Cybersecurity (City, most similar to us!)
 - 2 Dictatorial Cybersecurity (City)
 - 3 Beautiful Cybersecurity (City)
 - 4 Invisible Cybersecurity (City)
- Open challenges and future directions

1. Democratic Cybersecurity

Technical measures exist



[Control Panel Home](#)

-  [Device Manager](#)
-  [Remote settings](#)
-  [System protection](#)
-  [Advanced system settings](#)

View basic information about your computer

Windows edition

Windows 17 Pro

© 2015 Microsoft Corporation. (Almost) All rights reserved.

System

About Windows



Windows 17

Microsoft Windows

Version 1511 (OS Build 10586.104)

© 2015 Microsoft Corporation. (Almost) All rights reserved.

The Windows 17 Pro operating system and its user interface are protected by trademark and other pending or existing intellectual property rights in the United States and other countries/regions.

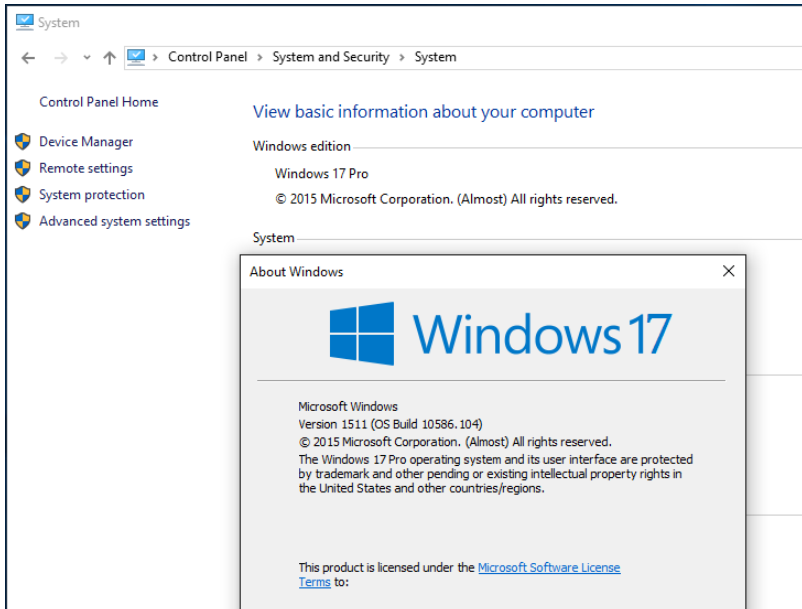
This product is licensed under the [Microsoft Software License Terms](#) to:

OK

[See also](#)

[Security and Maintenance](#)

Human factor: *deception*



Human factor: *error*



What comes to mind when you think of the causes of data loss? Hacking, viruses, natural disasters, power outages, and user error are the common culprits. But don't you think we tend to sort malicious, cybercriminal schemes and user error into separate buckets. When you review many security reports, the two appear mutually exclusive. In reality, they're more closely related than you'd think, as we depict in our latest humorous video.

User error, for instance, takes many shapes. It could be due to flippant behavior like leaving a computer unattended or knowingly accessing low security websites on company devices. Then again, it's harder to blame humans for being the agents of their own demise when you consider the prevalence of intelligent social engineering tactics that subtly break down security defenses in an organization.

In fact, findings by Federal Computer Week as relayed in a [Security Intelligence article](#) reveal that 59% of survey respondents believe "most information technology security threats that directly result from insiders are the result of innocent mistakes."

What Do We Mean by User Error?

According to [IBM's "2014 Cyber Security Intelligence Index,"](#) 95% of all security incidents involve human error.

OK sure, that sounds significant enough. But how do we *define* that human error?

It turns out that that 95% figure is largely due to email phishing, a form of social engineering. In the report, IBM claims the most common contributor to user error is "double clicking on an infected attachment or unsafe URL."

Human factor: *choice*

- Users may perceive security as a burden, e.g.
 - 2- and multi-factor authent.
 - Mastercard SecureCode vs 1-click purchase
 - Registration at first turn-on of mobile device
 - 3 passwords to secure a laptop
- Hence
 - choose to ignore it (e.g. browsers' warnings, mobile apps' permissions)
 - choose to bypass it (e.g. pics aside)



Democratic Cybersecurity

Strong human factor

- Humans interact somewhat freely with tech systems
- Combined system not necessarily secure

Many examples on Earth

- IBM X-Force Threat Intelligence Index 2018: *the potentially detrimental impact of an inadvertent insider on IT security cannot be overstated*
- Box/Dropbox file-share vulnerability
- “Frequent password changes are the enemy of security” (Ars Technica, Feb 2016)
- Many web-based attacks...

Democratic Cybersecurity in literature

- Shakespeare, Macbeth, Act 3, Scene 5:
*He shall spurn fate, scorn death, and bear
His hopes 'bove wisdom, grace, and fear.
And you all know, security is mortals' chiefest enemy*
- Freud's *fiction of omnipotence*:
“it won't happen to me”
- Nietzsche's *Turkish fatalism*:
“my computer cannot be protected”

Related work

- **Usable security** as attribute of socio-technical security
 - Learnability and simplicity don't ensure users will comply (e.g. 3 passwords at boot up; 2000 US Elections scandal)
- **Incentives or rewards** may contribute to s-t security
 - Must define the right incentive for security-compliant behaviour (e.g. why should I update my O.S.?)
- **Security economics** not to be taken for s-t security
 - Whatever good security measure must be balanced with investment to develop and deploy it

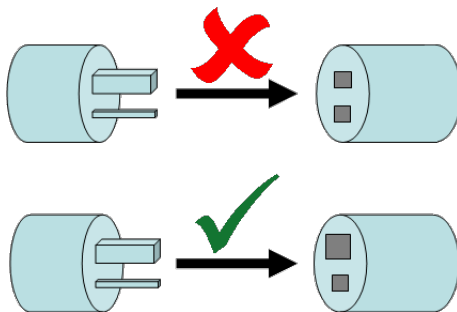
Democratic Cybersecurity: where we stand

- Long track record of attack&fix tales
- Users as “weakest link”, hardly possible to fully integrate with technology... still?
- No manuals any more, hence usability a must
- Even usability cannot ensure “user compliance”
- Dramatic need for more systematic approach
- The cybersecurity problem is still open on Earth

2. Dictatorial Cybersecurity

Dictatorial Cybersecurity

In brief: a poka-yoke



Dictatorial Cybersecurity

Almost zero-ed human factor

- Human interactions with the technical systems fully determined by the latter
- Human may only choose whether to initiate interaction

A few examples on Earth

- Password strength criteria (NIST 2004)
- Password strenght and usability criteria (NIST 2017)
- Can no longer disable authentication to mobile dev
- Training and regulations for sysadmins

Dictatorial Cybersecurity: where we stand

- Cybersecurity vs safety
- Cybersecurity more diverse hence more challenging
- Human may feel oppressed and ultimately blow up
- Yet unsure this is at all possible in general

3. Beautiful Cybersecurity

Understanding it from fiction: Peppa Pig

- Peppa: Hello, Suzy!
- Suzy: Hello, Peppa!
- Peppa: Why have you got that mask on your face?
- Suzy: So people don't know it's me. I'm in a secret club!
- Peppa: Wow! Can I be in your secret club?
- Suzy: Shh! It's not easy to get into. You have to say the secret word!
- Peppa: What word?
- Suzy: Blaba double!
- Peppa: Blaba double!
- Suzy: Right, you're in!

Understanding it from fiction: Benigni



Beautiful Cybersecurity

Account for the human factor by

- Security measure as inherent technical feature
- Security measure to add to positive experience

A few examples on Earth


- Laptop authenticated login by smart watch
- QR-code scanning rather than keying long string in
- Audio-visual cues
- Rewards
- Gamification

Beautiful Cybersecurity: perceptions



Research Article | [Open Access](#) | [Published: 30 July 2022](#)

Perceptions of Beauty in Security Ceremonies

[Giampaolo Bella](#) , [Jacques Ophoff](#), [Karen Renaud](#), [Diego Sempredoni](#) & [Luca Viganò](#)

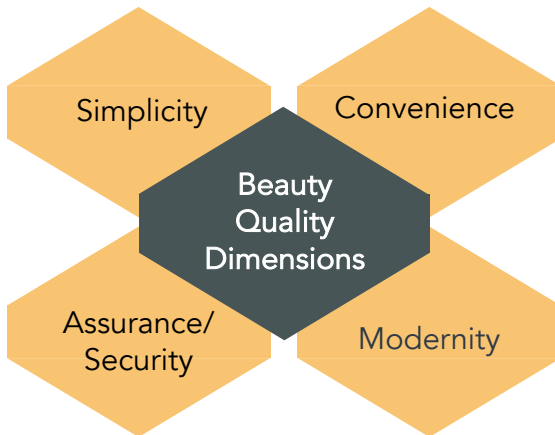
[Philosophy & Technology](#) **35**, Article number: 72 (2022) | [Cite this article](#)

1105 Accesses | **3** Altmetric | [Metrics](#)

Abstract

When we use secure computer systems, we engage with carefully orchestrated and ordered interactions called “security ceremonies”, all of which exist to assure security. A great deal of attention has been paid to improving the usability of these ceremonies over the last two decades, to make them easier for end-users to engage with. Yet, usability improvements do not seem to have endeared end users to ceremonies. As a consequence, human actors might subvert the ceremony’s processes or avoid engaging with it. Here, we consider whether *beautification* could be one way of making ceremonies more appealing. To explore beautification in this context, we carried out three studies. Study 1 surveyed 250 participants to derive a wide range of potential dimensions of “beautiful ceremonies”. These statements were sorted into dominant themes and converted into statements, which fed into the second study, with 309 respondents, to reveal the *dominant* dimensions constituting beauty. Study 3 asked 41 participants to carry out a Q-sort, which revealed the ways that people *combine* the identified dimensions when characterising security ceremonies as “beautiful”. These studies have allowed us to pin down the

Beautiful Cybersecurity: perceptions



Beautiful Cybersecurity: where we stand

- Strong subjectivity bias
- Working on “beautification process”
- Beautiful vs. secure tradeoff
- Yet unsure this is at all possible in general
- Perceptions of beauty in cybersecurity available

4. Invisible Cybersecurity

Invisible Cybersecurity

Almost zero-ed human factor

- Conceal security measure till it is invisible
- Human will not feel it

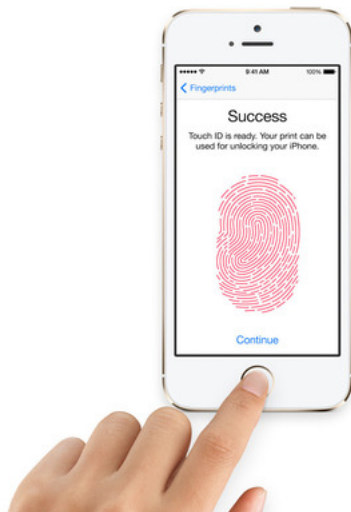
A few examples on Earth

- Mobile phone authentication
- In-restaurant payment software for cash register
- Car remote control
- Flight boarding card

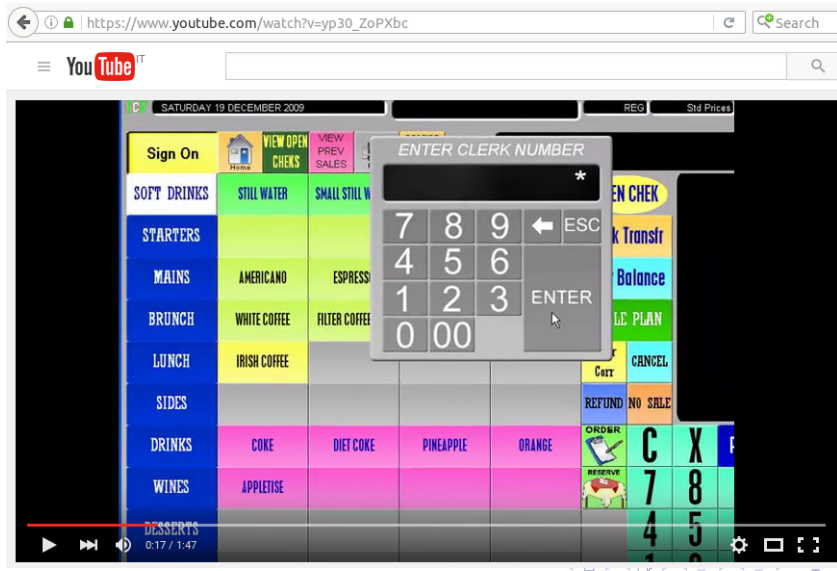
Approaches to Invisible Cybersecurity

- 1 Integrate security measure to *existing* system functionality
- 2 Integrate security measure to *new* system functionality
- 3 Integrate two or more security measures *together*
- 4 Simplify security measure *internally*

Example of approach 1: Iphone5S



Example of approach 2: ICRTouch EPoS



Example of approach 3: disc decryption

Install

Who are you?

Your name:

Your computer's name:
The name it uses when it talks to other computers.

Pick a username:

Choose a password:

Confirm your password:

☐ Log in automatically

☒ Require my password to log in

☐ Encrypt my home folder


Back Forward

► Copying files...

Example of approach 3: remote car-alarm



Example of approach 4: a boarding pass?



BRITISH AIRWAYS

CHARLTON/RICHARD
BA 269 LOS ANGELES LAX

SEAT
2A

GATE CLOSES
1545

GATE
46


CLASS
FIRST

CHECKED BY

NOT VALID FOR TRAVEL: NOT F13/1940/15618

BOARDING PASS
Carte d'accès à bord/Boardkarte/Targeta de embarque/Carta d'imbarco

SUBJECT TO CONDITIONS OF CARRIAGE, COPIES OF WHICH MAY BE OBTAINED ON REQUEST. PLEASE SEE IMPORTANT NOTICES ON THE BACK OF THIS DOCUMENT.




FIRST CLASS
PASSENGER TICKET AND BAGGAGE CHECK

NAME OF PASSENGER
CHARLTON/RICHARD


FROM LONDON HEATHROW [LHW]
TO LOS ANGELES [LAX]

CARRIER/FLIGHT	CLASS	TIME
BA 269	FIRST	1605

GATE	GATE CLOSES	SEAT	SMOKE
46	1545	2A	XX 


PCS. CK.WT. UNCK. WT. SEQ.NO.
2 0 0 146

BRITISH AIRWAYS




BRITISH AIRWAYS

BOARDING PASS



Seq. No. 001
e-ticket - no coupon



ICHIRO NIKKO you're ready to fly

Flight	From	To	Seat
BA0006	NARITA (TOKYO) Terminal 2	HEATHROW (LONDON) Terminal 5	29A

Date	Gate closes	Departure time
25 September	10:40	10:55

Operating airline	Class	Booking reference
British Airways	World Traveller	5Q46MO

BAG DROP SECURITY BOARDING



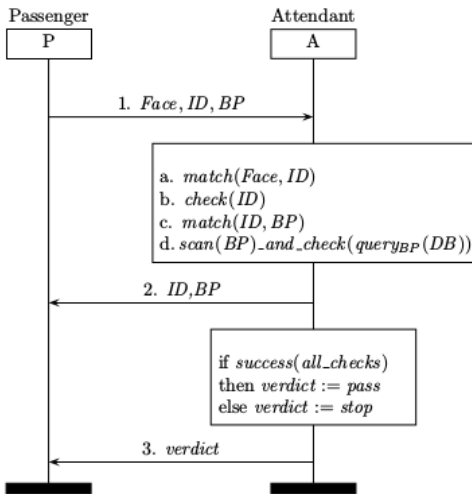
A Boarding Pass from Wikipedia

“A boarding pass is a document provided by an airline during check-in, giving a passenger permission to board the airplane for a particular flight. As a minimum, it identifies the passenger, the flight number, and the date and scheduled time for departure. ”

“Most airports and airlines have automatic readers that will verify the validity of the boarding pass at the jetway door or boarding gate.”

The flight boarding protocol

msc Flight Boarding (traditional)



- Checks a/b , c/d can be swapped
- Authentication by ID, authorisation by BP
- Check c is crucial
- Years ago:
 $d. check(BP)$

Real-world news: attack scenarios?

Ryanair passenger gets on wrong plane and flies to Sweden instead of France - Mirror Online - Chromium

M Ryanair passenger g x

www.mirror.co.uk/news/uk-news/ryanair-passenger-gets-on-wrong-plane-946207

News Politics Football Sport Celebs TV & Film Weird News Most read Videos Qu

TRENDING PANAMA PAPERS WEATHER EGYPTAIR DYNAMO RHIAN SUGDEN ROYAL FAMILY Technology Money Travel Fashion Mur

M News UK News Ryanair

Ryanair passenger gets on wrong plane and flies to Sweden instead of France

00:00, 30 JUN 2012 | UPDATED 01:06, 30 JUN 2012 | BY RICHARD SMITH

The teenager got on the flight by accident due to a last-minute gate change at Stansted

f t G+ p 193 SHARES

Enter your e-mail for our daily newsletter Subscribe

Helicopter Tour Dubai
Visit Dubai From Sky! Several Packages Available
795 AED

Real-world news: attack scenarios?

https://www.independent.co.uk/travel/news- 80%

INDEPENDENT

Support us

Contribute

Subscribe

NEWS CORONAVIRUS ADVICE UK POLITICS US POLITICS 2020 ELECTION VOICES SPORT CULTURE INDY/LIFE INDYBEST INDY100 LONG READS

INDY/LIFE



RYANAIR PASSENGER LANDS IN WRONG ITALIAN CITY

The passenger only realised when he looked out of the window and realised the landscape looked different

Helen Coffey | @LenniCoffey | Thursday 23 May 2019 12:44



Informal analysis

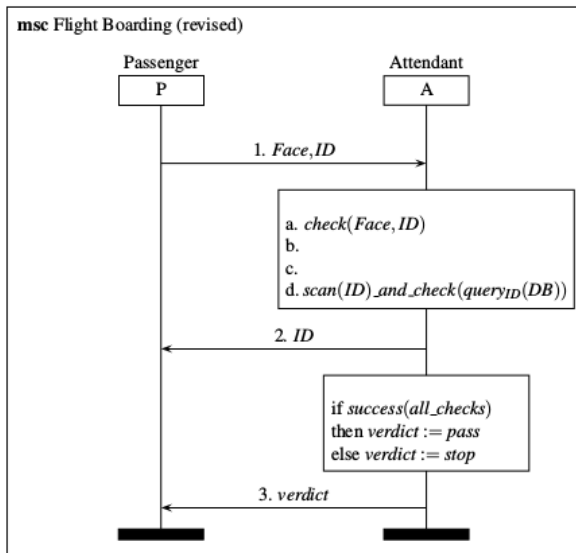
- Properties
 - 1 Authentication
 - 2 Authorisation
- Phases (country specific)
 - 1 Check-in phase (overbooking, seat choice)
 - Authentication (needed?)
 - 2 Security phase (being “clean”)
 - Authentication/Authorisation (needed?)
 - 3 Boarding phase (who boards)
 - Authentication/Authorisation
- Items
 - 1 Ticket or reservation number (needed?)
 - 2 ID
 - 3 DB
 - 4 Boarding pass (needed?)

Taking approach 4 to Invisible Security over the Boarding Phase

Challenge

Can we dispose with the boarding pass entirely and yet keep the entire protocol secure?

The flight boarding protocol revised



- **Electronic ID**
- *BP* completely disposed with
- Empty checks *b*, *c*
- *ID* used for both authentication and authorisation
- Security measure made invisible

Invisibility to attendant

- Revision 1: **Electronic ID** (just seen)
 - Empty checks b, c : security more invisible for attendant
 - Less hassle
 - Less room for “deviations” hence for human error
 - Resulting protocol more secure?
- Revision 2: **Electronic ID with biometric sample**
 - Camera or fingerprint reader
 - Check a made technical and initiated by passenger
 - Check d made technical and initiated by passenger
 - Attendant's role emptied as Agent's at Border Control

Invisibility to attendant

- Revision 1: **Electronic ID** (just seen)
 - Empty checks b, c : security more invisible for attendant
 - Less hassle
 - Less room for “deviations” hence for human error
 - Resulting protocol more secure?
- Revision 2: **Electronic ID with biometric sample**
 - Camera or fingerprint reader
 - Check a made technical and initiated by passenger
 - Check d made technical and initiated by passenger
 - Attendant's role emptied as Agent's at Border Control

Invisibility to passenger

- + Hands-free travel:
no boarding passes to carry!
- Needs to remember seat :
boarding memo vs. actual boarding pass
 - Hence just use airline or airport app

In Dubai airport...

Invisible Security prototyped for boarding protocol by means of “fish tunnel”!

Invisibility to passenger

- + Hands-free travel:
no boarding passes to carry!
- Needs to remember seat :
boarding memo vs. actual boarding pass
 - Hence just use airline or airport app

In Dubai airport. . .

Invisible Security prototyped for boarding protocol by means of “fish tunnel”!

Invisibility not always possible



TECHNICA

[BIZ & IT](#)

[TECH](#)

[SCIENCE](#)

[POLICY](#)

[CARS](#)

[GAMING & CULTURE](#)

ALEXA VS. ALEXA —

Attackers can force Amazon Echos to hack themselves with self-issued commands

Popular “smart” device follows commands issued by its own speaker. What could go wrong?

DAN GOODIN - 3/6/2022, 2:00 PM



Invisible Cybersecurity: where we stand

- Less subjectivity than with Beautiful Cybersecurity
- Reduces human intervention hence human error
- Depends on the very measure
- Invisibility may reduce awareness? So?
- Yet unsure this is at all possible in general

Conclusions — abstract

- Study the Cybersecurity planet to improve cybersecurity on Earth!
- Formalise and engineer the new cybersecurity approaches that arise

Conclusions — precise

- We need to move on from Democratic Cybersecurity
- Dictatorial cybersecurity works but may turn up frustrating
- Beautiful cybersecurity works but must be balanced to the core property and may suffer subjectivity
- Invisible cybersecurity works but may hinder awareness
- We already know that there are more cities ...