Cybersecurity: the Cross Border Perspective

Usable Authentication (UA)

Secured IT-systems and their human-centric focus

COSTIN ENACHE

- Romanian born
- Moved to Germany twenty years ago, when he co-founded Detack GmbH, a German cyber security company.
- Has often visited WA in the last years
- He has over twenty years of experience in IT security auditing and vulnerability assessment of financial institutions, state organizations and industrial enterprises and has been working as a senior security consultant and auditor on the international scene

DETACK FACTS

- Privately held (2001~)
- Ludwigsburg, Germany (2005~)
- R&D Arm: Praetors AG, Beckenried, Switzerland (2010~)
- Expertise: High-end IT security services and solutions
- Product portfolio: Premium security audits, consulting / R&D & solutions
- Certification: ISO 27001
- Activity: 70% in solutions, 30% in services
- Industry concentration to date: Finance, insurance, industry, energy
- Mining industry – Autumn 2020: Participation at virtual business delegation to Australia for German companies active in the mining industry, organised by German-Australian Chamber of Commerce with the support of German Federal Ministry for Economic Affairs and Energy

User Authentication

Definition:

- **Wikipedia**: “Authentication is the act of proving an assertion, such as the identity of a computer system user. In contrast with identification, the act of indicating a person or thing's identity, authentication is the process of verifying that identity.”

Attributes:

- **Usability / Comfort**: how easy it is for the right person to authenticate
- **Privacy**: home much private data one has to give away to authenticate
- **Intrusiveness**: level of interference in one’s private sphere required to authenticate
- **Security**: how hard it is for the wrong person to authenticate
- **Risk**: the risk level the holder of authenticated asset is exposed to (compliance + regulations set thresholds)
- **Cost**: how much it costs to set up, maintain, and support

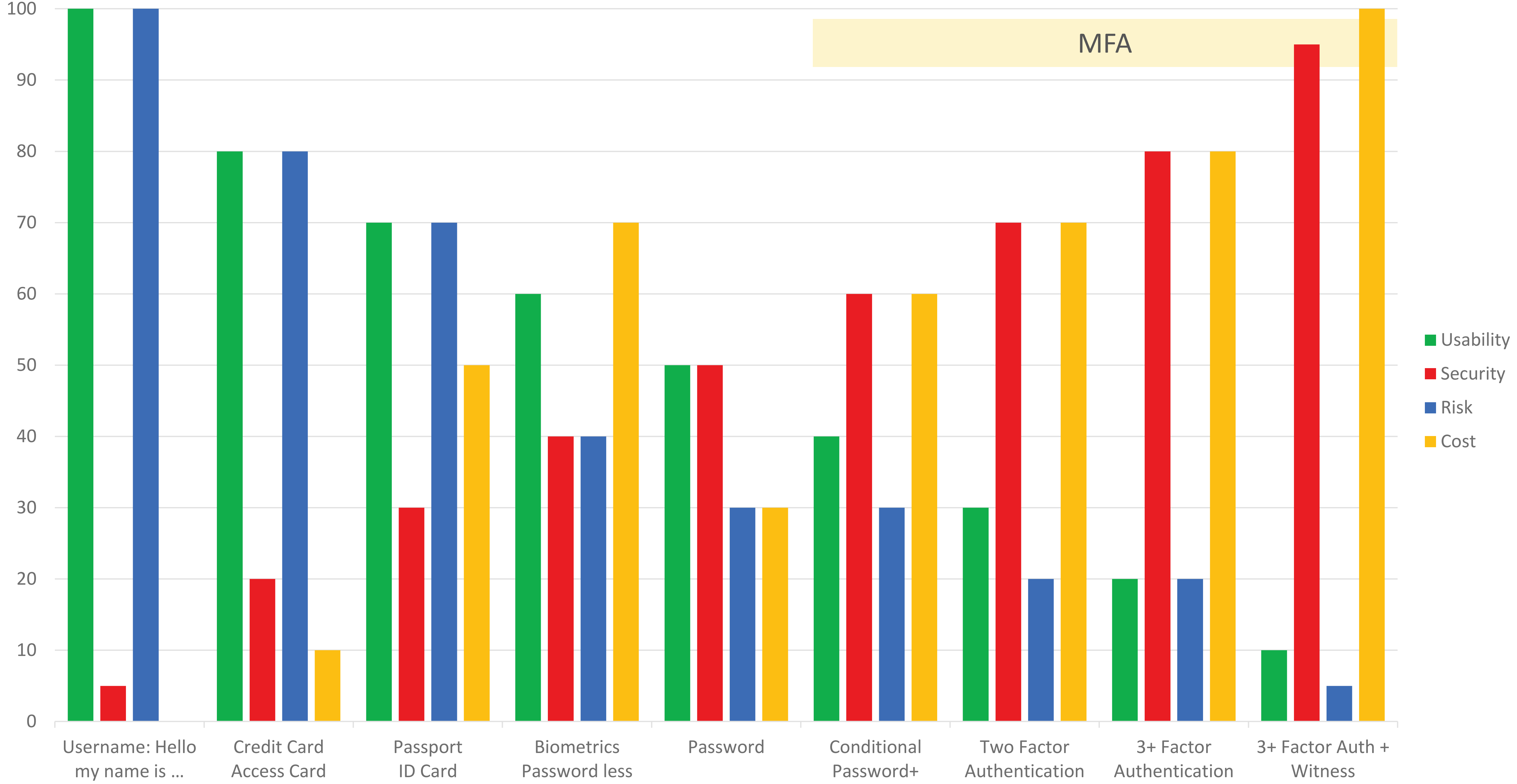
Authentication Factors

- **Something you know**: typically passwords, PINs, password phrases
- **Something you have**: car key, credit card, bank OTP token, mobile phone, identity card, passport
- **Something you are**: biometrics, e.g. fingerprints, retinas, passport photo, 3D face scan

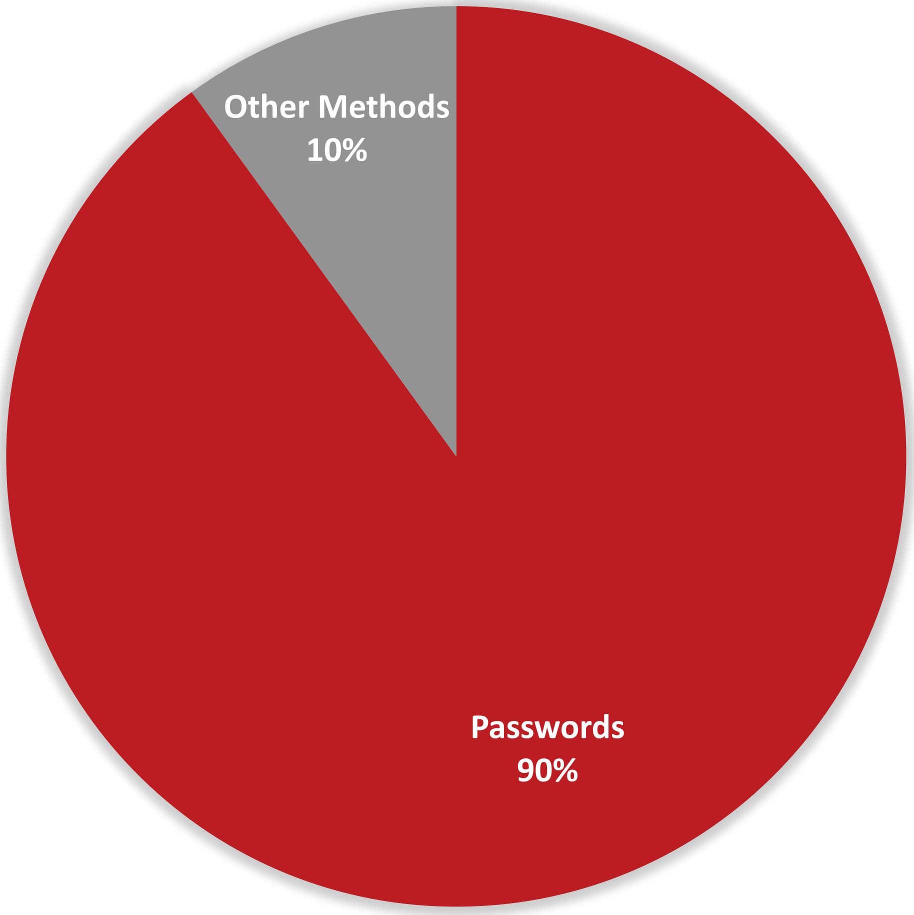
Authentication Methods

- **Single factor**: most often passwords, but occasionally biometrics (e.g. fingerprint) or object (e.g. access card)
- **Multi factor:** any combination of two or more factors, typically a password plus another factor
- **Conditional**: dynamic, most of the time single factor, with an additional factor required in case of anomalies
- **(Password less**: buzzword used in marketing of delegated solutions that minimize the use of the password**)**
- **(Delegated:** also marketing, when using Google or Microsoft or Facebook to authenticate the user**)**

Authentication Methods Comparison



Authentication Methods In Use Today



German story: PSD 2 “Strong Customer Authentication”, banks and the customers’ (lack of) acceptance – Is this the (cyber) future also for Australia?

The new EU’s Payment Services Directive “PSD2” come into force (September 2019)

The aim: to make online banking and electronic payment safer in the European Economic Area.

PSD2 and user authentication:

The user /customer has to identify yourself in two different ways to complete an online purchase or bank transaction. The two-factor authentication basically means having a customer to identify themselves with two different elements of identity from the categories of “knowledge”, “possession” or “inherence”:

“Knowledge” (something only the user knows): e.g. password or PIN
“Possession” (something only the user possesses): e.g. token or Smartphone
“Inherence” (something that identifies the payer): e.g. fingerprints

To make a payment by online bank transfer, in addition to the user ID (the account number and the password), the bank customer must enter henceforth a TAN immediately generated for the transaction by SMS, bank app or TAN generator. Alternatively, the fingerprint on the Smartphone can be used. The old paper TAN lists (iTAN) issued by German banks has been abolished and replaced with this two-factor authentication.

Although the two-factor authentication for online bank transfers is already the norm. What is new, however, is that from now customers will have to identify themselves with the two-factor authentication when they log in on their bank’s online platform. When the customers want to log into their bank account online, they not only need username and password or account number and PIN, but they also have to confirm your identity with a security procedure in a further step. To identify themselves with the two-factor authentication when they log in on their bank’s online platform is not really accepted by the customers, the most of the German banks searched for the legal possibility to avoid this, for example if the cyber risk is considered low.
Because of the lack of acceptance European Banking Authority (EBA) recommends in October 2019 that **the implementation of “Strong Customer Authentication” should be put on hold till end of 2020:** German authority BAFIN decided the same
The new deadline to implement Strong Customer Authentication (SCA) has been pushed back by fifteen month but soon the time is coming to be implemented. We will see if the customers will be now happy to accept.

What is the situation in Australia / WA ?
Have you encountered any cases related to this topic?
Who should prevail? The bank or the customer?