Bring a healthy second life to legacy password systems

Introduction - Fed up with Password?

Few people would disagree that the current form of password system is hated and fed up with. Interestingly, some people even go as far as to allege that the password should be removed from digital identity altogether.

Let us first look at the logic of the 'password-less' proposition - "The password is so vulnerable to theft and abuse. What is so vulnerable to attack is detrimental to security. Remove the detrimental element, that is, the password, and will have a solid digital identity security". Does it sound reasonable?

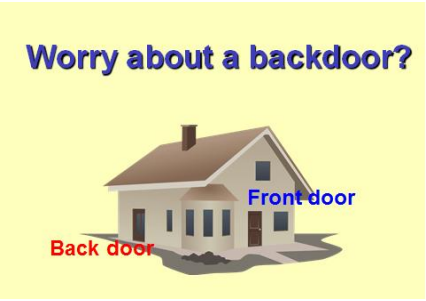
Then, what do you think about this 'army-less' proposition? – "The army is so vulnerable to air attack. What is so vulnerable to attack is detrimental to defence. Remove the detrimental element, that is, the army, and we will have a solid national defence." Does it sound reasonable as well?

We could also analyse the effect of password-less proposition from another angle; Assume that the password (what we remember) has been removed from digital identity. Then digital identity platforms would have only two authenticators - physical tokens (what we possess) and biometrics (what our body features are).

Biometrics by its probabilistic nature requires a fall-back measure against false rejection, and only the physical token could be the fall-back measure for biometrics in this situation where the password is no longer available. Here we have two scenarios.

(1) authentication by a physical token. Its security effect is plainly illustrated below.

(2) authentication by a biometric tool used in 'two-entrance' deployment (as against 'two-layer' deployment) with a physical token as the fall-back measure. Its security is even lower than (1); Math tells us that the attack surface increases in the former case, meaning that the defence is weaker.



** The opposite security effects of 'two-entrance' and 'two-layer' deployments will be closely explained later in Appendix 1.

What We Know for Certain about Various Authentication Factors

Below is all what logic leads us to.

A: 'Yes/No' on feeding correct passwords and 'Yes/No' on presenting correct tokens are deterministic, whereas biometrics which measures unpredictably variable body features of living animals in ever changing environments is probabilistic.

B: It is practically impossible to compare the security of a strong or silly password with that of a poorly or wisely deployed physical token even though both passwords and tokens are deterministic,

C: Direct comparison of something deterministic and something probabilistic would absolutely bring us nowhere.

D: Deterministic authenticators can be used on its own, whereas a probabilistic authenticator would lose its availability when used on its own.

E: Deterministic authenticators can be used together in a security-enhancing 'multi-layer' deployment, whereas probabilistic authenticators can be used with another authenticator only in a security-lowering 'multi-entrance' deployment unless we can forget the availability.

F: Removal of the password (secret credential) brings a catastrophic loss of security as examined above. It also makes a grave threat to democracy; our identity must not be established while we are asleep or otherwise unconscious in a democratic society.

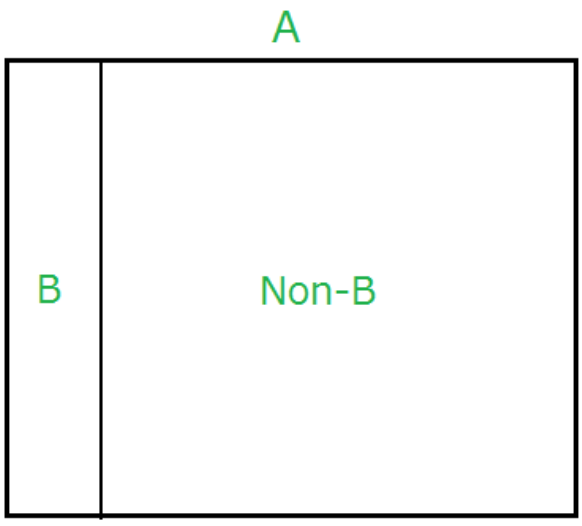
G: PIN belongs to the family of password as a numbers-only password; alleging that a password can be displaced by a PIN is like alleging that the 'knife' cab be displaced by a 'paper knife'.

H: Password, token and biometrics are 'authenticators', while two/multi-factor schemes, decentralized/distributed digital identity, single-sign-on schemes and password management tools are all 'deployment of authenticators'; We would obtain nothing by comparing the former with the latter.

Little Noticed Aspect of Non-Text Secret Credentials

Shall we start from these observations? - No safe and orderly societal life would exist without solid identity assurance. And, no solid identity assurance would exist without solid secret credential for identity authentication, whereas the text-password as a conventional secret credential is no longer manageable.

Then, we will naturally get to the observation that we could and should look to 'Non-Text' secret credential as illustrated below.



'A' is made of 'B' and 'Non-B'

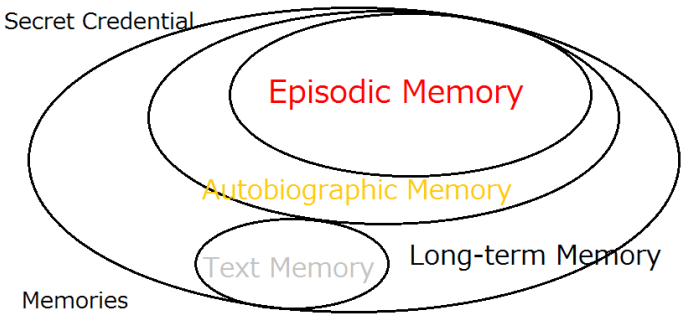
'B' is too insufficient

Where 'A' is absolutely necessary, can we afford to ignore 'Non-B'?

It's a no-brainer question

Torturous password login is history

The login can now be joyful, healing and heartening with Expanded Password System (EPS) that enables us to use our pleasant episodic image memory that had been acquired decades ago and solidly inscribed deep in our brain.



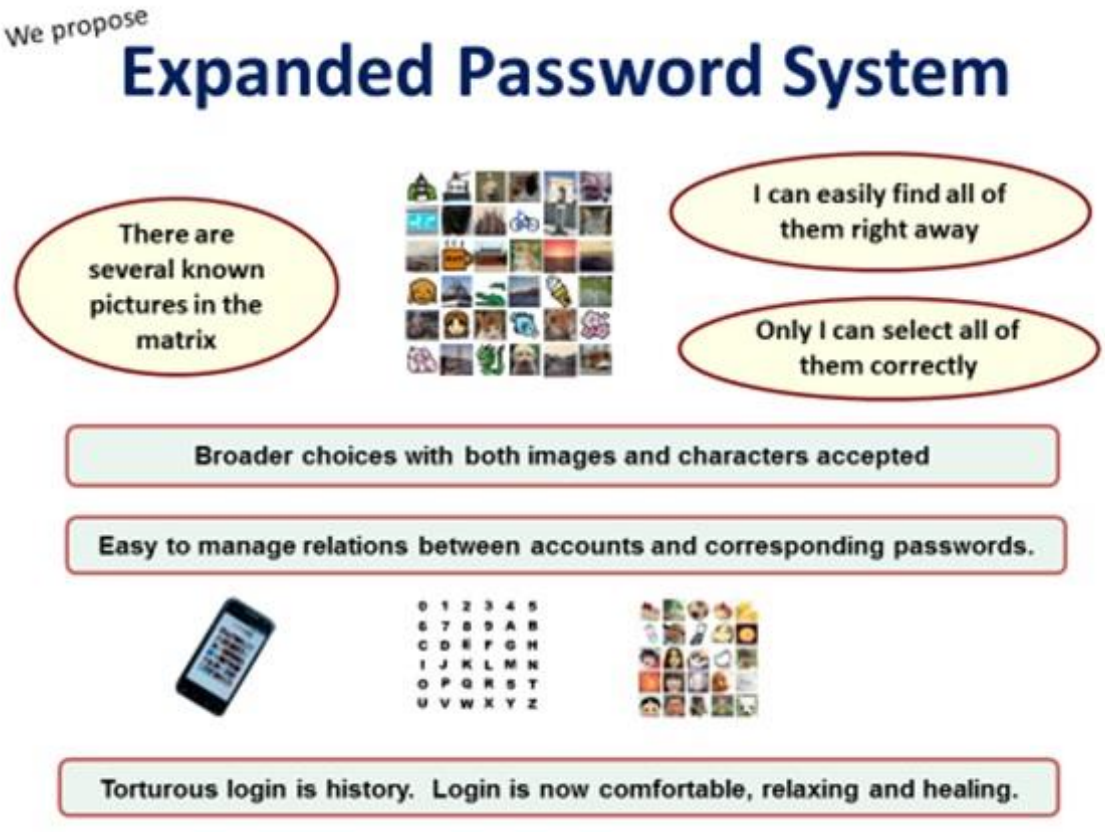
Here is a 90-second video for Expanded Password System.

By the way, ‘Easy-to-Remember’ is one thing. ‘Hard-to-Forget’ is another - The observation that images are easy to remember has been known for many decades; it is not our theme.

What we discuss is that ‘images of our emotion-coloured episodic memory’ is ‘Hard to Forget’ to the extent that it is ‘Panic-Proof

Images of toys, dolls, dogs and cats, for example, that our children used to love for years would jump into our eye even when we are placed in heavy pressure and caught in severe panic. It never fails to brings us joy and comfort.

Furthermore, Expanded Password System (EPS) brings us such desirable merits as enabling us to
(1) recognise dozens of different secret credentials effortlessly
(2) manage the correspondence between the accounts and the passwords
(3) re-generate cryptographic keys on-the-fly
(4) provide a solid defence against advanced persistent threats



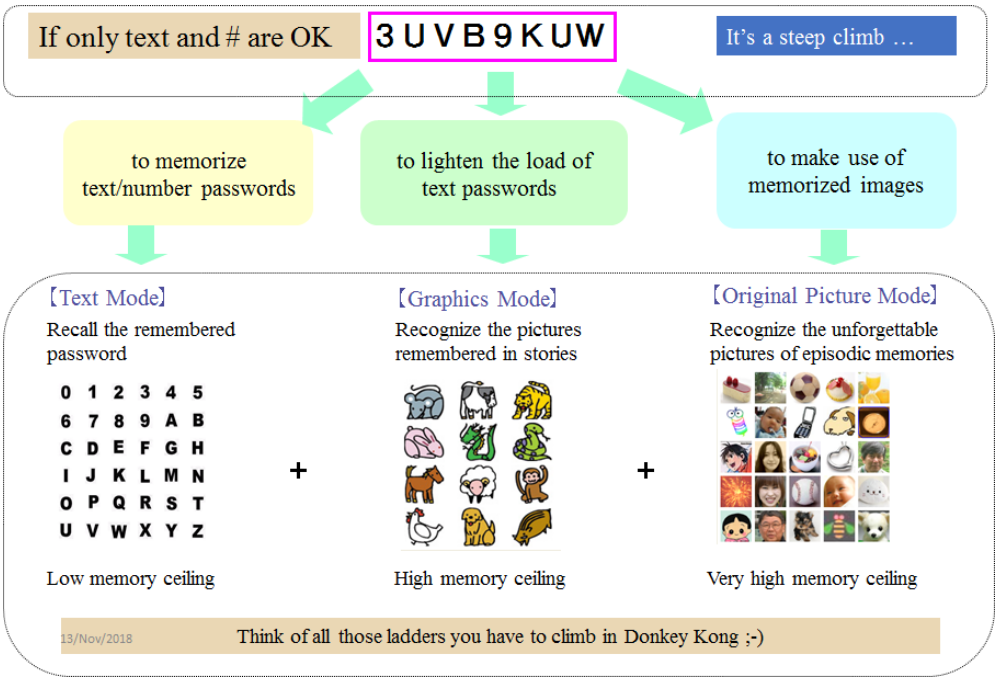
Below are the further explanations for the above.

(1) Wide choice of secret credentials

We could opt to continue to use the remembered passwords as before, although the memory ceiling is very low. Most of us can manage only up to several of them.

We could opt to recognize the pictures remembered in stories where we want to reduce a burden of textual passwords. The memory ceiling is high, that is, we would be able to manage more and more of them.

Where we opt to make use of episodic image memory, we would only need to recognize the known and hard-to-forget images. There is virtually no memory ceiling, that is, we would be able to manage as many passwords as we like, without any extra efforts.

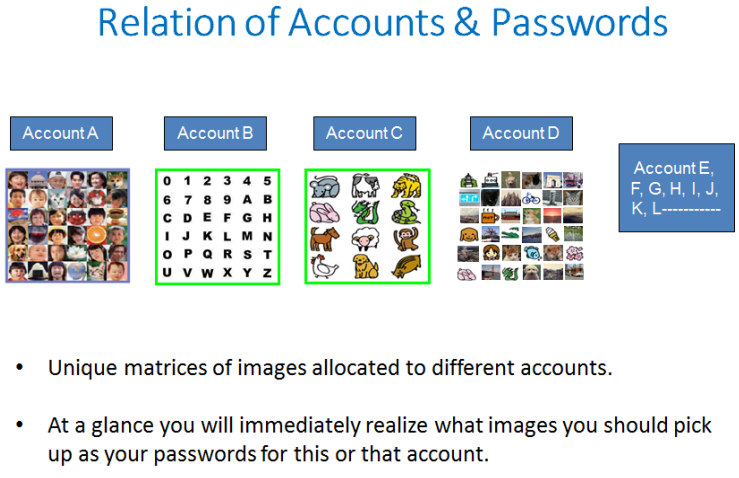


(2) Which passwords correspond to which accounts?

Being able to recall strong passwords is one thing. Being able to recall the correspondence between accounts and passwords is another.

When different sets of images are allocated to different accounts, those unique image matrices will be telling you which images you should pick up as your credential for this or that account.

When using hard-to-forget images of our episodic memories, Expanded Password System (EPS) will free us from the burden of managing the relation between accounts and the corresponding passwords.



By the way, password managers would be helpful if used modestly not to create a single point of failure, although we obviously cannot rely on them for unlocking our computers and phones offline.

(3) On-the-fly regeneration of cryptographic keys by our episodic memory

Expanded Password System, that provides 'wide choice of secret credentials' and enables us to intuitively manage 'correspondence between accounts and passwords', makes it easily practicable to get cryptographic keys re-generated on-the-fly from what we had firmly remembered as episodic memory.

This function is especially helpful for the safe account recover with distributed/decentralized identity management systems such as self-sovereign identity for which we do not presuppose a central server storing people's secret credentials.

** Try and experience the simulation of 'On-the-fly Key Re-generation' by yourself at our website https://www.mnemonicidentitysolutions.com/

Pick up 3 to 6 images and you will see a high-entropy code generated from the sum of identifier data of the images you picked up. Select the same images again and notice the same code is generated. Even when the images are shuffled, the same code is generated for the same set of images.

Assume that you had embedded and selected your 'hard-to-forget' and 'panic-proof' images of your episodic memory that had been pleasantly and solidly inscribed in your brain for years or decades and you will easily realize why EPS has been deployed for national defense in Japan for 8 years since 2013,

(4) Defence against Advanced Persistent Threats

Episodic image memory also helps us achieve such objectives as to

(1) prevent OTP-based 2-factor authentication from getting compromised
(2) come up with very resilient 2-channe/factor authentication
(3) thwart hard-to-prevent inside jobs.

as discussed closely in Appendix 2

'Visual-Manual Attack' as against 'Automated Attack'

You might have come up with this question – "Selection of several images on a matrix of 36 images, for instance, would not give us the level of entropy that we need for cybersecurity. Can we feel safe?"

Our answer is "We could consider the threats of 'visual-manual attacks on display' and 'automated attacks on stored data' separately, say, we should be able to think of the measures to cope with them separately.

A figure of '20-bit', for instance, would be just a bad joke against automated attacks on stored data, whereas it would make a pretty tall wall against visual-manual attacks on display, particularly when the positions of images are shuffled on each trial. And, we know that shoulder-surfing could be thwarted effectively.

As for what level of mathematical strength humans' image memory can generate/regenerate against automated attacks, you could try the image-to-code conversion at our website https://www.mnemonicidentitysolutions.com/

Bring a healthy second life to legacy password systems

No need to replace or re-build the existing text password systems for implementing Expanded Password System for achieving higher security as well as better user-friendliness.

Hearing Expanded Password System (EPS) accepts non-text memory objects such as visual images as well as texts, you might be led to suppose that you need to consider a big investment to replace or re-build the existing text password systems.

It is not the case. All that you need to do is ensure that your password system accepts very long passwords, desirably hundreds of characters, for obtaining very high-entropy hashed values that can stand fierce brute force attacks.

Generating High-Entropy Password like

xtyax9d4294dlelEYVz
wo/gadleowUxO93/x7
?lwble84xo9xloPxLxeo
dtyYDidex&&xeigo@y...
.....Hwx

Decades-old conventional text password systems would be able to enjoy a healthy second life where our EPS-enabled password regeneration module for the global citizens becomes available.

Who Adopted EPS for What?

A telecom company who built a payment system designed for a million online shoppers adopted EPS for accepting ‘Hard-to-Forget’ and yet ‘Hard-to-Break’ credentials and for reducing the helpdesk cost drastically. Actually 140,000 online shoppers enjoyed the no friction login for 5 years.

An IT corporation who built a security-conscious corporate network adopted EPS deployed in 2-channel/2-factor scheme for accepting ‘Very Hard-to-Break’ and yet ‘Hard-to-Forget’ credentials. 1,200 employees have long enjoyed the good balance of security and usability.

Japan’s Self-Defence Ground Force, aka, Army, adopted our product for accepting ‘Panic-Proof’ and yet ‘Hard-to-Break’ credentials. The number of licenses has increased more than 10-fold over the 8-year period from 2013 and is set to increase further.

When and how EPS was developed?

With the core concept invented in early 2000, we launched the business operation in late 2001 under the name of Mnemonic Security, Inc, which was the world’s first company to provide the software products that offer ‘Hard-to-Forget’, ‘Hard-to-Break’ and ‘Panic-Proof’ digital identity authentication. The business progressed successfully with US$1m commercial adoptions over the first several years.

We started, however, to feel the painful headwind from around 2008; People got carried away by the hype of wrongly-used biometrics, particularly overwhelming in Japan, which drove us to decide not to stick to the activity in Japan.

We have successfully made a tangible progress since then. The solid theory of our EPS proposition is made clear by OASIS recognition as a standard candidate, publishing by Taylor & Francis, selection as a finalist by Financial Data and Technology Association for ‘Summit and Awards 2019’ in Edinburgh and adoption by AFCEA for ‘2020 Solution Review Problem Sets’. We are steadily getting recognized as Pioneer and Thought Leader in this domain.

*** The invention process is summarised in Appendix 3.

Launching the global operations from UK

We registered Mnemonic Identity Solutions Limited in UK in August 2020 as the global headquarters with the mission of globally promoting 'identity assurance by our own volition and memory for 'secure digital identity in post-pandemic cyberspace.

The aim of our enterprise is to make EPS solutions readily available to all the global citizens: rich and poor, young and old, healthy and disabled, literate and illiterate, in peace and in disaster.

We expect EPS to stay with us over many generations until humans discover something other than Digital Identity for our safe and orderly societal life. We look to the people who share such a long-term view and support us as such.

Once the Covid pandemic subsides in UK and Japan, we will resume the active pursuit of the global objective.

Hitoshi Kokumai
Managing Director, Mnemonic Identity Solutions Limited

Profile: Hitoshi kokumai is an advocate of 'Identity Assurance by Our Own Volition and Memory' and the inventor of Expanded Password System that enables people to make use of episodic image memories for intuitive and secure identity authentication. Besides that, he has kept raising the issue of wrong usage of biometrics and the false sense of security it brings for 20 years.
https://www.linkedin.com/today/author/hitoshikokumai

……

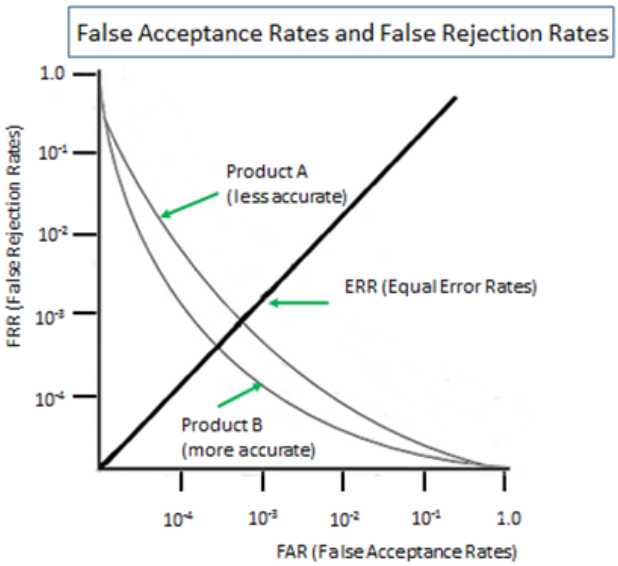
Appendix 1 - Quantitative Examination of Multiple Authenticator Deployment

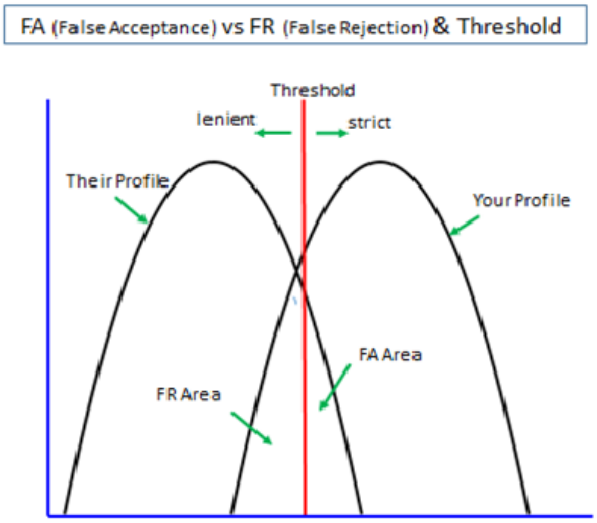
It appears that there are so many security professionals who pay no attention to the exactly opposite effects of 'multi-layer' and 'multi-entrance deployments. 'Multi-Layer' is also represented by 'In-Series', 'In-Addition-To', 'All/BothAnd' and 'Conjunction' in logic, while 'Multi-Entrance' by 'In-Parallel', 'In-Stead-Of', 'EitherOr' and 'Disjunction'. Let me offer a quantitative examination of multiple authenticators deployed in two different ways.

Vulnerability (attack surface) of an authenticator is generally presented as a figure between 0 and 1. The larger the figure is, the larger the attack surface is, i.e., the more vulnerable. Assume, for instance, as just a thought experiment, that the vulnerability of the PKI-enabled token (x) be 1/10,000 and that of the password (y) be 10 times more vulnerable, say. 1/1,000. When the two are deployed in 'multi-layer' method, the total vulnerability (attack surface) is the product of the two, say, (x) and (y) multiplied. The figure of 1/10,000,000 means it is 1,000 times more secure than (x) alone.

On the other hand, when the two authenticators are deployed in 'multi-entrance' method, the total vulnerability (attack surface) is obtained by (x) + (y) – (xy), approximately 0.0011. It is about 11 times less secure than (x) alone. So long as the figures are below 1, whatever figures are given to (x) and (y), deployment of 2 authenticators in 'multi-layer' method brings higher security while 'multi-entrance' deployment brings lower security. As such 'multi-layer' and 'multi-entrance' must be distinctly separated when talking about security effects of multiple authenticators.

The same calculation applies to biometrics used in cyber space where it has to rely on a fallback password/PIN deployed in 'multi-entrance' method against false rejection. You might assume that biometrics deployed with a password/PIN in 'multi-layer' method should bring us a very high security. But, very sadly, this scenario never comes true. When rejected by biometrics, what can we do? We will only see that we are unable to login even if we can feed our password/PIN.





The above graphs show why false acceptance and false rejection are inevitable with probabilistic biometrics. A falsely rejected person need to be rescued by a fall-back measure.

Footnote: Some people may wonder why (xy) is deducted from the sum of (x)+(y).

When (x) and (y) is very small, the (xy) is very close to 0, which we can practically ignore. But we should not ignore it when the figures are considerably large.

Suppose a case that both the two authenticators are deployed in an extremely careless manner, for instance, that the attack surfaces of (x) and (y) reach 70% (0.7) and 60% (0.6) respectively. If simply added the figure would be 130% (1.3). It conflicts with the starting proposition the figures being between 0 and 1.

Imagine a white surface area. Painting 70% of it in black leaves 30% white surface. Painting 60% of the remaining 30% in black will result in 88% black and 12% white surfaces. Painting 60% first in black and then painting 70% of the remaining 40% brings the same result of 88% black and 12% white. So does "(x)+(y)¬-(xy)". The overall vulnerability (attack surface) is 0.88 (88%) in this case.

Appendix 2 - Advanced Persistent Threats in Digital Identity

We could make meaningful contributions in these areas as (1) preventing the compromise of an OTP (one time password) from affecting the overall security of 2F authentication, (2) preventing the OTP from getting compromised in the first place and (3) preventing the inside jobs.

Below are the conclusions that we reached.

1. Making a password drastically stronger will help.

We could consider an extremely simple quasi-two-factor authentication made of a remembered password (what we remember) and a memo/storage with a long random password written/stored on (what we possess), which we can use right away at no cost. If properly hashed, the resulting high-entropy hashed value can stand fierce brute force attacks. Theft/copy of the memo/storage alone would not affect when the remembered password is unknown to the criminals.

Then, 'Image-to-Password Conversion' , when put on the market as an app software, will bring better balance of security and user-friendliness at a much higher level.

2. EPS-applied 2-channel authentication will help.

With our 2-channel scheme, the onetime code can be recovered and sent to the server only by the legitimate user who retains the secret credential in their brain.

Further details are provided in this slide "2-Channel Authentication with No Physical Tokens and No SMS" for the specifics.

It is also referred to as a powerful phishing deterrent in "Targeted/Spear Phishing and Expanded Password System"

This 2-channel scheme is not just a hypothesis, but was actually implemented in the real world for corporate use.

3. Distributed cryptographic solution could help.

An encryption key gets reproduced by any combination of 3 out of 10 registered operators, for instance, and gets eliminated after operation. It would be extremely hard to quietly bribe or threaten 3 people at a time
o

This scheme is not just a concept but the prototype software proved to work.

Appendix 3 - When and how Expanded Password System was invented?

The concept of our Expanded Password System was born in early 2000 when we were talking with our patent attorney about a 2-dimensional code like QR Code applied to security of telecommunications.

The first idea was to print a 2D code that stores a long password on a piece of card. Freed from the burden of remembering hard-to-remember passwords, we would be able to make logins just by scanning the 2D code sitting on the card. This idea was, however, thrown away a few hours later because such a card is so easily left behind, lost, stolen, copied and abused.

The second idea was a Pattern-On-Grid made of dozens of 2D codes printed on a card. A criminal, if they has access to the card, would still have to try all the possible combinations, whereas the user would only need to remember the positions and patterns. We produced a prototype system and announced it at a local trade fair with such a catchphrase as "Hide a tree in a forest". This project was thrown away half a year later. We came to conclude through repeated trials that this was just a castle on the sand. Easy-to-remember patterns are known to criminals. Complicated patterns unknown to criminals are hard for us to remember.

The third idea was to put different graphics or emoji to 2D codes. We thought that graphics and emoji should be easier to remember. When preparing for patent applications, we realized that we could do with only the pictures and threw away 2D codes altogether.

Shortly thereafter, very fortunately, we got acquainted with researchers of cognitive psychology, from whom we learnt the merits of making use of our autobiographic image memory.

At that time, we reckoned that people would be crying about the password predicament in several years and we should prepare ourselves for it in time. Our government agencies were very supportive in those days and we were able to come up with the basic line-up of software products in 2004 – 2008, having made some sales to a couple of forward-looking corporate customers.

In retrospect we apparently launched this enterprise too early. People did not start crying about the password predicament and media remained quiet until recently.