Get ahead Coming Disruptions in Cyber Security by Working Collaboratively

Christine Ziske, Kikusema AB, Mariestad, Sweden
christine.ziske@kikusemamail.de
Ulf Ziske, KikuSema GmbH, Berlin, Germany
ulf.ziske@kikusemamail.de

Abstract:
Today's authentication is based on Multi-Factor-Authentication using combinations of passwords, software token, hardware token and biometrics. But these tools don't really avoid that 95% of the breaches go directly through the front door. When the hackers have entered they'll have access to all secrets.
The objective should be that the unauthorized access to users' credentials does no longer lead to serious consequences. A new kind of security is needed. We must overcome the so-called 'Keyhole Security' by a stepwise transition into a world of diversity of secret items and Collaborative Security. Security is only guaranteed if several different instances participate in the process based on mutual trust and coincidence of interests. Each 'value' or 'secret' must be protected by encrypting instead of only locking the door.
The human factor must be strengthened. We are convinced that the human factor is an essential factor within the authentication process and need to be supported and augmented by tools.
To explain our concept of Collaborated Security we introduce new terms: The Pass Space and Scrambled Secrets.
One possible functioning of Collaborated Security can be visualized by a Pass Space with 1350 spheres.
The Pass Space contains security related data, like user accounts, data, bank accounts, technical information, executable programs.
The Pass Space can be manipulated by the involved instances or by tools, i.e. human actions, biometrics, software, servers and 'salted' passwords. By using the Pass Space you'll get 'Scrambled Secrets'. Scrambled Secrets is a security algorithm containing several components and using simultaneously multiple keys or only one key. The idea behind the Scrambled Secrets is not only locking the door of your 'safe' by using a simple 'True-False-Authentication-Mechanisms' but rather protecting your values and transactions themselves by encrypting.
To demonstrate our ideas and to spread the technical feasibility, we've developed apps and protocols.
The app Scrambled Secrets demonstrates the functioning of Collaborative Security. The APP FabulaRosa supports users in dealing with passwords or memorized secrets by augmenting their abilities. The Five New Protocols are aimed to the whole authentication process.

Keywords: Collaborative Security, Multi-Instance-Mode, Split-Key-Approach, Pass Space, Scrambled Secrets, Human-Factor

1. Crisis of the Virtual Word

In decades there will be a crisis in Information and Communication Technology comparable to the banking crisis. The impact will not remain virtual. An expected loss of confidence in the Internet, apps and enterprises will be generate huge and real economic deficits. The diversification into many small 'islands of trust' and Collaborate Security could tone down this crisis. (Ziske, 2015)
According to Sun Tzu, it says: Whoever defeats the enemy without battle really understands warfare (Sunzi, 2011) we must bring together all the tools already available for strong authentication and secured working processes with authorized results in an easy but secure way to avoid further breaches.
But there are always unexpected, hardly predictable ways for bypassing rules or IT systems.
That why "Building taller walls and digging deeper moats is not solving our problems". (Yoran, 2015)
It's time to change the mindset and new tools are needed. This need of change means that new terms of thinking become to be necessary.

2. New Terms of Thinking

The new thinking should include the following concepts

1. Collaborated Security vs. Keyhole Security
2. Multi-Instance-Authentication vs. Multi-Factor–Authentication
3. Pass Space & Entropy
4. Scrambled Secrets vs. Security through Obscurity
5. Five New Protocols
6. Augmentation of the Human Factor

2.1 Collaborated Security vs. Keyhole Security

The theft of user data is increasing. The objective should be that the unauthorized access to users' credentials does no longer lead to serious consequences. 95% of breaches go directly through the front door. One of the latest severe attack is the cyber-attack on Germany's government IT network. The hacker group Snake used the federal academy for public administration as an entry gate. The Mobile Incident Response Team (MIRT) is tasked to investigate whether the attackers have succeeded in placing technical backdoors in networks to prevent further attacks. (Brühl et al, 2018).
And if they have entered the front or the back door they'll have access to all secrets.
The thinking of a so-called Keyhole Security and even the concept of Single sign-On must overcome.
Keyhole Security that means only protecting the access to your 'values or secrets' and not protecting these values themselves.
Already in 2015 NSA-Director Michael Rogers has claimed the 'Split-Key-Approach' as a real option against 'back doors' in his speech at Princeton University. (Nakashima et al, 2015)
Collaborated Security is necessary, that means security is only guaranteed if several different instances are participating in the process based on mutual trust and coincidence of interests.
The cryptographical basics for sharing a secret have already been created by an algorithm of Adi Shamir a few decades ago. (Shamir, 1979)

2.2 Multi-Instance-Authentication vs. Multi-Factor-Authentication

The Multi-Instance-Mode means that several instances can be simultaneously involved in authentication and secured working processes with authorized results. These instances or so-called agents could be different persons, institutions or technical agents. A technical agent could be an appliance or store containing biometric information that can be used to authenticate the identity, e.g. national identity cards administrated by the government. Institutional agents also called web agencies could be: authorities like state authorities for identity confirmation or financial institutions to confirm the authenticity of a banknote or share. A digital signature could be a web agency too. The Multi-Instance-Mode allows the inclusion of mutual trust. Trust is a new quality.
Responsibility and trust are shared. Trust arises through the consistency of interests. Only together the authentication process can be carried out.
The Multi-Factor-Authentication uses many different tools, such as smart cards, biometrics or geolocation but presents only one instance in the process.

2.3 Pass Space & Entropy

The working of Collaborated Security can be visualized by a so-called Pass Space with 1350 spheres.
Each sphere shows the number of the character from UTF16 character set. This character set includes 65,535 characters. The extension of the Pass Space equals 65,535 with the power of 1350.

The entropy is $1{,}350 * \log_2(65{,}535) = 21{,}599.9703$.

The calculation is based on the work of Claude Shannon (Roch, 2009) who introduced the term 'Entropy' on the advice of John von Neumann as a mathematical criterion of the sufficient randomness.
"You should call it entropy. Nobody knows what entropy really is, so in a debate you will always have the advantage." (von Neumann, 1940/41)

The size of the Pass Space is a huge one. The Pass Space could contain security related data, like user accounts, data, bank accounts, technical information, executable programs, and property claims (banknotes, shares).

The Pass Space can be manipulated by the involved instances or by tools, i.e. human actions, biometrics, software, server and 'salted' passwords. The Pass Space works on its own algorithm. By using the Pass Space you'll get 'Scrambled Secrets'.

2.4 Scrambled Secrets

Scrambled Secrets is a security algorithm containing several components and using simultaneously multiple keys or only one key. The different keys could be applied by different instances.
An essential property of Scrambled Secrets is to create one or more keys using an innovative graphical interface and the extremely good memorability by people, below called agents. The involved agents can simultaneous collaborate by using multiple keys for authentication or for encryption/decryption of sensitive data or secrets. That gives confidence, visibility and control of the data to the agents.

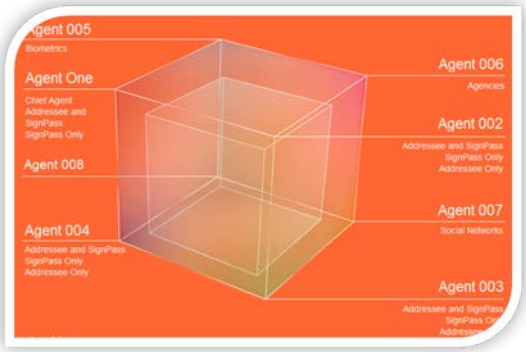

Figure 1: Multi-Instance-Mode

These agents could be different persons, institutions (government/security agencies) and technical agents.
A technical agent could be an appliance or store containing biometric information that can be used to authenticate the identity, e.g. national identity cards administrated by the government.
Institutional agents are called web agencies.
Web agencies that means different authorities like state authorities for identity confirmation or e.g. financial institutions to confirm the authenticity of a banknote or a share. In addition, an automatically mechanism such a signature could be understand as a web agency too.
The APP Scrambled Secrets demonstrates and illustrates the functioning and the influence of the involved agents on the Pass Space. Possible potential applications are the processing of images, texts, and technical program code, as well as the creating of keys and strong passwords.

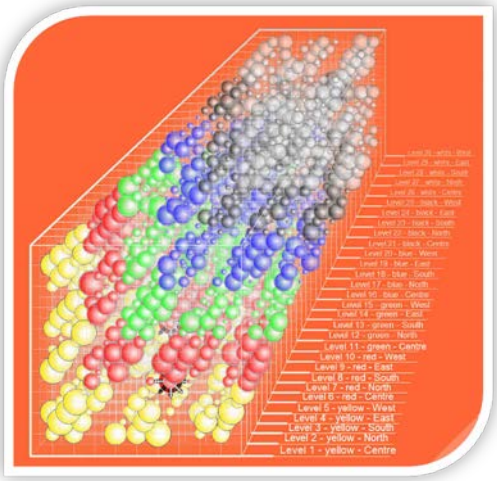

Figure 2: Pass Space

The APP 'Scrambled Secrets' enables you to scramble and unscramble your secrets.
This can be combined by using a Multi-Instance-Mode. Up to eight instances which could be a mixture of different or technical factors with different simultaneous authorities can be involved in the process.

Multi-Instance-Mode means that up to 8 different instances or agents can be involved in the process. The working of Scrambled Secrets is visualized by a so-called Pass Space with 1350 spheres. Each sphere shows the number of the character from UTF16-character set. This character set includes 65,353 characters.
The idea behind the Scrambled Secrets is not only locking the door of your safe by using a simple 'True-False-Authentication-Mechanisms' but rather protecting your 'values' themselves by encrypting.
The thinking of a so-called Keyhole Security must overcome. Security is only guaranteed if several different instances participate in the process and by protecting your 'values' themselves. Values or secrets could be money or important business data, technical spoken that are files, like textual information, images, videos or another software.
The idea to scramble secrets means to encrypt each value, security item or secured working process separately. That means not only encrypting the whole hard disk rather encrypting each file, banknote or share in your 'safe'. This scrambling enables to save data in the cloud in a way that these data are worthless and not exploitable for others. Further data can be protected from unauthorized reading and modification.
Feasible scenarios using the Scrambled Secrets could be: image authentication, real electronic money or the jointed control of machines. Once adopted the solution can help to assure that security, privacy, interoperability and ease of use are significantly improved for all parties, which are involved in the authentication process.
In contrast the strategy of Security by Obscurity means only to protect the access to 'values' by being unclear and difficult to understand or see. Once this access was forced by hackers, they'll have access to all secrets.

2.5 Five New Protocols

In order to support our ideas and to spread the technical feasibility, we've developed the 'Five New Protocols'.
The Five New Protocols were developed to overcome current issues within the authentication process.
Protocol 1 – QR Code
Protocol 2 – Stealth Mode
Protocol 3 – Secret Based Login
Protocol 4 - Encrypted User Data
Protocol 5 – Multi-Instance-Authentication/Scrambled Secrets

Firstly, because passwords can be hacked the Stealth Mode was developed.
Secondly because the addressees possible protect user credential insufficiently sensitive data can be misused. That's why the idea of transferring 'content free strings' was born.
Finally, there is a need to overcome the so-called Keyhole Security which means only locking the door of your safe by using a simple 'True-False-Authentication-Mechanisms'.
There is the problem of authentication in public spaces with untrusted devices. This problem could be solved by Protocol 1. Between personal smart phones and public devices, a password is transferred by QR-Code.
By using the Protocol 1 the real password is transferred. This disadvantage is solved by applying the Protocol 2, the Stealth Mode. The password is changed within a certain frame so that it cannot be identified during the valid period.
With the Protocol 3 the attack of the password transfer is avoided. Only a 'content-free string' will be send to the user. During the handling of the login by FabulaRosa the string will be scrambled.
Protocol 4 enables the user to encrypt and decrypt complex data locally within FabulaRosa by using the complex password matrix. It is suitable for user's credentials, files, and applications.
The idea behind Protocol 5 or Scrambled Secrets is protecting your 'values' themselves by encrypting. This can be combined by using a Multi-Instance-Mode. Up to eight instances which could be a mixture of different technical factors with different simultaneous authorities can be involved in the process.

These protocols were already developed in 2010. After 8 years only the QR-Code is used of many users in different apps.
The mass of data breaches has not caused service provider on Internet to introduce real innovations, such as the 'Stealth Mode'. Innovations are being hesitantly introduced. The change of mindset and its implementation is an even more cumbersome task. Innovations must prevail against the 'sluggish user' who prefers convenience rather than security. It is not easy to put Sun Tzu's principles of being proactive into practice. The question: how does innovation work and how to put it into practice is always difficult to answer.

2.6 Augmentation of the Human Factor

An essential component is the 'human factor'; the conscious, intentional, human act. That's a very controversial topic. It is important to consider whether and when the human factor should be included or excluded. We believe that security can only be achieved through the involvement of the persons concerned.
One of the six design principles for military ciphers stated by August Kerckhoffs (1883) is:
it must be possible to communicate and remember the key without using written notes, and correspondents must be able to change or modify it at will.
These days this key is the password of a user. The access to user accounts and the protecting of data is usually based on password authentication.
The huge amount of attacks against passwords, like brute force (Kelley et al, 2012), dictionary (Bonneau,2012) and social engineering makes it essential to use secure passwords. At this point the user's ability to create 'secure passwords' came into the focus. (Bonneau, 2010)
A long range of studies appeared on wrong or predictable user behaviour (Yan et al, 2004), (Taneski et al, 2014), (Ur et al, 2015) and how about choosing secure passwords (Schneier, 2014), (R. Shay, 2014).
In addition, users need to cope with different password implementations at services on the Internet (Moritz et al, 2017). A lot of password requirements, which are fixed rules regarding password length and the allowed characters were postulated. These requirements are highly diverging between services. (AlFayyadh et al, 2012)
Last June the NIST-Guidelines on secure passwords have been completely revised. It is no longer talking passwords but 'Memorized Secrets'. Memorized Secrets should be interpreted to include passphrases and PINs as well as passwords. Now the user would have the option of assigning 64-character long passwords of any characters, including the space. The memorized secrets should be simple and easy to remember. For example, the password could be a sentence. And there is no need longer to change passwords regularly. (Grassi et al, 2017)
The new NIST-Guidelines on Digital Identities made some studies obsoleted. (Bonneau, 2012)
All this leaves the user in a real dilemma. Per se the user is completely on her/his own and needs practical help. Because we are convinced that the human factor and the password are the essential factors within the authentication process we were seeking after tools suitable for supporting users and augmenting their abilities.

2.6.1 Augmentation by graphical interface with an extremely good memorability - FabulaRosa

What if having the possibility to handle this huge number of logins or accounts in an easy way? The solution could be an innovative graphical interface with an extremely good memorability. We've developed an app to meet these requirements. The APP FabulaRosa provides you with complex and long passwords by drawing only one image on a virtual 'Compass Rose' and applying universal things such as colours and directions and patterns, and the passwords are not stored at all; they are generated in the moment you draw the image on the screen.

2.6.2 FabulaRosa and Entropy

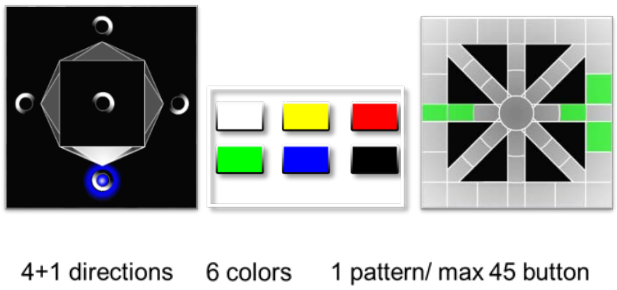

Figure 3: FabulaRosa- Interface

You can choose 5 directions, 6 colours and 45 buttons that equals 30 levels.
30 levels by 45 buttons equals 1350 possibilities to activate a button. That represent a combination amount of 65,535 1350 = 1.7 e+6502
In other words, the extension of the Key Space, rather called Pass Space, is 65,535 with the power of 1350, which equals 1.7 with the power of e+6502. The entropy is $1{,}350 * \log_2(65{,}535) = 21{,}599.9703$

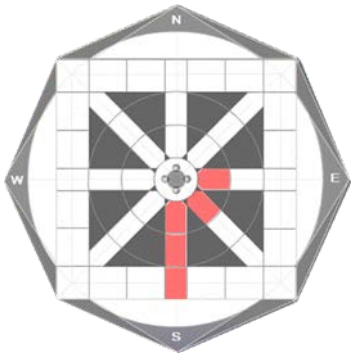

Figure 4: FabulaRosa - Pattern Interface

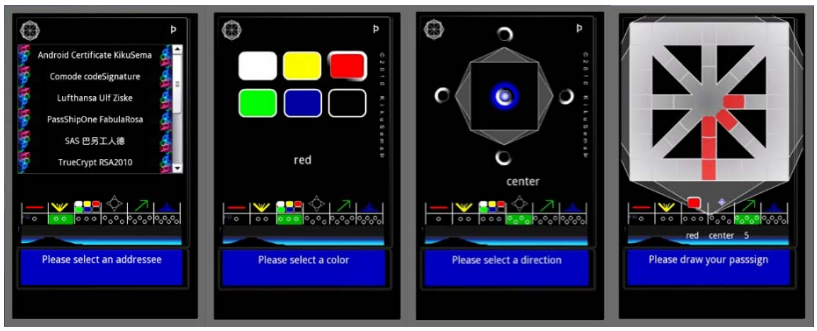

Figure 5: FabulaRosa – Screens of the app

3. Conclusions

We are convinced that a new kind of security is needed. We have to overcome the so-called Keyhole Security by a stepwise transition into a world of diversity of secret items and Collaborative Security.
Security is only guaranteed if several different instances participate in the process. Collaborative Security that means working together in a Multi-Instance-Mode. The Multi-Instance-Mode allows the inclusion of mutual trust. Trust is a new quality. Responsibility and trust are shared. Trust arises through the consistency of interests. Only together the authentication process can be carried out.
The human factor has to be strengthened. Only the competence of a human being is qualified to be the primary factor in authentication.
The modern citizen is part of a worldwide system, in which (s)he is in relation to Third Parties, like e-commerce provider, Internet service provider, Trust centre and to the government of the homeland and of other countries with their own interests.
The available resources of the citizens for acting in their own interest cannot keep pace with the accelerated development of Third Parties' resources. Personal security will reach by taking individual responsibility, by being the active party.
There is a difference between knowing the path or walking the path. We have already started to walk the path. We had transferred our ideas into apps, like Scrambled Secrets, FabulaRosa and the Five New Protocols.
We have combined the idea of applying universal things such as colours, directions and patterns in combination with touch screens for expanding the capabilities of users. We came up with the idea to expand the using of usual character set of 94 types by graphical characters taken from the UTF16-character set. Furthermore, we came up with the idea of sharing responsibility and developed the APP 'Scrambled Secrets' based on the concept of the Pass Space.
Our vision is that once adopted our concepts and apps can help to assure that security, privacy, interoperability and the ease of use will be significantly improved for all parties, which are involved in the authentication process.
We are looking for committed partners to walk together on the path. The News Needs Friends!

References

AlFayyadh, B., Thorsheim, P., Jøsang, A. and Klevjer, J. (2012) "Improving usability of password management with standardized password policies", *Proc. SAR-SSI.*

Bonneau, J. (2012) "The science of guessing: analyzing an anonymized corpus of 70 million passwords", *IEEE Symposium on Security and Privacy*, pp 538–552.

Bonneau, J., Herley, C., Van Oorschot, P.C. and Stajano, F. (2012) "The quest to replace passwords: A framework for comparative evaluation of web authentication schemes", *Security and Privacy (SP)*, IEEE Symposium, pp 553–567.

Bonneau, J. and Preibusch, S. (2010) "The password thicket: technical and market failures in human authentication on the web" in Proceedings of the Ninth Workshop on the Economics of Information Security *(WEIS)*.

Brühl, J. and Tanriverdi, H. (2018) "IT-Sicherheit, Was Sie über den Hackerangriff auf das Regierungsnetz wissen müssen", [online], http://www.sueddeutsche.de/digital/hacker-regierungsnetz-fragen-1.3887668.

Grassi, P.A., Fenton, J.L., Newton, E.M., Perlner, R.A., Regenscheid, A.R., Burr, W.E. and Richer, J.P. (2017) "Digital Identity Guidelines. Authentication and Lifecycle Management", *NIST Special Publication* 800-63, Version 1.0.2, pp 13–15, [online], https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf.

Horsch, M., Braun, J. and Buchman, J. (2017) "Password Assistance", Open Identity Summit (OID), Lectures Notes in Informatics. German Informatics Society.

Kelley, P.G., Komanduri, S., Mazurek, M. L., Shay, R., Vidas, T., Bauer, L., Christin, N., Cranor L.F. and Lopez, J. (2012) "Guess Again (Again and Again): Measuring Password Strength by Simulating Password-Cracking Algorithms". *Proc. SP. IEEE.*

Kerckhoffs, A. (1883), "La cryptographie militaire", *Journal des sciences militaires.* Volume 9, pp 5–38 & 161–191.

Nakashima, E. and Gellman, B. (2015), "As encryption spreads, U.S. grapples with clash between privacy, security", [online], https://www.washingtonpost.com/world/national-security/as-encryption-spreads-us-worries-about-access-to-data-for-investigations/2015/04/10/7c1c7518-d401-11e4-a62f-ee745911a4ff_story.html?utm_term=.116b3866d463.

Roch, A., (2009) Claude E. *Shannon: Spielzeug, Leben und die geheime Geschichte seiner Theorie der Information*, Gegenstalt Verlag, Berlin.

Schneier, B. (2014) "Choosing secure passwords", [online], https://www.schneier.com/blog/archives/2014/03/choosing_secure_1.html.

Shamir, A. (1979) "How to share a secret", *Communications of the Association for Computing Machinery*, Vol. 22, Issue 11, pp 612-613.

Shay, R., Komanduri, S., Durity, A.L., Huh, P.S., Mazurek, M.L., Segreti, S.M., Ur, B., Bauer, L., Christin, N. and Cranor, L.F. (2014) "Can long passwords be secure and usable?", Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, ser. CHI '14. New York, NY, USA: ACM, pp 2927–2936, [online], http://doi.acm.org/10.1145/2556288.2557377.

Sunzi. (2011) *Die Kunst des Krieges*, Translated by Eisenhofer. H., Nikol Verlagsgesellschaft Hamburg.

Taneski, V., Hericko, M. and Brumen, B. (2014) "Password security – No change in 35 years?", *Proc. MIPRO. IEEE.*

Ur, B., Segreti, S.M., Bauer, L., Christin, N., Cranor, L.F., Komanduri, S., Kurilova, D., Mazurek, M.L., Melicher, W. and Shay, R. (2015) "Measuring real-world accuracies and biases in modeling password guessability", *Proceedings of the 24th USENIX Security Symposium. USENIX.*

Von Neumann, J. (1940/41) "Conversation, between John v. Neumann and Claude Shannon, occurred between fall 1940 to spring 1941 at the Institute for Advanced Study, Princeton, New Jersey", [online], http://www.eoht.info/page/Neumann-Shannon+anecdote.

Yan, J.J., Blackwell, A.F., Anderson, R.J. and Grant, A. (2004) "Password Memorability and Security: Empirical Results", *IEEE Security & Privacy*, Volume 2, Issue 5.

Yoran, A. (2015) "Escaping Security's Dark Ages", RSA Conference San Francisco, [online], https://www.youtube.com/watch?t=10&v=op-2Aj6Wizo.

Ziske, U. (2015) "KikuSema GmbH Takes Part in the Challenge – Change Today's Security Thinking - with a Multi-Instance-Mode/Split-Key-Approach", [online], https://www.businesswire.com/news/home/20150420005370/en/KikuSema-GmbH-Takes-Part-Challenge-%E2%80%93-Change#.VdiY85txD4Y.