IRSTI 81.93.29

[1]R.R. Safin, [2,3*]A.S. Abdiraman, [2]A.M. Nurusheva, [3]L.S. Aldasheva

[1] Linnovate Ltd., Minsk, Belarus
[2]L.N. Gumilyov Eurasian National University, Astana, Kazakhstan
[3]Astana IT University, Astana, Kazakhstan
(e-mail: Ruslan@v-office.org, a.s.abdiraman@gmail.com, nurusheva.assel@mail.ru, Laura.Aldasheva@astanait.edu.kz)

Comparison of information security methods of information-communication infrastructure: Multi-Factor Authentication

Abstract. Sensitive information was always one of the big trade-offs we always exchange big secrets for small ones. On one hand, memorization of small secrets on the other hand tons of services requires a dedicated secret for each one. And when one of the services will be compromised it affects all services with the same password and credential. The main purpose of this article is to discuss multiple factors and increase security trade-offs differently. We will try to compare MFA (Multi-Factor Authentication), 2FA (Two Factor Authentication), 2SV (Two-Step Verification), and 1FA (One Factor Authentication) and investigate the password-free future.

Keywords: MFA, personal data, cybercrimes, data leakage, vulnerability, verification, authentication.

DOI: doi.org/10.32523/2616-7263-2022-140-3-114-124

Introduction

We now live in a reality where a password is not a guarantee of security and protection of information. Most passwords can be cracked in a few minutes (hours, days, but anyway less than eternity). No one wants to face stealing identity or some private information like accounting, financial, personal (PII), or health data. [1, 2]

Usually, users don't want to memorize small secrets (in this context we mean passwords) and try to write them on stickers and place them on their monitor.

For this situation, a solution might be a password manager to trade off a few small secrets with one. For some workflow, we can protect this password manager with biometric protection like a fingerprint or via face recognition. And this solution might work in the world without phishing attacks. [3, 4]

To prevent this type of attack we can implement website address verification, and it might work for attacks on the password autocompletion mechanism. But this doesn't work for social engineering attacks.

Also, some experts recommend 2FA with mobile applications and TOTP (Time-based one-time password) [5, 6] or HOTP (HMAC-based one-time password) [7, 8] one-time passwords. But this solution doesn't work with spear-phishing in couple with social engineering [9].

We can try to improve our MFA application with push notifications and send push notifications to verify user activity.

But this method doesn't work with multistep attacks and bombing users via push notification to indulge and press accept access in pushes.

The rapid development of the IT sector leads to accelerated application and introduction of digital innovations, and these innovations require highly qualified engineers who can implement those innovations and build modern infrastructures and services.

As we all know in the world high demand for highly skilled engineers, but Universities can't provide enough qualified specialists. Based on this statement we can predict a fast growth of consulting companies and contractors who supports this growth for market makers [10].

The Cybercrimes landscape moved from standalone hackers to highly motivated teams targeted to destruct companies' and governments' infrastructures, including critical infrastructure. Those actors communicate and use different tactics and tools. Many of those tools is a legitimate tool for daily automation and configuration duties. So that big part (in that case we can say that all of today's available antivirus or endpoint detection and response tools) can't prevent those attacks.

In that article, we try to provide ways to avoid these risks and improve the security of companies' infrastructure.

Methods

This article described the reasons and purposes for implementing a multi-factor/multi-step verification process. And some pieces of historic information about the changes in the authentication process.

As a starting point, we considered the article [11] about the Time-Based One-Time Password (TOTP) Algorithm. This document describes the specification of TOTP (Time-based one-time password) and HOTP (HMAC-based one-time password), in this document we saw a description of two types of one-time password notation. A big part of this document describes generating one-time passwords from predefined secret keys based on a time vector or event-based vector to verify accounts.

The most challenging task of describing this technology was the method of generating a strong one-time password and trust's legal provisioning relationship. This term means if I have something, and I know something, and it means I am an authorized/identified person. This fact depends on something that has physical nature for example hardware token or some smartphones (in that case mentioned smartphone with some specific application. This application should not have access to the internet and should run in an isolated environment to prevent leakage of secrets from this application), or smartcard; but this something changes depending on time or usage factor.

For time-based secrets recommended time frame is equivalent to 30 seconds, this parameter was chosen based on the security and usability equation. To decrease the effect of time drift issues (when server and token have different time and requires synchronization) in most cases allowed to use two one-time passwords earlier than the current which meant that we increase the time frame to 90 seconds.

As for HMAC-based one-time passwords, it synchronizes one-time passwords based on ticks and allows only incremented one-time passwords from the generation vector.

For that case we can use a simple example of TOTP realization:

```
import (
    «time»
)
...
totp := gotp.NewDefaultTOTP([]byte(«secret key»))
timestamp := time.Date(2022, 05, 20, 11, 28, 13, 0, time.UTC)
code := totp.At(timestamp)

if totp.VerifyAt(code, timestamp) {
    panic(fmt.Error(«invalid OTP code»))
}
```

In this example, we can configure the number of digits used for generation TOTP and this code propose ways to correct time frames by *VerifyWithinWindow(OTP, timestamp, validationWindow)*

To provide a more detailed view of TOTP and HOTP realization, let's deep dive to reference realization of this algorithm in golang.

HOTP:

```
type HOTP struct {
   OTP
}
func NewHOTP(secret string, digits int, hasher *Hasher) *HOTP {
   otp := NewOTP(secret, digits, hasher)
   return &HOTP{OTP: otp}
}
func NewDefaultHOTP(secret string) *HOTP {
   return NewHOTP(secret, 6, nil)
}
func (hs *HOTP) At(count int) string {
   return h.generateOTP(count)
}
func (hs *HOTP) Verify(otp string, count int) bool {
   return otp == hs.At(count)
}
```

TOTP:

```
import «time»
type TOTP struct {
   OTP
   interval int
}
func (tm *TOTP) At(timestamp int) string {
   return tm.generateOTP(tm.timecode(timestamp))
}
func (tm *TOTP) Now() string {
   return tm.At(currentTimestamp())
}
func (tm *TOTP) NowWithExpiration() (string, int64) {
   interval64 := int64(tm.interval)
   timeCodeInt64 := time.Now().Unix() / interval64
   expirationTime := (timeCodeInt64 + 1) * interval64
   return tm.generateOTP(int(timeCodeInt64)), expirationTime
}
func (tm *TOTP) Verify(otp string, timestamp int) bool {
   return otp == tm.At(timestamp)
}
func (tm *TOTP) timecode(timestamp int) int {
   return int(timestamp / tm.interval)
}
```

In this part of this article, we discussed ways to provide ways to generate one-time passwords to mitigate stealing user accounts attacks.

Results

As a result of the previous step, we prepare the two most popular variants of one-time password algorithms. These algorithms provide us with ways to generate strong one-time passwords. In this paragraph, we move forward with the logical realization of these algorithms.

Figure 1 shows a generic architecture of generation time-based one-time passwords. This works without any additions to the piece of code from the previous paragraph.

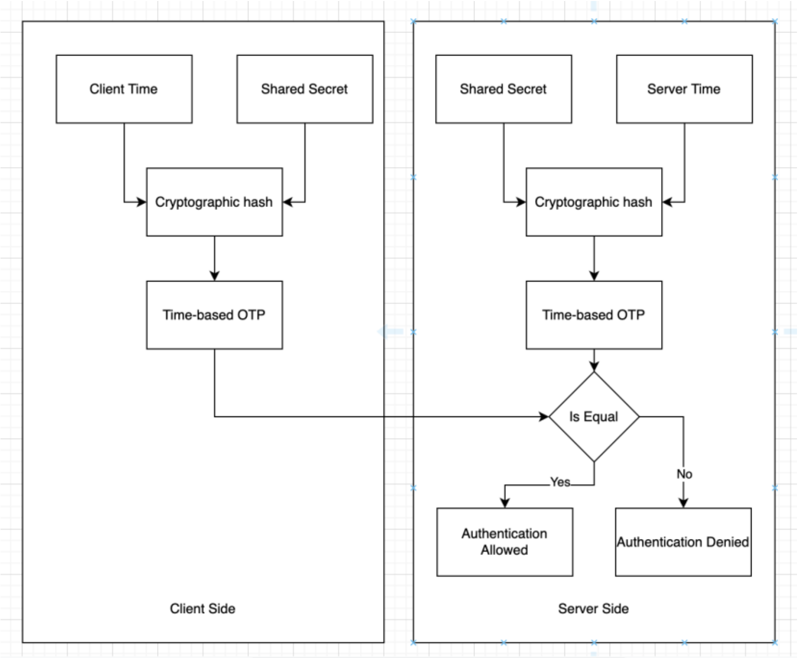


Figure 1. Architecture diagram generation TOTP

As we can see, all parts work independently and don't depend on others. One vulnerability is the exchange of shared secrets, but in most cases, we can accept this risk because we do not simply exchange secrets but verify the first generated one-time password after exchange. This simple algorithm provides a big step to improve the security of the authentication process. We can stop worrying about stealing passwords because without shared secrets and time stamps it is impossible to verify user identity and access to a protected part of an application.

But as with every solution, a time-based one-time password has a weak side. For our case, it is time synchronization, because with a different and not precise time on both sides we can't generate these codes. In case when we don't want to worry about time synchronization, we need to move forward with a hmac-based one-time password. This algorithm is provided in Figure 2 and is based on code from the previous paragraph.

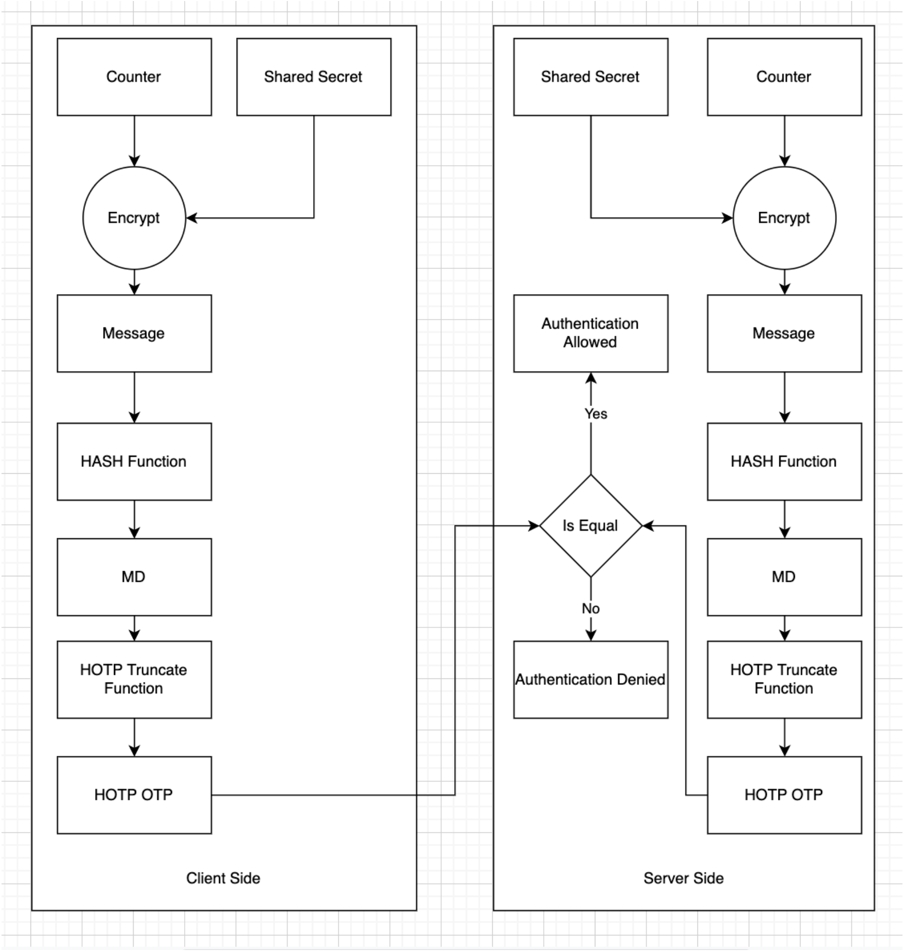


Figure 2. Architecture diagram generation HOTP

Flow with HOTP looks better because we don't affect by time synchronization issues, but at the same time we need to count our security codes and save the counter to generate valid tokens.

Simple use of MFA mitigates phishing [12] and spear phishing [13] attacks those attacks provide a possibility to steal login and password but MFA/2FA tokens prevent this risk.

The diagram in Figure 3 provides one of the possible examples of a multi-phase phishing attack chain.

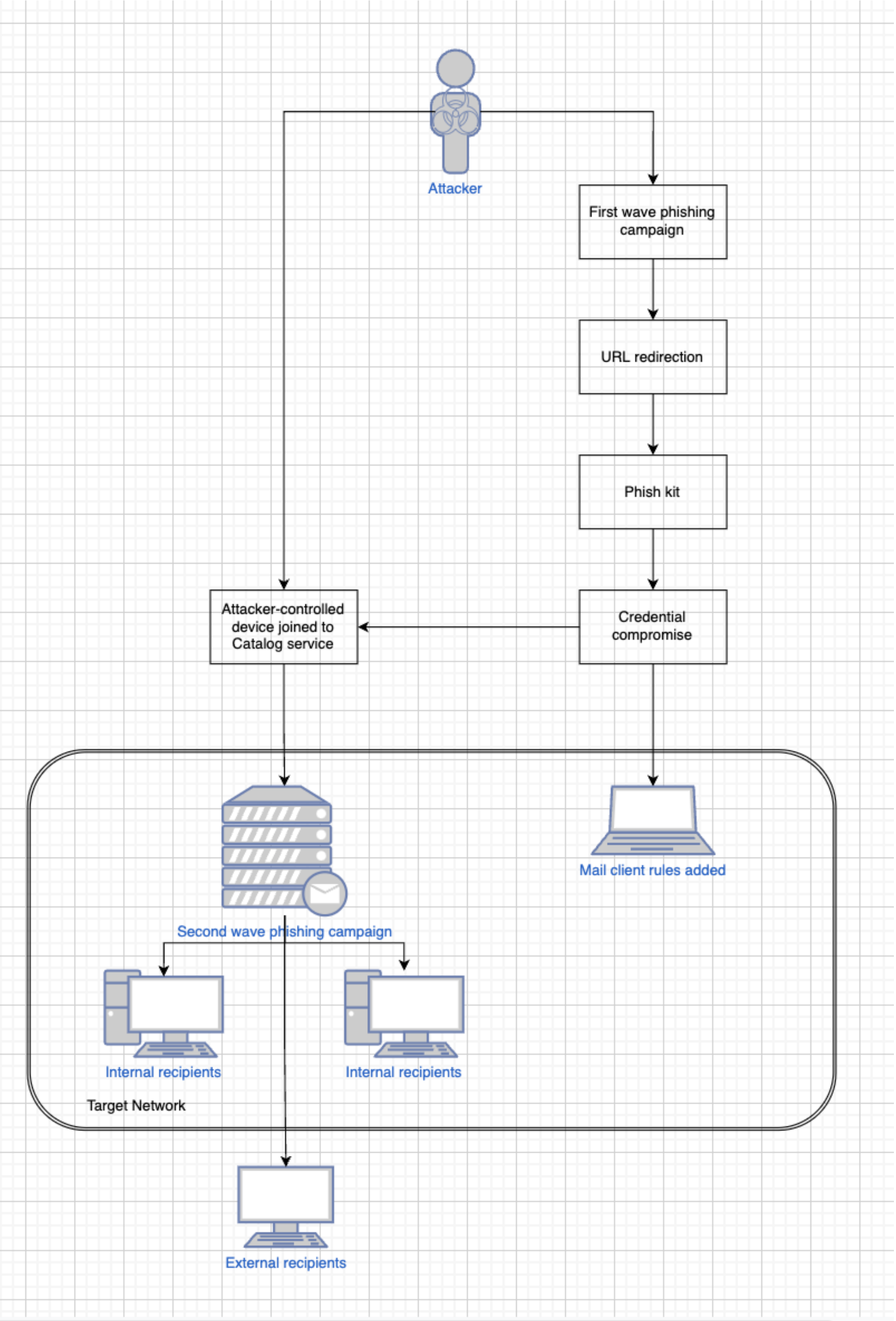
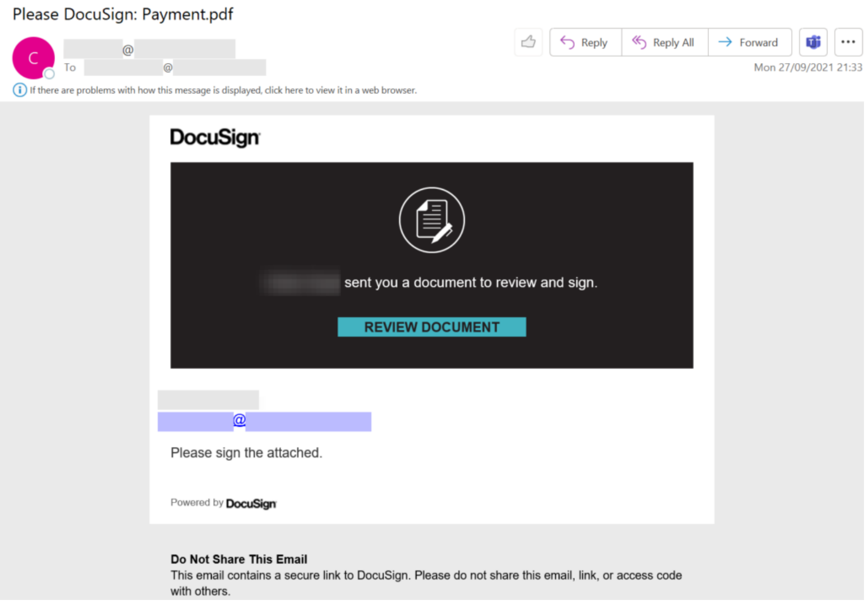


Figure 3. Multi-phase phishing attack chain

For sure most phishing and spear phishing attacks for most users look like legitimate mails, for example, phishing DocuSign mail in Figure 4.



Please DocuSign: Payment.pdf

C [redacted]@[redacted]

To [redacted]@[redacted]

Mon 27/09/2021 21:33

If there are problems with how this message is displayed, click here to view it in a web browser.

DocuSign

[redacted] sent you a document to review and sign.

[redacted]

[redacted]@[redacted]

Please sign the attached.

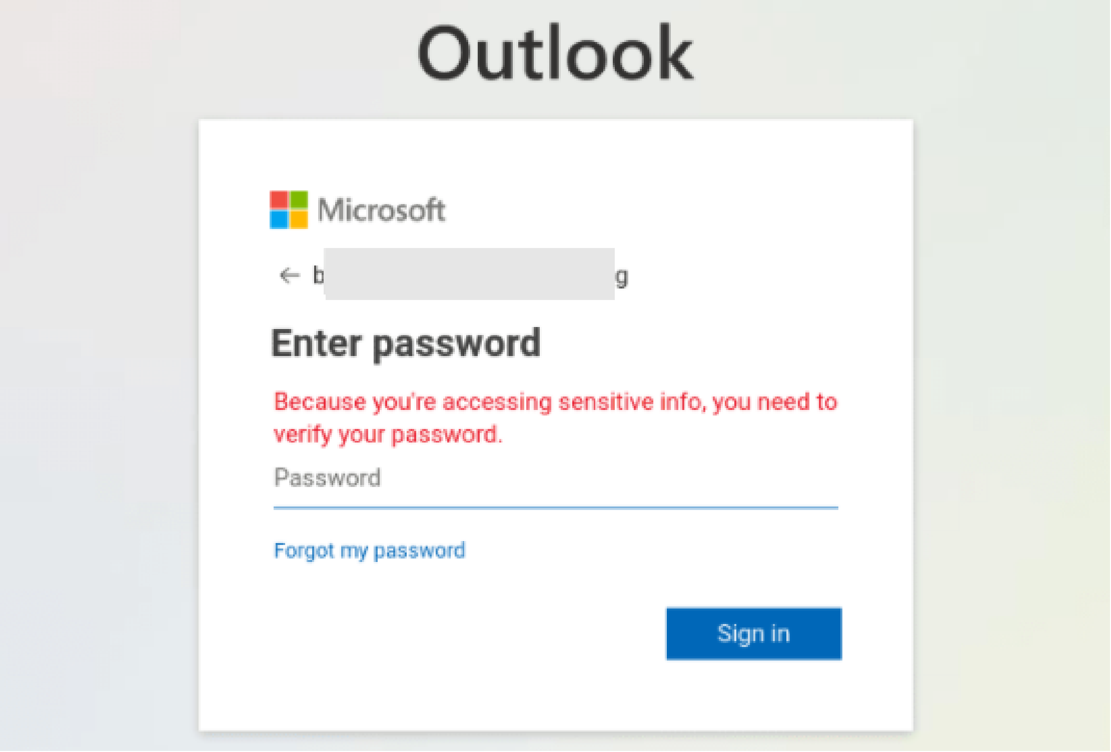
Powered by DocuSign

Do Not Share This Email

This email contains a secure link to DocuSign. Please do not share this email, link, or access code with others.

Figure 4. First-stage phishing email spoofing DocuSign

End-user followed by the link in the email will be faced with a login page for example as provided in Figure 5.



Outlook

Microsoft

← b[redacted]g

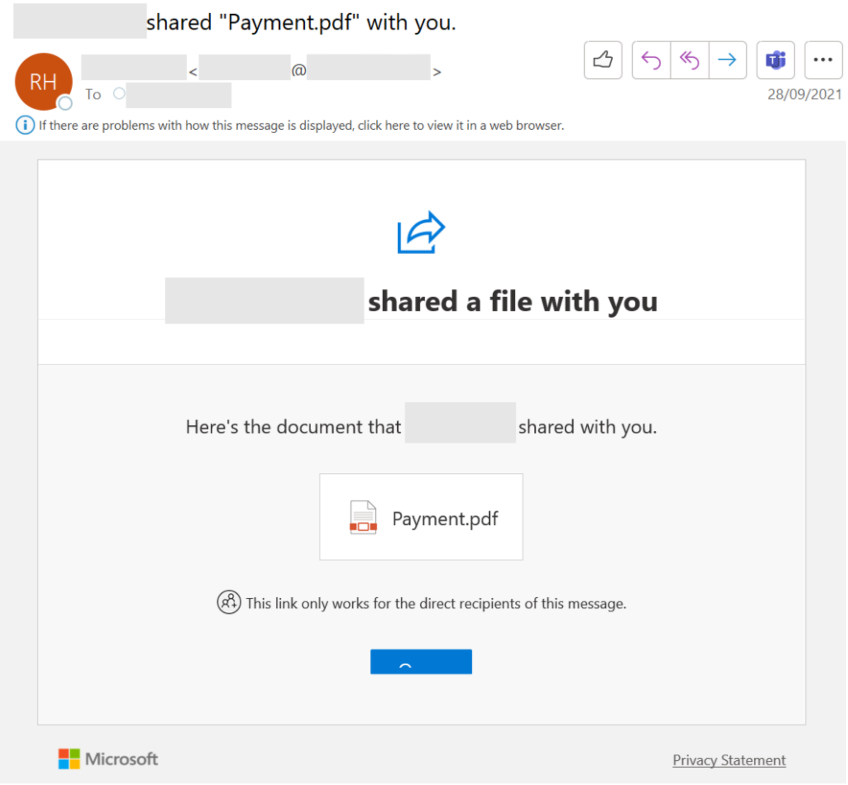
Enter password

Because you're accessing sensitive info, you need to verify your password.

Password

Figure 5. Phishing page with username prepopulated

And after this step attacker moves forward and tried to attack new victims inside the organization. An example of the email is in Figure 6.



[redacted] shared "Payment.pdf" with you.

RH [redacted] < [redacted] @ [redacted] >

To [redacted]

28/09/2021

If there are problems with how this message is displayed, click here to view it in a web browser.

[redacted] shared a file with you

Here's the document that [redacted] shared with you.

Payment.pdf

This link only works for the direct recipients of this message.

Microsoft

Privacy Statement

Figure 6. Second-stage phishing email spoofing SharePoint

Discussion

There was described a few methods of MFA and 2FA authentication, all companies move forward to the password-free future. As we can see the world has a few ways to propose MFA for every user, but we need to remain a difference between MFA/2FA and 2SV (two-step verification) because in many cases 2SV looks very similar, but it is different.

Many banks forced their clients to use SMS as a second factor, but the realization of this second factor provided flow to reset user password with only access to SMS and knowledge something about a user for an example ID number (this number not private information and has simple and well-known generation rules). With these two components, we can reset passwords for all bank accounts in all ex-USSR countries without any exception.

And as we discussed before, this is not a true way of using MFA.

Based on these statements and knowledge investigated earlier in this article we have enough knowledge to check and prove the security of each service provided or don't provide multifactor authentication possibility.

Conclusion

This article describes a few realizations developed to provide secured access and minimize the risks of phishing attacks. As described above lack of security awareness among users or employees shouldn't affect the security of their and company data. New reality provides us with an opportunity to work from home, to make our work-life reality more flexible and faster than was before, but new challenges and threats make some changes to our daily routine and habits. That's not insane that's just our new reality and we need to evolute in this new reality, like the first people in the stone age we need to improve our habits, including new methods, and continuously move forward to the new challenges to the new achievements.

References

1. Y. Fujita, A. Inomata and H. Kashiwazaki Implementation and Evaluation of a Multi-Factor Web Authentication System with Individual Number Card and WebUSB, 2019 20th Asia-Pacific Network Operations and Management Symposium (APNOMS), Matsue, Japan, 2019. P. 1-4.

2. B. O. ALSaleem and A. I. Alshoshan, Multi-Factor Authentication to Systems Login, 2021 National Computing Colleges Conference (NCCC), Taif, Saudi Arabia, 2021. P. 1-4.

3. C. Hamilton and A. Olmstead, Database multi-factor authentication via pluggable authentication modules, 2017 12th International Conference for Internet Technology and Secured Transactions (ICITST), Cambridge, UK, 2017. P. 367-368.

4. H. Khalid, S. J. Hashim, S. M. S. Ahmad, F. Hashim and M. A. Chaudary New and Simple Offline Authentication Approach using Time-based One-time Password with Biometric for Car Sharing Vehicles, 2020 IEEE Asia-Pacific Conference on Computer Science and Data Engineering (CSDE), Gold Coast, Australia, 2020. P. 1-7.

5. Roger A. Grimes One-Time Password Attacks in Hacking Multifactor Authentication, Wiley, 2021, P.205-226.

6. S. Yang and J. Meng Research on Multi-factor Bidirectional Dynamic Identification Based on SMS, 2018 IEEE 3rd Advanced Information Technology, Electronic and Automation Control Conference (IAEAC), Chongqing, China, 2018. P. 1578-1582.

7. L. Dostalek Multi-Factor Authentication Modeling, 2019 9th International Conference on Advanced Computer Information Technologies (ACIT), Ceske Budejovice, Czech Republic, 2019. P. 443-446.

8. W. -S. Park, D. -Y. Hwang and K. -H. Kim, A TOTP-Based Two Factor Authentication Scheme for Hyperledger Fabric Blockchain, Tenth International Conference on Ubiquitous and Future Networks (ICUFN), Prague, Czech Republic, 2018. P. 817-819.

9. I. Gordin, A. Graur and A. Potorac Two-factor authentication framework for private cloud, 2019 23rd International Conference on System Theory, Control and Computing (ICSTCC), Sinaia, Romania, 2019. P. 255-259.

10. Z. Alamsyah, T. Mantoro, U. Adityawarman and M. A. Ayu, Combination RSA with One Time Pad for Enhanced Scheme of Two-Factor Authentication, 2020 6th International Conference on Computing Engineering and Design (ICCED), Sukabumi, Indonesia, 2020. P. 1-5.

11. H. Seta, T. Wati and I. C. Kusuma, Implement Time Based One Time Password and Secure Hash Algorithm 1 for Security of Website Login Authentication, 2019 International Conference on Informatics, Multimedia, Cyber and Information System (ICIMCIS), 2019. P. 115-120.

12. Ometov A., Bezzateev S., Mäkitalo N., Andreev S., Mikkonen T., Koucheryavy Y. Multi-factor authentication: A survey, Cryptography. 2018. Vol.2. №1. P. 1 – 31.

13. Saqib R.M., Khan A.S., Javed Y., Ahmad S., Nisar K., Abbasi I.A., Haque M.R., Julaihi A.A. Analysis and Intellectual Structure of the Multi-Factor Authentication in Information Security, Intelligent automation and soft computing. 2022. Vol.32. №3. P. 1633-1647.

[1]Р.Р.Сафин, [2,3*]Ә.С.Әбдіраман, [2]А.М.Нурушева, [3]Л.С.Алдашева

[1] Linnovate Ltd, Минск, Беларусь

[2]Евразийский национальный университет имени Л.Н.Гумилева, Астана, Казахстан

[3]Astana IT University, Астана, Казахстан

Сравнение методов защиты информации информационно-коммуникационной инфраструктуры: многофакторная аутентификация

Аннотация. Конфиденциальная информация всегда была одним из важных компромиссов, мы всегда обмениваем большие секреты на маленькие. С одной стороны, запоминание маленьких секретов, с другой - при множестве сервисов требуется отдельный секрет для каждого из них. И когда одна из служб будет скомпрометирована, это повлияет на все службы с одинаковым паролем и учетными данными. Основные цели данной статьи - обсудить множество факторов и рассмотреть повышение безопасности компромиссов разными способами. Мы попытаемся сравнить MFA (многофакторная аутентификация), 2FA (двухфакторная аутентификация), 2SV (двухэтапная проверка) и 1FA (однофакторная аутентификация) и исследовать будущее без паролей.

Ключевые слова: MFA, персональная информация, киберпреступления, утечка данных, уязвимость, верификация, аутентификация.

[1]Р.Р.Сафин, [2,3*]Ә.С.Әбдіраман, [2]А.М.Нурушева, [3]Л.С.Алдашева

[1] Linnovate Ltd, Минск, Беларусь

[2] Л.Н.Гумилев атындағы Евразия ұлттық университеті, Астана, Қазақстан

[3]Astana IT University, Астана, Қазақстан

Ақпараттық-коммуникациялық инфрақұрылымда ақпаратты қорғау әдістерін салыстыру: көпфакторлы аутентификация

Андатпа. Құпия ақпарат әрқашан маңызды сауда-саттықтың бірі болды, біз әрқашан үлкен құпияларды кішкентайларға ауыстырамыз. Бір жағынан, кішкентай құпияларды есте сақтау, екінші жағынан, көптеген қызметтер әрқайсысы үшін жеке құпияны қажет етеді. Қызметтердің біреуі бұзылған кезде, ол бірдей пароль мен тіркелгі деректері бар барлық қызметтерге әсер етеді. Бұл мақаланың негізгі мақсаты-көптеген факторларды талқылау және сауда-саттықтың қауіпсіздігін әр түрлі жолмен арттыру. Біз MFA (көп факторлы аутентификация), 2FA (екі факторлы аутентификация), 2sv (екі сатылы тексеру) және 1fa (бір факторлы аутентификация) салыстырып, құпия сөздерсіз болашақты зерттедік.

Кілт сөздер: MFA, жеке ақпарат, киберқылмыс, деректердің ағуы, осалдық, верификация, аутентификация.

Information about authors:

Safin R.R. – Senior Development Engineer at Linnovate Ltd, Minsk, Belarus

Abdiraman A.S. – The 2nd year Ph.D. student in Information Security, L.N. Gumilyov Eurasian National University, Senior Lecturer of the Department of Intelligent Systems and Cybersecurity, Astana IT University, Astana, Kazakhstan.

Nurusheva A.M. – Ph.D., Acting Associate Professor of Information Security Department, L.N. Gumilyov Eurasian National University, Astana, Kazakhstan.

Aldasheva L.S. – Candidate of Technical Sciences, Senior Lecturer of the Department of Intelligent Systems and Cybersecurity, Astana IT University, Astana, Kazakhstan.

Сафин Р.Р. – Аға инженер-әзірлеуші Linnovate Ltd, Минск, Беларусь

Әбдіраман Ә.С. – «Ақпараттық қауіпсіздік» кафедрасының екінші курс докторанты, Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Интеллектуалды жүйелер мен киберқауіпсіздік департаментінің аға оқытушысы, Astana IT University, Астана, Қазақстан.

Нурушева А.М. – PhD, «Ақпараттық қауіпсіздік» кафедрасының доценті міндетін атқарушы, Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Астана, Қазақстан.

Алдашева Л.С. – техника ғылымдарының кандидаты, Интеллектуалды жүйелер мен киберқауіпсіздік департаментінің аға оқытушысы, Astana IT University, Астана, Қазақстан.