Beyond Passwords: Enforcing Username Security as the First Line of Defense

Thaier Fandakly[1] and Nicholas Caporusso[1]

[1] Fort Hays State University, 600 Park Street,
67601 Hays, United States
t_fandakly@mail.fhsu.edu, n_caporusso@fhsu.edu

Abstract. Combinations of account identifier (e.g., username) and key phrase (i.e., password) are among the most utilized form of credentials for several types of authentication purposes, such as, user verification, connection to public and private networks, and access to digital resources. Typically, usernames are considered a method of account or user identification, whereas passwords are regarded as the crucial component that protects from attackers and prevents breaches. As a result, the level of security of a set of digital credentials is primarily associated with the strength of the key phase, and most of the attention focused on promoting initiatives for increasing password security. Unfortunately, account identifiers received less consideration. Consequently, users are aware of how to enforce the security of their password, though they might prefer more convenient options. Contrarily, several bad practices are caused by overlooking usernames as the first line of defense. In this paper, we highlight the increasing importance of account names and we overview the main username practices that impact account security. Furthermore, we present the results of a study that evaluated how human factors and individuals' awareness impact username security.

Keywords: authentication · credentials · cybersecurity · password · identity theft

1 Introduction

Access control and digital authentication algorithms typically use a combination of two types of information for authorizing a user: account identifier and password. In general, the former serves the purpose of finding a specific resource (or user) in the system, whereas the latter requires solving the challenge of knowing the secret word that grants access to the specific resource. To this end, the password is compared against the string associated with the identifier stored in the system. This method has been successfully utilized for decades for individual user accounts (e.g., e-mail mailbox, social media, and on-line banking accounts) as well as for accessing resources that can be shared among multiple users (e.g., public wireless networks).

Unfortunately, in the recent years, cyberattacks have become increasingly fierce thanks to the accessibility of information on the Internet, the availability of more powerful computational and network resources, and the development of more invasive techniques for threatening victims [1]. As an example, clusters of distributed devices, that is, a botnet, can be utilized in a coordinated, brute-force attack to significantly reduce the time to crack (TTC), as discussed in [2]. Furthermore, as technology progresses and TTC decreases, more sophisticated key phrases are required in order to maintain a minimum level of security [3].

As a result, several organizations, such as, the National Institute of Standards and Technology (NIST), started issuing and updating guidelines for enforcing security of digital identities and for ensuring that specific assurance levels are met [4]. However, several factors prevent users from adopting best practices. On the one hand, lack of risk awareness and cybersecurity training is among the leading cause of weak credentials. Nevertheless, several studies showed that users tend to compromise security in favor of convenience. This, in turn, increases the success probability of attacks and the resulting damage, especially if the same information is reused among multiple different accounts or resources.

Although frameworks suggest a holistic approach to security, breach reports, cybersecurity guidelines, and awareness programs are primarily focused on increasing password security only; they give less attention to enforcing strong usernames. As a consequence, several malpractices regarding account identifiers are overlooked. For instance, users are provided with the opportunity of updating their passwords in most websites, whereas the possibility of changing account name is not considered, and, in some cases, not even allowed. Indeed, negligence in credentials management increases the impact of breaches: most recent cyberattacks are measured in millions of leaked credentials [5]. Moreover, some attacks address less-valuable targets with the purpose of gathering account credentials that can be exploited to access other platforms: in 2016, over 7 million accounts were leaked from a community on Minecraft, a popular virtual world especially utilized by youth for gaming and playful creativity [6]. Furthermore, hackers typically disseminate databases containing breached accounts in the dark web, which aggravates the problem: the so-called Anti Public Combo List contains more than 500 million usernames and passwords from various unrelated cyberattacks and data leaks that occurred over the past several years [7]. Simultaneously, this increases the risk and occurrence of credential stuffing, that is, the automated injection of breached username and password pairs on popular websites.

In this paper, we focus on the robustness of account names, and we present the results of a study in which we analyzed the human factors that affect security of credentials. Specifically, we were interested in evaluating whether technical background, security awareness, and familiarity with information technology have an influence on individuals' approaches to username generation strategies.

2 Related Work

A large body of scholarly work in cybersecurity mainly focused on passwords: studies showed that most users tend to create short and convenient key phrases that incorporate pieces of personal information, and that they reuse them across multiple accounts [8]. Therefore, in addition to stimulating awareness programs and guidelines for enforcing the security of passwords, research fostered the development of systems for generating more robust key phrases (e.g., requiring minimum length and special symbols) and more sophisticated access control procedures (e.g., two-factor authentication). Nowadays, users are provided with a considerable number of options for enforcing their password, though they might decide to deliberately ignore them.

In contrast, usernames received negligible attention: only a few studies specifically investigate their impact on account integrity [4] [5]. Nowadays, most Internet accounts use user's e-mail address or phone number as identification criteria, especially on popular web platforms (e.g., Facebook), whereas research focused on more personalized access credentials, such as, biometric identification. Nevertheless, regardless of the type of information utilized to recognize a user, account names are the first line of defense from a security standpoint, especially in websites that contain more valuable information (e.g., bank accounts, trading data), in personal devices, and in other private digital resources (e.g., routers and Wi-Fi connection).

The authors of [9] reported that very little attention has been given to the format of usernames and they concluded that most organizations use some variation on the first and last name of the user as an account identifier. This, in turn, makes usernames very easy to obtain. In [10], the authors studied that typically usernames reflect owner's habits and personal information. As for passwords, easy-to-understand usernames are convenient for individual user accounts even in presence of password management software [11]; moreover, identifiers are subject to the widely adopted practice of reusing the same name across multiple accounts [12].

3 Human Factors in Username Practices

The convenience of an easy-to-understand account name relies in the possibility of using strings that make it easier for users to identify a specific resource they want to get access to. This is particularly the case of open wireless networks (e.g., in airports, hotels, and cafeterias) for which a clear reference to the resource (e.g., AirportFree-Wifi) makes it seamless for users to identify which network they can connect to. Indeed, this is suitable for assets that are meant to be easily discovered and utilized by individuals who potentially are not aware of the existence of said resource. In this case, the ergonomic aspect of an account name is a significant factor that justifies security trade-offs. On the contrary, user accounts, private wireless networks, and other digital assets that require higher degrees of privacy and access control should involve less compromise and guarantee security levels that are proportional to the sensitivity of information in a single account and to the potential risk that breaching one account has on other resources. In this regard, considering human factors is crucial for solving the optimization problem resulting from the inevitable trade-off between usability and complexity, that is, between effort to use and effort to crack.

In this Section, we review the key aspects that affect the security of account names: some of them (i.e., 3.1, 3.2, 3.3, and 3.4) are related to how access control systems are designed, whereas other factors (i.e., 3.5 and 3.6) are primarily determined by users' behavior. A third group of items consists of potential strategies that can be implemented as an improvement. Their technical characteristics and impact on ergonomics are detailed.

3.1 Account Names Shown in Clear

Access screens in personal computers, as well as registration and access forms on websites, typically show the account name in clear, whereas passwords are hidden or masked using characters that prevent individuals, including the user, from seeing them. Although password managers are designed to provide an additional security measure, they implement this mechanism as well [11]. This, in turn, might contribute to educating users that account names do not involve any security concerns and might lead to the misperception that account identifiers are expendable.

3.2 Social Exposure of Username

Indeed, risk is proportional to the number of people who have access to the account name and to the resource: while it can be lower for the credentials of a personal computers in a household, it is extremely higher in social media websites, where the account name (i.e., login identifier) and nickname are utilized interchangeably, openly shared with acquaintances, and exposed to billions of unknown users. Moreover, social media dynamics inherently promote advertising the account name in various ways as an instrument for gaining popularity and followers. Additionally, some platforms use the username itself as an access credential. In this context, the security of the account basically translates to the time required to crack the password only, as the username is already known. Although most social media websites have robust systems for preventing brute-force attacks, several hacking techniques could be utilized together to neutralize them.

3.3 Real-time Feedback about Duplicate Usernames

Some websites incorporate systems that facilitate account name selection by providing users with real-time feedback about their account identifier: as they type, the system notifies them if the name they chose is already taken, so that they can pick a different one. Although this streamlines account creation, it exposes existing account names to botnet attacks that could leak lists of usernames by attempting them. The impact of this breach might be significant because once account names are known, they can be exploited for further intrusion involving brute-force attacks to the password component of credentials, only. Indeed, such platforms might prevent this type of risk by introducing traffic-limiting and anti-bot systems. Nevertheless, given the probability of account name reuse, breached lists could be utilized to target other or resources that implement less-secure protocols against attackers.

3.4 E-mail Utilized as Account Name

As discussed earlier, nowadays most websites utilize e-mail addresses as account identifiers, which, in turn, might facilitate username breaches: e-mails are featured in company directories, on business cards, and among contact information in websites. Also, they are perceived as communication tools that can be advertised with no other risk than receiving more spam. Moreover, as it is very common in organizations to use standard e-mail formats (e.g., firstname.lastname@organization.website) [9], usernames are easy to guess.

3.5 Account Names Based on Personal Information

The dynamic described in 3.4 might induce individuals in the malpractice of reusing the same pattern (i.e., some combination of first and last name) as an account identifier for other resources or websites. As discussed in [13], the probability that two usernames refer to the same physical person strongly depends on the entropy of the username string itself. Experiments showed that weak usernames can be utilized to identify the same individual on different platforms and gather more information about their identity [9]. This is especially true when a single account name is reused. However, research showed that individual components of an identifier created using personal information (e.g., the nickname or last name) are enough to associate multiple accounts on different resources to a unique individual [12].

3.6 Account Name Reuse

Considering users' approach to password reuse, they might have a high tendency to reiterate the same identifier for other resources. As a result, both their username and key phrase are not unique. Furthermore, users' switching behavior results in keeping accounts open even if they are not being utilized [14]: information in the username can be used as a stepping stone to attack other services or websites that might have lower levels of security, for identity theft purposes [12]. The risks of the exposure of identifiers and passwords have been detailed by [15].

3.7 Strength Meters

Indeed, avoiding account reuse mitigates the impact of breaches. Conversely, having a more secure username reduces the risk of brute-force cyberattacks. In this regard, length and entropy are two fundamental features that determine the difficulty to guess a string, and thus, they are relevant to security, because they increase the time to crack [9]. Password meters utilize them for calculating the strength of key phrases and for providing users with feedback that helps them increase TTC. Unfortunately, studies showed that individuals approach password meters as a checklist and they do not enforce security beyond the minimum required level [16]. Using two strength meters (one for the identifier and one for the key phrase) might affect usability.

3.8 Enabling Account Name Change

In addition to creating a strong key phrase that maximizes TTC, changing password often is among the most effective practices for maintaining an account secure. This is already implemented in wireless networks and computer authentication. However, very few websites offer the option of modifying the account name, though most of them provide users with the option of changing their key phrase and even require users to update their password. Enabling the possibility of modifying their account names might help protect credentials. Indeed, this might disrupt the dynamics of websites, such as, social media, that use the account name as a nickname. Conversely, this opportunity could be utilized in other types of resources: to avoid impacting convenience, it could be given as an option, or requested ad hoc, whenever a major security concern arises.

3.9 Forcing Account Name Expiration

Many accounts, especially in the corporate world, have passwords that expire [17]. Username expiration could be forced in cases that require higher levels of security, such as, bank accounts. However, users might find it very inconvenient, though they are familiar with the procedure (i.e., similar to changing the password). Indeed, this would contribute to minimizing users' digital footprints, because accounts would automatically be deactivated upon expiration of the username. Nevertheless, many usability aspects make this option less actionable; as a remedy, it could be possible to define an expiration time that is inversely proportional to usage; this is to prevent deprecating accounts that are not utilized very often without having the possibility of alerting users; on the other hand, this would create some inconvenience for the users of resources that are frequently accessed, who would be required to change their username more often. Additionally, this solution might be beneficial from a privacy standpoint, as it would limit the number of resources that store users' information. On the other hand, websites would not accept this measure because it would affect their total user count, which is utilized by many companies to demonstrate large user bases, though they could use more accurate metrics (e.g., monthly active users).

4 Study

In the previous Section, we reviewed several aspects related to the security of a username and we discussed how human factors and ergonomics are involved in systems for account creation and access. Nevertheless, as the objective of our research is to improve the trade-off between effort to use and effort to crack, we realized a study to evaluate how users perceive the items described in Section 3 in terms of security and convenience of their account names.

Several datasets resulting from breaches enable investigating dynamics, such as, account name reuse. Conversely, our objective was to analyze: (1) whether users have a different approach to securing their identifiers depending on the type and importance of information in the account, and (2) the optimal trade-off between effort to use and effort to crack. To this end, we created a survey that asked respondents questions about their awareness and behavior in username generation in the context of several types of accounts requiring different levels of security.

A total of 120 participants (74 males and 46 females aged 31±11) were recruited for this study: 20 subjects (G1) were sampled among people with a cybersecurity background or expertise, whereas the rest (G2) consisted of individuals with no specific training. By doing so, we utilized respondents with cybersecurity skills as a control group. Moreover, the survey consisted of questions that enabled us to compare the perception of username practices and password behavior.

5 Results and Discussion

In our analysis, we evaluated the aspects involved in the security and convenience trade-offs that are related to both system design and user behavior (i.e., 3.1, 3.2, 3.3, 3.4, 3.5, and 3.6). Results are reported in Table 1. Specifically, the answers of G1 were used as a gold standard to evaluate the difference in terms of perceived security between the two groups.

Conversely, in regard to convenience, we aggregated the data of the two groups: this skewed the results, though it had a negligible impact on the outcome of our analysis. This was for a two-fold reason: (1) although there was statistical significance (p=0.05) between the groups for two of the considered dimensions, we found that perception of convenience was in general independent from cybersecurity training; also, (2) password generation and verification systems serve all users in the same fashion without considering their individual background or awareness.

Table 1. Results are shown in terms of perceived security (Sec), perceived convenience (Conv), and occurrence (Occ). As for the former two dimensions, a Likert scale (1 being the least secure/convenient) was utilized to collect responses; values regarding occurrence were directly collected in percentages. Data are reported separately for the control group (G1) and respondents with no cybersecurity training (G2).

Security factor	**Sec. G1**	**Sec. G2**	**Conv.**	**Occ. G1**	**Occ. G2**
Show the account name in clear (3.1)	2.12	3.61	4.23	98.75%	100.00%
Use login information as account name (3.2)	3.34	3.98	4.15	87.33%	78.22%
Give real-time feedback on duplicate username (3.3)	3.53	4.62	3.11	8.44%	11.33%
Use the e-mail address as account name (3.4)	2.44	4.32	4.54	68.80%	72.10%
Use personal information as account name (3.5)	1.98	3.64	4.12	74.12%	79.78%
Reuse the same name for multiple accounts (3.6)	1.52	3.37	4.27	82.22%	86.93%

Furthermore, we analyzed perceived security for the countermeasures outlined in Section 3 (i.e., 3.6, 3.7, 3.8, and 3.9) and we compared it with users' willingness to adopt them. Responses from the control group were considered as the gold standard in terms of perceived security, whereas the willingness to adopt was considered separately for each group. Table 2 and Figure 1 show the results. In general, individuals with a cybersecurity background tended to be more open towards adopting mechanisms for protecting account names, though the difference between groups is not statistically significant (p=0.05). Forcing account name expiration was perceived as affecting usability the most, and therefore this practice might be recommended only in websites that require higher protection standards.

Nevertheless, having the option of changing account name was accepted by the majority of respondents, and it received approximately 89% of preferences. Furthermore, users perceived that they would not be affected by removing real-time feedback about existing user names (i.e., 3.3), as this option was the most favored (a total of 90% on average among the two groups). However, this might be caused by lack of awareness of the consequences.

Table 2. Perceived security (Sec) of prevention measures and willingness to adopt (WTA) them. As the control group was utilized as a gold standard, values for 3.1 through 3.6 are similar to the ones shown in Table 1.

Prevention measure	WTA G1	WTA G1	Sec. G1
Mask account name (3.1)	76.11%	59.31%	2.12
Separate account name and nickname (3.2)	68.40%	55.32%	3.34
Prevent real-time feedback on username (3.3)	96.70%	84.21%	3.53
Avoid using e-mail as account name (3.4)	65.66%	87.11%	2.44
Avoid using personal information in account name (3.5)	74.12%	79.11%	1.98
Preventing account name reuse (3.6)	56.12%	51.09%	1.52
Use strength meters (3.7)	85.58%	78.29%	4.01
Enable account name change (3.8)	96.63%	81.04%	4.23
Force account name expiration (3.9)	8.20%	11.31%	4.45

In general, users without cybersecurity training perceived current username practices as secure, and their responses show that they are more worried about their passwords. This is consistent with the literature and with current practices. However, account leak due to real-time feedback was perceived as resulting in minimal risk by both G1 and G2. This practice was reported in 9.89% of cases, only.

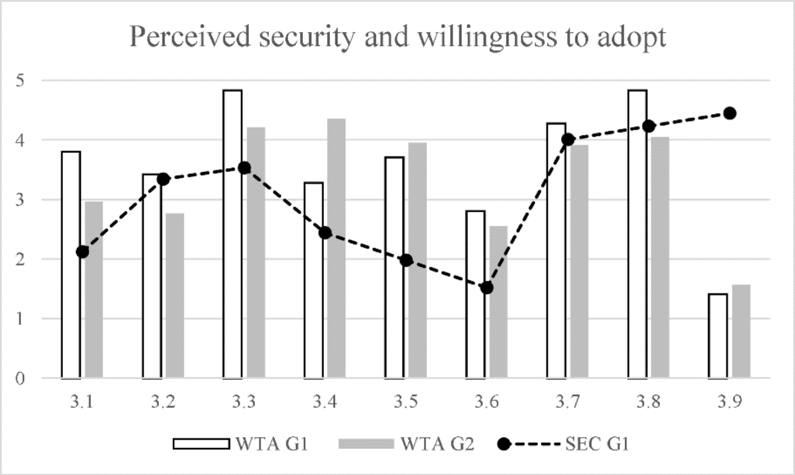

Fig. 1. Perceived security (line) and willingness to use (bars). Data about willingness to adopt (shown in Table 1) were converted from percentage to a Likert-equivalent to improve visualization. Labels on the X axis correspond to the security items outlined in Section 3 and described in Table 1.

Indeed, users know that reusing accounts that include personal information diminishes security, though both G1 and G2 reported doing it on average in 78.17% and 83.36% of the cases, respectively. This is consistent with findings in the literature [18], which report that users are aware of malpractices but they prefer to more convenient options because they think they will not be affected by an attack. We did not detail account type because we found no statistically significant difference in perceived convenience and security.

6 Conclusion

Maintaining a secure account is the result of the continuous application of multiple strategies and practices that together contribute to preventing cyberattacks. In this paper, we focused on the importance of user credentials, and specifically, account names, in enforcing the security of accounts and authentication systems as the first line of defense. Indeed, there are alternatives to text-based account names: studies showed that graphical authentication might be safer than a long complex password that users might potentially forget. However, the authors of [19] highlighted that access control methods that contain graphical components are at high risk especially on mobile devices, because the authentication process can be followed on the screen. Moreover, although access methods based on biometrics [20] are increasingly being implemented in hardware devices, string-based account identifiers are still widely utilized in software and websites to enable individuals to log in.

We reviewed current practices in creating and using access credentials and we discussed the main issues associated with poor username security. In addition to highlighting the role of human factors in authentication systems, we outlined the risks caused by common practices and their implications in terms of user experience, and we detailed how the lack of strategies for enforcing username protection affects the trade-off between convenience and security.

Moreover, we reported the results of a study in which we evaluated users' awareness of best practices, their behavior and perceived usefulness in regard to methods for securing accounts, and their potential compliance with measures for improving username security. From our findings, we can conclude that most users do not perceive the lack of username robustness as a threat for their account information and, thus, they do not take any specific prevention measures, regardless of their background. The results are particularly relevant as we did not find any statistically significant difference in the case of accounts holding sensitive information.

References

1. Caporusso, N., Chea, S. and Abukhaled, R., 2018, July. A Game-Theoretical Model of Ransomware. In International Conference on Applied Human Factors and Ergonomics (pp. 69-78). Springer, Cham. https://doi.org/10.1007/978-3-319-94782-2_7
2. Dev, J.A., 2013, August. Usage of botnets for high speed md5 hash cracking. In Innovative Computing Technology (INTECH), 2013 Third International Conference on (pp. 314-320). IEEE.
3. Brumen, B., & Taneski, V. (2015) Moore's curse on textual passwords. 2015 28th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), https://doi.org/10.1109/MIPRO.2015.7160486
4. National Institute of Standards and Technology Special Publication 800-63B. Natl. Inst. Stand. Technol. Spec. Publ. 800-63B, 78 pages (June 2017). https://doi.org/10.6028/NIST.SP.800-63b

5. Onaolapo, J., Mariconti, E. and Stringhini, G., 2016, November. What happens after you are pwnd: Understanding the use of leaked webmail credentials in the wild. In Proceedings of the 2016 Internet Measurement Conference (pp. 65-79). ACM.
6. Lenig, S. and Caporusso, N., 2018, July. Minecrafting Virtual Education. In International Conference on Applied Human Factors and Ergonomics (pp. 275-282). Springer, Cham. https://doi.org/10.1007/978-3-319-94619-1_27
7. T. Hunt. 2017. Password reuse, credential stuffing and another billion records in Have I been pwned. (May 2017). Retrieved January 31, 2018 from https://www.troyhunt.com/password-reuse-credential-stuffing-and-another-1-billion-records-in-have-i-been-pwned/
8. Stainbrook, M. and Caporusso, N., 2018, July. Convenience or Strength? Aiding Optimal Strategies in Password Generation. In International Conference on Applied Human Factors and Ergonomics (pp. 23-32). Springer, Cham. https://doi.org/10.1007/978-3-319-94782-2_3
9. Basta, A., (2015). Computer Security and Penetration Testing, 2nd Edition. Cengage Learning, 20130808. Retrieved from VitalBook file.
10. Shi, Y. (2018, March). A method of discriminating user's identity similarity based on username feature greedy matching. Paper presented at the 2018 2nd International Conference on Cryptography, Security, and Privacy. https://doi.org/10.1145/3199478.3199512
11. Wang, L., Li, Y., & Sun, K. (2016). Amnesia: A Bilateral Generative Password Manager. 2016 IEEE 36th International Conference on Distributed Computing Systems (ICDCS), 313-322.
12. Jenkins, J. L., Grimes, M., Proudfoot, J., & Lowry, P. B., (2013). “Improving password cybersecurity through inexpensive and minimally invasive means: Detecting and deterring password reuse through keystroke-dynamics monitoring and just-in-time warnings,” Information Technology for Development, vol. 20(2), pp. 196–213
13. Perito, D., Castelluccia, C., Kaafar, M. A., & Manils, P. (2011). How Unique and Traceable Are Usernames? Privacy Enhancing Technologies Lecture Notes in Computer Science, 1-17. https://doi.org/10.1007/978-3-642-22263-4_1
14. Xiao, X. and Caporusso, N., 2018, August. Comparative Evaluation of Cyber Migration Factors in the Current Social Media Landscape. In 2018 6th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW) (pp. 102-107). IEEE. https://doi.org/10.1109/W-FiCloud.2018.00022
15. Thomas, K., Li, F., Zand, A., Barrett, J., Ranieri, J., Invernizzi, L., …Bursztein, E. (2017, October). Data breaches, phishing, or malware? Understanding the risks of stolen credentials. Paper presented at the 2017 ACM SIGSAC Conference on Computer and Communications Security. https://doi.org/10.1145/3133956.3134067
16. Caporusso, N. and Stainbrook, M. 2019, July. Comparative Evaluation of Security and Convenience Trade-offs in Password Generation Aiding Systems. In International Con-ference on Applied Human Factors and Ergonomics. Springer. To be published
17. Johansson, J. M., Brezinski, D., I., & Hamer, K. L. (2011). U.S. Patent No. US13277423. Washington, DC: U.S. Patent and Trademark Office.
18. Tam, L., Glassman, M., & Vandenwauver, M. (2010). The psychology of password management: a tradeoff between security and convenience. Behaviour & Information Technology, 29:(3), 233-244, https://doi.org/10.1080/01449290903121386
19. Bošnjak, L., & Brumen, B. (2018). Improving the Evaluation of Shoulder Surfing Attacks. Proceedings of the 8th International Conference on Web Intelligence, Mining and Semantics. https://doi.org/10.1145/3227609.3227687
20. Bevilacqua, V., Cariello, L., Columbo, D., Daleno, D., Fabiano, M.D., Giannini, M., Mastronardi, G. and Castellano, M., 2008, September. Retinal fundus biometric analysis for personal identifications. In International Conference on Intelligent Computing (pp. 1229-1237). Springer, Berlin, Heidelberg.