



Projektgruppe

Sicherheit in verteilten Systemen





Bewerbung für Themen

Bewerbung

- Wir stellen heute Themen vor.
- Falls du an einem der Themen interessiert bist oder eine eigene Idee hast, bewirb dich bitte mit einem **Exposé mit kurzem Plan für das Thema.**
- Wir wählen Studenten anhand ihrer Exposés aus.
- Du kannst für mehrere Themen ein Exposé einreichen, allerdings nicht für mehr als 5 Themen.



Exposé

Kurzes Dokument (max. 2 Seiten) - Zeige, dass du in der Lage bist, wissenschaftlich zu schreiben.

(1) Motivation: Warum sollte das gewählte Thema untersucht werden?

(2) Related work des gewählten Themas: Verwandte Arbeiten anderer Wissenschaftler.

(3) Fragestellung(en) und Ziele des gewählten Themas.

(4) Geplanter zeitlicher Rahmen: Präsentiere deinen geplanten zeitlichen Rahmen für die Recherche und die Erforschung des Themas...

Bewerbung

- Bitte sende dein Exposé per E-Mail an die Person, welche das Thema präsentiert.
- **Deadline für das Exposé: 9. April**
- Am **16. April** wirst du informiert, ob du für dein favorisiertes Thema akzeptiert/nicht akzeptiert wurdest.
- **Anmeldeschluss des Labs in BASIS: 30.04.2019**

Ablauf - Zusammenfassung

1. Entscheide dich für ein/mehrere **Themen** (max. 5)
2. Bewirb dich für das Thema mit einem **Exposé** (max. 2 Seiten)
3. Falls du für ein Thema akzeptiert wurdest:
 1. Durchführung der Studie/Forschung
 2. Arbeite an dem Thema
 3. Schreibe einen wissenschaftlichen **Report**
 4. **Präsentation**



Wissenschaftliches Arbeiten

Eine kurze Erinnerung



Beim schreiben von Reports, Exposés, etc...

- Zitiere richtig:

Green and Smith [32] discussed the issue of security API usability providing examples and gave high-level recommendations to reduce developer errors.

- ..und referenziere in der Quellenangabe:

[32] Matthew Green and Matthew Smith. 2016. Developers are Not the Enemy!: The Need for Usable Security APIs. IEEE Security & Privacy 14, 5 (2016), 40–46

*Falls du eine Abbildung von anderen Wissenschaftlern nutzt,
gib die Quelle an:*

	Gender	University	Study program	Age	Nationality	Semester	How familiar are you with				Total skills
							Java	PostgreSQL	Hibernate	Eclipse IDE	
JN1	Male	University of Bonn	MSc Computer Science	NA	Bangladeshi	8	6	4	4	6	20
JN2	Female	University of Bonn	MSc Computer Science	23	Pakistani	3	3	1	1	6	11
JN3	Male	University of Bonn	MSc Computer Science	25	Uzbek	2	5	3	2	5	15
JN4	Male	University of Bonn	BSc Computer Science	23	German	6	5	2	1	6	14
JN5	Female	University of Bonn	MSc Computer Science	27	Indian	5	5	4	1	6	16
JP1	Male	University of Bonn	MSc Computer Science	25	Chinese	5	5	1	1	4	11
JP2	Male	University of Bonn	BSc Computer Science	22	German	4	6	6	1	6	19
JP3	Male	University of Bonn	MSc Computer Science	26	Iranian	4	4	2	2	6	14
JP4	Male	Aachen University	MSc Media Informatics	27	Indian	2	4	2	1	3	10
JP5	Male	Aachen University	MSc Media Informatics	25	NA	2	2	1	1	2	6
SN1	Male	University of Bonn	MSc Computer Science	24	German	10	6	4	1	5	16
SN2	Male	University of Bonn	BSc Computer Science	20	German	2	7	5	2	4	18
SN3	Male	University of Bonn	BSc Computer Science	24	German	8	6	3	1	6	16
SN4	Male	University of Bonn	MSc Computer Science	25	Syrian	3	7	5	7	7	26
SN5	Male	University of Bonn	BSc Computer Science	19	German	2	5	4	1	4	14
SP1	Male	University of Bonn	MSc Computer Science	25	NA	4	4	3	2	4	13
SP2	Male	University of Bonn	MSc Computer Science	25	Syrian	4	6	3	4	4	17
SP3	Male	University of Bonn	BSc Computer Science	20	German	2	5	3	1	4	13
SP4	Male	University of Bonn	BSc Computer Science	25	German	10	5	3	1	5	14
SP5	Female	University of Bonn	MSc Computer Science	NA	Indian	4	5	4	4	6	19

Table 1: Participant's demographics of Naiakshina et al. [1]

.. und referenziere in der Quellenangabe.

Außerdem...

- Abbildungen, Diagramme, Tabellen etc. müssen **nummeriert, betitelt** und **aus dem Text heraus referenziert** werden!
- **Wissenschaftliche** und **objektive** Sprache!
- Wir empfehlen die Nutzung von LaTeX, z.B., Overleaf

NO GO : Copy & Paste



- Vergewissere dich über die **Glaubhaftigkeit** deiner Quellen!
- Überprüfe ihre Zuverlässigkeit!
- Wikipedia ist **keine** wissenschaftliche Quelle!
- Copy& Pasting von ganzen Sätzen, Paragraphen etc. ohne Referenz ist ein Plagiat und ist unzulässig!

Vorsicht!

- Wir nutzen **Plagiatssoftware** zum Überprüfen der Abgaben.

- *Plagiat = Nichtbestehen des Kurses*

- **Deswegen: Zitiere richtig und nutze kein Copy & Paste!**

the quality of a developer's mental model and task performance [14]. The reason developers go with MD5 and SHA-1 is not that they are bad, but that they are easy to implement and easy to use. The initial ideas for protecting passwords in Unix operating systems came from Morris and Thompson [20]. Morris and Thompson's conceptual cost of hashing algorithms also means higher cost used a slow one-way function to encode passwords, the output of developers, MD5 is many orders of magnitude faster to brute force than which has stored in the database. The purpose of having slower the same password than script. Which means when you have a list of ideas so that it would impede hackers from determining password/large number of users your password lookup on similar hardware the trial and error or via dictionary attacks. They also introduced a salt for script. Meaning you will have to invest more in the concept of salt which prevented an attacker from using algorithms. Which is why some developers generally try to use multiple accounts at once, and also stored off precomputed values completely, but it also makes you vulnerable to brute force attacks. While it was good for its time, their solution won't hold. Looking Tables, Reverse Lookup Tables and Rainbow Tables. The main approach to store a password in a database due to increases in hardware performance which it allows a poorly implemented hashing is as bad as not having any. Dictionary attacks and precomputed tables make again [7]. history of hashing et al. The best approach to store a password in a database solution came in 1999 with bcrypt which was actually a password hashing algorithm. A salting a mandatory strong password specifically designed to fill the gap that Unix systems had. introduced lowercase letters, uppercase letters, numbers, and special characters. Version 2 of the standard made a password require at least 8 characters with at least 3 of 12 character types. Database server were introduced replacing general purpose computing advanced not directly accessible from the internet, potentially via a different hardware solution introduced in 2002 named PBKDF2 which covered from most web applications. Researchers [21] found that the originally intended to be a password based key derivation function common error faced by the developers in the password storage [PKDF2] that is, a function that turns a password into a cryptographic key. One area was hashing the password without using a proper salt. Another key used to encrypt and decrypt documents. Since 1999 the stored password vulnerable to rainbow-table attacks [14]. have similar requirements to functions used to protect passwords [7]. [6]. The second most common error was storing the plain text passwords. Version 2 of the standard made a password require at least 8 characters, 46.9% of a total of 19 (19.8%) participants used a word that also be applicable to storing unencrypted passwords in the database instead of a random salt. Version 1 (3%) participants used [16]. In 2009 Colin Percival introduced scrypt [22] which is an MD5, while an 8.3% used SHA-1 family hashes. Instead of using a password open bcrypt, in web there are several ideas about a memory hash function, four (4.2%) used encryption to secure passwords. [6] fact the web is saturated with advice on how to store passwords. This is highly discouraged, since an attacker who fully implement such a solution for a web base system, ranging from access to the decryption key is able to recover plain text and/or encrypted passwords. The problem is that it is impractical. The problem has been discussed around securing user passwords. A professional recommendation since there is no authoritative hash algorithms have been developed for storing passwords need an authentication, being developers here they should do it. So that an attacker can decrypt them even if they get access to the database. [23] [24] [25] [26] [27] [28] [29] [30] [31] [32] [33] [34] [35] [36] [37] [38] [39] [40] [41] [42] [43] [44] [45] [46] [47] [48] [49] [50] [51] [52] [53] [54] [55] [56] [57] [58] [59] [60] [61] [62] [63] [64] [65] [66] [67] [68] [69] [70] [71] [72] [73] [74] [75] [76] [77] [78] [79] [80] [81] [82] [83] [84] [85] [86] [87] [88] [89] [90] [91] [92] [93] [94] [95] [96] [97] [98] [99] [100] [101] [102] [103] [104] [105] [106] [107] [108] [109] [110] [111] [112] [113] [114] [115] [116] [117] [118] [119] [120] [121] [122] [123] [124] [125] [126] [127] [128] [129] [130] [131] [132] [133] [134] [135] [136] [137] [138] [139] [140] [141] [142] [143] [144] [145] [146] [147] [148] [149] [150] [151] [152] [153] [154] [155] [156] [157] [158] [159] [160] [161] [162] [163] [164] [165] [166] [167] [168] [169] [170] [171] [172] [173] [174] [175] [176] [177] [178] [179] [180] [181] [182] [183] [184] [185] [186] [187] [188] [189] [190] [191] [192] [193] [194] [195] [196] [197] [198] [199] [200] [201] [202] [203] [204] [205] [206] [207] [208] [209] [210] [211] [212] [213] [214] [215] [216] [217] [218] [219] [220] [221] [222] [223] [224] [225] [226] [227] [228] [229] [230] [231] [232] [233] [234] [235] [236] [237] [238] [239] [240] [241] [242] [243] [244] [245] [246] [247] [248] [249] [250] [251] [252] [253] [254] [255] [256] [257] [258] [259] [260] [261] [262] [263] [264] [265] [266] [267] [268] [269] [270] [271] [272] [273] [274] [275] [276] [277] [278] [279] [280] [281] [282] [283] [284] [285] [286] [287] [288] [289] [290] [291] [292] [293] [294] [295] [296] [297] [298] [299] [300] [301] [302] [303] [304] [305] [306] [307] [308] [309] [310] [311] [312] [313] [314] [315] [316] [317] [318] [319] [320] [321] [322] [323] [324] [325] [326] [327] [328] [329] [330] [331] [332] [333] [334] [335] [336] [337] [338] [339] [340] [341] [342] [343] [344] [345] [346] [347] [348] [349] [350] [351] [352] [353] [354] [355] [356] [357] [358] [359] [360] [361] [362] [363] [364] [365] [366] [367] [368] [369] [370] [371] [372] [373] [374] [375] [376] [377] [378] [379] [380] [381] [382] [383] [384] [385] [386] [387] [388] [389] [390] [391] [392] [393] [394] [395] [396] [397] [398] [399] [400] [401] [402] [403] [404] [405] [406] [407] [408] [409] [410] [411] [412] [413] [414] [415] [416] [417] [418] [419] [420] [421] [422] [423] [424] [425] [426] [427] [428] [429] [430] [431] [432] [433] [434] [435] [436] [437] [438] [439] [440] [441] [442] [443] [444] [445] [446] [447] [448] [449] [450] [451] [452] [453] [454] [455] [456] [457] [458] [459] [460] [461] [462] [463] [464] [465] [466] [467] [468] [469] [470] [471] [472] [473] [474] [475] [476] [477] [478] [479] [480] [481] [482] [483] [484] [485] [486] [487] [488] [489] [490] [491] [492] [493] [494] [495] [496] [497] [498] [499] [500] [501] [502] [503] [504] [505] [506] [507] [508] [509] [510] [511] [512] [513] [514] [515] [516] [517] [518] [519] [520] [521] [522] [523] [524] [525] [526] [527] [528] [529] [530] [531] [532] [533] [534] [535] [536] [537] [538] [539] [540] [541] [542] [543] [544] [545] [546] [547] [548] [549] [550] [551] [552] [553] [554] [555] [556] [557] [558] [559] [560] [561] [562] [563] [564] [565] [566] [567] [568] [569] [570] [571] [572] [573] [574] [575] [576] [577] [578] [579] [580] [581] [582] [583] [584] [585] [586] [587] [588] [589] [590] [591] [592] [593] [594] [595] [596] [597] [598] [599] [600] [601] [602] [603] [604] [605] [606] [607] [608] [609] [610] [611] [612] [613] [614] [615] [616] [617] [618] [619] [620] [621] [622] [623] [624] [625] [626] [627] [628] [629] [630] [631] [632] [633] [634] [635] [636] [637] [638] [639] [640] [641] [642] [643] [644] [645] [646] [647] [648] [649] [650] [651] [652] [653] [654] [655] [656] [657] [658] [659] [660] [661] [662] [663] [664] [665] [666] [667] [668] [669] [670] [671] [672] [673] [674] [675] [676] [677] [678] [679] [680] [681] [682] [683] [684] [685] [686] [687] [688] [689] [690] [691] [692] [693] [694] [695] [696] [697] [698] [699] [700] [701] [702] [703] [704] [705] [706] [707] [708] [709] [710] [711] [712] [713] [714] [715] [716] [717] [718] [719] [720] [721] [722] [723] [724] [725] [726] [727] [728] [729] [730] [731] [732] [733] [734] [735] [736] [737] [738] [739] [740] [741] [742] [743] [744] [745] [746] [747] [748] [749] [750] [751] [752] [753] [754] [755] [756] [757] [758] [759] [760] [761] [762] [763] [764] [765] [766] [767] [768] [769] [770] [771] [772] [773] [774] [775] [776] [777] [778] [779] [780] [781] [782] [783] [784] [785] [786] [787] [788] [789] [790] [791] [792] [793] [794] [795] [796] [797] [798] [799] [800] [801] [802] [803] [804] [805] [806] [807] [808] [809] [810] [811] [812] [813] [814] [815] [816] [817] [818] [819] [820] [821] [822] [823] [824] [825] [826] [827] [828] [829] [830] [831] [832] [833] [834] [835] [836] [837] [838] [839] [840] [841] [842] [843] [844] [845] [846] [847] [848] [849] [850] [851] [852] [853] [854] [855] [856] [857] [858] [859] [860] [861] [862] [863] [864] [865] [866] [867] [868] [869] [870] [871] [872] [873] [874] [875] [876] [877] [878] [879] [880] [881] [882] [883] [884] [885] [886] [887] [888] [889] [890] [891] [892] [893] [894] [895] [896] [897] [898] [899] [900] [901] [902] [903] [904] [905] [906] [907] [908] [909] [910] [911] [912] [913] [914] [915] [916] [917] [918] [919] [920] [921] [922] [923] [924] [925] [926] [927] [928] [929] [930] [931] [932] [933] [934] [935] [936] [937] [938] [939] [940] [941] [942] [943] [944] [945] [946] [947] [948] [949] [950] [951] [952] [953] [954] [955] [956] [957] [958] [959] [960] [961] [962] [963] [964] [965] [966] [967] [968] [969] [970] [971] [972] [973] [974] [975] [976] [977] [978] [979] [980] [981] [982] [983] [984] [985] [986] [987] [988] [989] [990] [991] [992] [993] [994] [995] [996] [997] [998] [999] [1000].

Weitere Informationen...



- Kannst du in dieser Guideline finden: [Link to Guideline](#)¹
- Wir erwarten, dass deine Abgabe **den Standards der Guideline entsprechen!**

¹ https://net.cs.uni-bonn.de/fileadmin/ag/martini/lehre/Leitfaden_Ausarbeitungen-v05.pdf

Präsentationen

- Nutze **Seitenzahlen**
- Nutze **Gliederungspunkte** (3-5 Punkte pro Folie)
- Gestalte deine Präsentation visuell ansprechend.

