

## BIBLIOGRAPHY

### Books

Price, J., & Gunderloy, M. (n.d.). *Mastering™ Visual C#™.NET*.  
(1120080332)

Carpenter, T. (2012). *Microsoft Windows Operating System Essentials*. John Wiley & Sons, Inc. (Vol. 21). John Wiley & Sons, Inc.  
16 Jun 2020

Pérez, M., & Binders, B. L. R. (2003). *Kali Linux Revealed*. WD info (Vol. 3).

Sarka, D. Radevojivec, M. Durkin, W. (2018). *SQL Server 2017 Developer's Guide*. Packt Publishing

Peterson, L. L., & Davie, B. S. (2012). *In Praise of Computer Networks : A Systems Approach Fifth Edition*. Elsevier Masson SAS.

Hennig, T., Bradly, T., Linson, L., Purvis, L., & Spaulding, B. (2010). *Microsoft Access Small Business Solutions*. Wiley Publishing Inc.

Galin, D. (2018). *Software Quality: Concepts and Practices*. Wiley Publishing Inc.

Barot, T., & Oren, E. (2015). *The Dawn of the Social Messaging Era*.  
Towncenter.Gitbooks. Retrieved from [https://towcenter.gitbooks.io/guide-to-chat-apps/content/introductionthe\\_dawn\\_of/](https://towcenter.gitbooks.io/guide-to-chat-apps/content/introductionthe_dawn_of/)

### Journals and Publications

Engel, K. (2014). *The Rise and Fall of Instant Messengers*. [Blog posts].  
<http://www.whoishostingthis.com/blog/2014/10/22/instant-messengers/>

Cummings, M.L. (2004). "The Need for Command and Control Instant Message Adaptive Interfaces: Lessons Learned from Tactical Tomahawk Human-in-the-Loop Simulations." *CyberPsychology & Behavior* 7(6): 653–61.  
<http://www.liebertonline.com/doi/abs/10.1089/cpb.2004.7.653>.

Flanagin, A.J. (2005). "IM Online: Instant Messaging Use Among College Students." *Communication Research Reports* 22(3): 175–87.  
<http://www.tandfonline.com/doi/abs/10.1080/00036810500206966>.

Sweigart, C. (2003). "Instant Messaging Security." (Security 401): 1–39.  
<https://www.giac.org/paper/gsec/3907/introduction-computer-security-incident->

response/106281.

- Chavan, S. (2003). *Understanding Instant Messaging (IM) and its Security Risks*. [whitepaper].  
<https://www.sans.org/reading-room/whitepapers/protocols/understanding-instant-messaging-im-security-risks-1239>
- Lokven, T.V. (2011). "Review and Comparison of Instant Messaging Protocols." [https://www.cs.ru.nl/bachelorscripties/2011/Tim\\_van\\_Lokven\\_\\_\\_0438006\\_\\_\\_Review\\_and\\_Comparison\\_of\\_Instant\\_Messaging\\_Protocols.pdf](https://www.cs.ru.nl/bachelorscripties/2011/Tim_van_Lokven___0438006___Review_and_Comparison_of_Instant_Messaging_Protocols.pdf)
- Yulianto, B., Eileen H., Lusiana C.D., and Timothy Y.A. (2015). "Architecture and Implementation of Instant Messaging in Educational Institution." *Procedia Computer Science* 59(Iccsci): 5–13.  
<http://dx.doi.org/10.1016/j.procs.2015.07.331>.
- Letuchy, E. (2009). "Erlang at Facebook." *Architecture*: 40.  
<https://www.erlang-factory.com/upload/presentations/31/EugeneLetuchy-ErlangatFacebook.pdf>
- Zheng, L., and Stephan R. (2005). "Instant Messaging : Architectures and Concepts." *ACS Seminar*: 1–10.  
<https://pdfs.semanticscholar.org/0492/f4755b207172801e83b6a36015e74e8ac40e.pdf>
- Singh, G., and Supriya S. (2013). "A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security." *International Journal of Computer Applications* 67(19): 33–38.  
<http://research.ijcaonline.org/volume67/number19/pxc3887224.pdf>.
- Abba, I.M., Dela Cruz, M.T., Eaganathan, U., Gabriel, J. (2013). *Development of LAN Chat Messenger (LCM) Using Rational Unified Process (RUP) Methodology With Object Oriented Programming*. [Whitepaper].  
[https://worldconferences.net/proceedings/aics2013/toc/papers\\_aics2013/](https://worldconferences.net/proceedings/aics2013/toc/papers_aics2013/)
- Padate, R., and Aamna P. (2014). "Encryption and Decryption of Text Using AES Algorithm." 4(5): 883–86.  
[http://www.ijetae.com/files/Volume4Issue5/IJETAE\\_0514\\_138.pdf](http://www.ijetae.com/files/Volume4Issue5/IJETAE_0514_138.pdf)
- Mahajan, P. & Sachdeva, A. (2013). *A Study of Encryption Algorithms AES, DES and RSA for Security*. Global Journal of Computer Science and Technology Network, Web & Security, 3(15).

[https://globaljournals.org/GJCST\\_Volume13/4-A-Study-of-Encryption-Algorithms.pdf](https://globaljournals.org/GJCST_Volume13/4-A-Study-of-Encryption-Algorithms.pdf)

- Krishna, M., Jamwal, P., Chaitanya, K. S. R., Kumar, B.V. (2011). *Secure File Multi Transfer Protocol Design*. Journal of Software Engineering and Applications, 4, 311-315. [http://file.scirp.org/pdf/JSEA20110500008\\_40176219.pdf](http://file.scirp.org/pdf/JSEA20110500008_40176219.pdf)
- Del Pozo I., and Mauricio I. (2015). "CI: A New Encryption Mechanism for Instant Messaging in Mobile Devices." *Procedia Computer Science* 63(Mcs): 533–38. <http://dx.doi.org/10.1016/j.procs.2015.08.381>.
- Muller, M. J., Raven, M. E., Kogan, S., Millen, D. R., & Carey, K. (2003). Introducing chat into business organizations: Toward an instant messaging maturity model. *Group '03*, 50–57. <https://doi.org/10.1145/958160.958168>.
- Calinawan, C. C. (2015). Hybrid Encryption Algorithm Implementation on Electronic Mail Service. *SMCC Higher Education Research Journal*, 1(January), 1–16. <https://doi.org/https://dx.doi.org/10.18868/sher1j.01.00115.01>
- Mantoro, T., & Zakariya, A. (2012). Securing E-mail Communication Using Hybrid Cryptosystem on Android-based Mobile Devices. *TELKOMNIKA (Telecommunication, Computing, Electronics and Control)*, 10(4), 807–814. <https://doi.org/10.12928/telkomnika.v10i4.397>
- Eddie Law, K. L., & Leung, R. (2003). A design and implementation of active network socket programming. *Microprocessors and Microsystems*, 27(5–6), 277–284. [https://doi.org/10.1016/S0141-9331\(03\)00026-7](https://doi.org/10.1016/S0141-9331(03)00026-7)
- Nath, P. B., & Uddin, M. (2015). TCP-IP Model in Data Communication and Networking American Journal of Engineering Research ( AJER ). *American Journal of Engineering Research*, (10), 102–107. Retrieved from [http://www.ajer.org/papers/v4\(10\)/N04101020107.pdf](http://www.ajer.org/papers/v4(10)/N04101020107.pdf)
- Sarmah, N., & Hachan, M. (2018). Vulnerability Assessment and Penetration Testing (VAPT). *International Journal of Recent Trends in Engineering and Research*, 4(3), 326–330. <https://doi.org/10.23883/IJRTER.2018.4135.TRU9K>
- Gawhale, S. N. (2016). Results of Penetration Testing on different Windows Client Operating Systems, 156(6), 43–45. Retrieved from <https://www.ijcaonline.org/archives/volume156/number6/gawhale-2016-ijca-912531.pdf>

## Thesis and Dissertations

- Agustin, M.A. (2012). *Development of Hidden in Plain Sight (HIPS) Encryption*. Technological University of the Philippines (TUP), Philippines
- Torres, J.P. (2012). *Development of FileGuard: Steganography Software*. Technological University of the Philippines (TUP), Philippines
- Talpur, S. (2016). *Design and Implementation an Online Lab Exerciss for Teaching Developoment of client using socket programming in C*, Univesity of Patras, Greece
- Huong, M. H. (2014). *Implementation of AES (Advanced Encryption Standard) algorithm in communication application*. University of Malaysia Pahang, Malaysia

## Electronic SourcesX

- Desjardins, J. (2016). *The Evolution of Instant Messaging*.  
<http://www.visualcapitalist.com/evolution-instant-messaging/>
- Oikarinen, J (1988). *Founding IRC*. <http://www.mirc.com/jarkko.html>
- Vermaja, J. (n.d.). *Applicability of Instant Messaging in the Military Command and Control Systems*. [Powerpoint slides].  
[https://www.netlab.tkk.fi/opetus/s38310/04-05/Kalvot\\_04-05/vermaja\\_010305.ppt](https://www.netlab.tkk.fi/opetus/s38310/04-05/Kalvot_04-05/vermaja_010305.ppt)
- Gotrunk (2017). *The Business Benefits of Instant Messaging*.  
<https://gotrunk.com/the-business-benefits-of-instant-messaging/>
- Blvd, S.C. (2002). "Securing Instant Messaging." *Symantec Enterprise Security*: 3.  
<https://www.symantec.com/avcenter/reference/secure.instant.messaging.pdf>.
- Condon, S. (2017). *Hipchat Hacked, User Account Info and Some Content Potentially Compromised*. ZDNet News. <http://www.zdnet.com/article/hipchat-hacked-user-account-info-and-some-user-content-potentially-compromised/>
- Personage, H. (2008). "The Forensic Recovery of Instant Messages from MSN Messenger and Windows Live Messenger." (January).  
<http://computerforensics.parsonage.co.uk/downloads/msnandlivemessengerartefacts/ctsofconversations.pdf>.

Oldenburg, D. (2002). *W00w00's Instant Message: Listen Up, AOL*. The Washington Post. [https://www.washingtonpost.com/archive/lifestyle/2002/01/05/w00w00s-instant-message-listen-up-aol/49b0d9fa-a8f8-4e95-a81b-587e852becb1/?utm\\_term=.529abf5c80c1](https://www.washingtonpost.com/archive/lifestyle/2002/01/05/w00w00s-instant-message-listen-up-aol/49b0d9fa-a8f8-4e95-a81b-587e852becb1/?utm_term=.529abf5c80c1)

Remijan, M. (2014), *AES Encryption between Java and C#*. [blogpost]. <http://mjremijan.blogspot.com/2014/08/aes-encryption-between-java-and-c.html>

Schmid, H. A. (n.d.). The Architecture of the Instant Messaging System I3M. Retrieved from <https://opus.htwg-konstanz.de/frontdoor/deliver/index/docId/53/file/schmid.pdf>

Ackermann, M. (2018). *Encrypted Instant Messaging Recommendations January 2017 Why should you care ?* Retrieved from <https://hackernoon.com/encrypted-instant-messaging-recommendations-january-2017-711c03af02cc>

Lutz, M. H., & Laplante, P. A. (2003). C# and the .NET framework: Ready for real time? *IEEE Software*, 20(1), 74–80. <https://doi.org/10.1109/MS.2003.1159034>

Stallings, W. (2004). *The Windows Operating System*. Retrieved from <https://pdfs.semanticscholar.org/a1af/90c6136f0ff0f67ec93cbaa47412c42aca8d.pdf>

## Patents

Lord, R. B., Hayes, T. N., & Uberti, J. (2016). *US 9,509,681 B2*. US. [https://doi.org/10.1016/j.\(73\)](https://doi.org/10.1016/j.(73))