UNIVERSIDADE DO EXTREMO SUL CATARINENSE
Curso de Ciência da Computação
Trabalho de Conclusão de Curso I
Prof. Dr. Rogério Antônio Casagrande
Profa. Dra. Merisandra Côrtes de Mattos Garcia

X

PROPOSTA DE TRABALHO DE CONCLUSÃO DE CURSO (TCC)

1. IDENTIFICAÇÕES

ALUNO

NOME: Augusto Savi
FASE: 7
TELEFONE RESIDENCIAL:
TELEFONE CELULAR: (48) 998685622
E-MAIL: guto_savi@unesc.net

PROFESSOR ORIENTADOR

NOME: Giácomo Antônio Althoff Bolan
DEPARTAMENTO: CIÊNCIA DA COMPUTAÇÃO
E-MAIL: kinhobolan@live.com

Área: Sistemas Multimídia
Orientador: Giácomo Antônio Althoff Bolan X

2. PROPOSTA DE TCC

TÍTULO DO PROJETO

Segurança e privacidade em trocas de mensagem de texto ponta a ponta realizadas em comunicadores instantâneos através de computadores

OBJETO DE ESTUDO

1. Segurança
2. Privacidade
3. Criptografia
4. Comunicação
5. Hardware

DEFINIÇÃO DO PROBLEMA

Segundo Oliveira et al. (2012), O conceito de segurança da informação está diretamente ligado com a proteção de um conjunto de dados, no sentido de preservar o valor que possuem para um indivíduo ou uma organização, visto o que remete a ser proteção da informação contra ataques que possam comprometer a integridade dos dados, tanto quanto sua confiabilidade e disponibilidade que são parte dos pilares da segurança da informação.

Com a abrangência das Tecnologias da Informação e Comunicação (TICs), é encontrado comunicadores instantâneos gratuitos que permitem a troca de mensagens de texto através de computadores conectados à internet.

Internet que por definição do Oxford Advanced Learner's Dictionary é uma internacional de computadores conectando outras redes e computadores que permite que as pessoas compartilhem informações em todo o mundo.

Ao mesmo tempo, os desafios de segurança também aumentam pois estão disponíveis várias ferramentas de software que ajudam hackers a atacar computadores facilmente sem muito conhecimento da área de informática (PACHGHARE, 2021), fazendo com que a maioria dos comunicadores instantâneos aplicassem criptografia no tráfego das mensagens.

Um exemplo de uso de criptografia nos comunicadores instantâneos é o uso do Signal Protocol pelo aplicativo de mensagens Whatsapp que usa a End-to-End Encryption(E2EE), para encriptar as mensagens e permitir com que apenas as pontas consigam acessar as mensagens, escondendo elas de qualquer indivíduo que poderia monitorar toda a comunicação entre as pontas (RASTOGI, 2017).

Porém malware, software maliciosos que tem alta propagação, tem como objetivo roubar informações, corromper arquivos ou apenas fazer atividades maliciosas para incomodar os usuários, sempre vêm com novas ideias para dificultar a detecção por antivírus. (Bergeron, 2001).

Um exemplo de malware que consegue burlar o E2EE é o Keylogger, uma ferramenta afim de gravar todas as teclas digitadas no teclado do computador e as envia para a pessoa que está realizando o ataque (R. Venkatesh e R. K. Sekhar, 2015).

Então todas as mensagens enviadas, e-mails, senhas digitadas através do teclado serão roubadas sem o usuário do computador perceber (Robbi Rahim, 2018).

Com isso, mesmo que o meio de comunicação esteja criptografado, o fato do computador estar infectado por um malware quebra todo o princípio da segurança da informação.

Sabendo que os teclados ainda permanecem como o meio de entrada mais popular para inserir grandes quantidades de textos sem erros (ZHANG, YAN, NARAYANAN, 2017).

Sendo assim, esta proposta de pesquisa, busca desenvolver uma solução para aumentar a segurança na comunicação ponta a ponta feita através de comunicadores instantâneos utilizando arduino como meio de encriptação entre o teclado do usuário e o computador.

Também se propõe a aplicação de testes para validar a efetividade da solução desenvolvida.

OBJETIVO GERAL

Desenvolver uma solução que aumenta a segurança e privacidade em trocas de mensagem de texto realizadas em comunicadores instantâneos através de computadores conectados à internet.

OBJETIVOS ESPECÍFICOS

Os objetivos específicos desta pesquisa consistem em:

1. Compreender o conceito de segurança da informação, criptografia, comunicação ponta a ponta e interfaces de comunicação com o computador;

2. Desenvolver uma solução capaz de aumentar a segurança e privacidade da comunicação realizada através de comunicadores instantâneos utilizando arduino como meio de encriptação entre o teclado do usuário e o computador.;

3. Empregar testes para validação de efetividade da solução desenvolvida;

4. Analisar os resultados dos testes empregados;

JUSTIFICATIVA

Atualmente os usuários e empresas protegem sua segurança e privacidade utilizando antivírus, software esse, que trabalha em tempo integral contra os malwares, realizando análise de anomalias, comportamental e técnicas de proteção binária, porém os malwares contra atacam, utilizando diferentes formas de entrada, ofuscação e manipulação de dados, dificultando a sua detecção (GENÇ, LENZINI, SGANDURRA, 2021).

Como o aumento de computadores com acesso a Internet cada vez mais onipresentes e essencial na vida corriqueira, foi exposto pela ITU (International Telecommunication Union) que o número de usuários que usam serviços de internet como comunicadores instantâneos atingiu 2,92 bilhões em 2014(ITU 2014). Porém como no mundo físico também existem criminosos na internet e com a utilização de malwares os criminosos cibernéticos, roubam informações confidenciais e esses roubos levam a danos graves e perdas financeiras. Para demonstração um relatório da Kaspersky Lab, até 1 bilhão de dólares foi roubado de instituições financeiras em 2 anos em todo o mundo com a utilização de malwares(Kaspersky, 2015) e outro relatório da Kingsoft de 2016 indicou que em média 2-5 milhões de computadores são infectados por dia(Kingsoft 2016) (YE, 2017).

Arduino que é uma plataforma eletrônica de código aberto, utilizada para prototipagem de projetos interativos de hardware e software que pode ser controlada por código(KONDAVEETI, 2021), podendo agir como um HID, Interface entre humanos e computadores(ZHAO, WANG, 2019) e contém a capacidade de agir como

um meio de coleta de entradas do usuário através do teclado, é uma ótima alternativa para agir como meio entre os hardwares(Arduino. 2015).

Utilizando o Arduino como um middleware entre o teclado externo e o computador, podemos adicionar mais uma camada de criptografia em momentos oportunos, como na troca de mensagens confidenciais realizada através de comunicadores instantâneos.

FUNDAMENTAÇÃO TEÓRICA

1. Segurança da informação.
2. Criptografia.
3. Internet.
4. Interfaces de comunicação humana.
5. Linguagem de programação.
6. Análise da validação realizada.
7. Hardware.
8. Trabalhos Correlatos.

METODOLOGIA

1. Realização do Levantamento bibliográfico;
   1.1. Estudo do conceito de criptografia;
   1.2. Estudo do conceito de Segurança da informação;
   1.3. Estudo de malwares;
   1.4. Estudo de interfaces de comunicação;

2. Seleção da criptografia que será empregada;

3. Desenvolvimento da solução.

4. Seleção e definição dos testes e medidas de efetividade a serem empregadas para validação da solução desenvolvida;

5. Realização da validação dos testes;

6. Análise da validação realizada;

RECURSOS NECESSÁRIOS

1. Hardware
   Notebook, 8Gb RAM, 1TB HD, Processador 2.40 GHz, com Windows;
   Arduino Board Model Due R3
   Adaptador USB A Fêmea para Micro USB Tipo OTG
   Teclado USB
2. Software
   Arduino IDE 1.8.19

DISPONIBILIDADE DOS RECURSOS CITADOS

Todos os recursos estão disponibilizados em ferramentas gratuitas encontradas na internet e/ou nos laboratórios de ciência da computação da UNESC e recursos próprios do acadêmico.

CRONOGRAMA

Etapas	2º SEMESTRE DE 2022					1º SEMESTRE DE 2023					2º SEMESTRE DE 2023				
	Ag.	Se.	Ou.	No.	De.	Fe.	Ma.	Ab.	Jun	Jul.	Ag.	Se.	Ou.	No.	De.
Realizar Levantamento bibliográfico;															
Estudo do conceito de criptografia															
Estudo do conceito de Segurança da informação															
Estudo de malwares															
Redação do projeto de Pesquisa															
Seleção da criptografia que será empregada															
Desenvolvimento a solução															
Seleção e definição dos testes e medidas de efetividade a serem empregadas para validação da solução desenvolvida															
Realização dos testes															
Análise da validação realizada															
Redação do TCC Final															
Elaboração da apresentação para defesa pública.															

BIBLIOGRAFIA

PERENDI, Daniel Matyas; GOPE, Prosanta. The Language 's Impact on the Enigma Machine. Cryptology ePrint Archive, 2021.

OLIVEIRA, Gabriella Domingos de et al. GESTÃO DA SEGURANÇA DA INFORMAÇÃO: perspectivas baseadas na tecnologia da informação (t.i.). 2012. 12 f. TCC (Graduação) - Curso de Biblioteconomia, Universidade Federal do Rio Grande do Norte (Campus Natal), Natal, 2012. Acesso em 5 jun. 2022.

MOREIRA, Michele Lopes; DE MEDEIROS SIMÕES, Anderson Savio. O uso do whatsapp como ferramenta pedagógica no ensino de química. Actio: Docência em Ciências, v. 2, n. 3, p. 21-43, 2017.

WHITMAN, Michael E.; MATTORD, Herbert J. Principles of information security. Cengage Learning, 2021.

Adelstein, Frank, Matthew Stillerman, and Dexter Kozen. "Malicious code detection for open firmware." Computer Security Applications Conference, 2002. Proceedings. 18th Annual. IEEE, 2002

Bergeron, Jean, et al. "Static detection of malicious code in executable programs." Int. J. of Req. Eng 2001.184-189 (2001): 79.

William, Stallings. Computer Security: Principles And Practice. Pearson Education India, 2008

TAHIR, Rabia. A study on malware and malware detection techniques. International Journal of Education and Management Engineering, v. 8, n. 2, p. 20, 2018.

R. Venkatesh and R. K. Sekhar, "User Activity Monitoring Using Keylogger," Asia Journal of Information Technology, vol. 15, no. 23, pp. 4758-4762, 2015.

RAHIM, Robbi et al. Keylogger application to monitoring users activity with exact string matching algorithm. In: Journal of Physics: Conference Series. IOP Publishing, 2018. p. 012008.

RASTOGI, Nidhi; HENDLER, James. WhatsApp security and role of metadata in preserving privacy. arXiv Prepr. arXiv1701, v. 6817, p. 269-275, 2017.

Adelstein, Frank, Matthew Stillerman, and Dexter Kozen. "Malicious code detection for open firmware." Computer Security Applications Conference, 2002. Proceedings. 18th Annual. IEEE, 2002.

Rad, Babak Bashari, Maslin Masrom, and Suhaimi Ibrahim. "Camouflage in malware: from encryption to metamorphism." International Journal of Computer Science and Network Security, 2012.

GENÇ, Ziya Alper; LENZINI, Gabriele; SGANDURRA, Daniele. Cut-and-Mouse and Ghost Control: Exploiting Antivirus Software with Synthesized Inputs. Digital Threats: Research and Practice, v. 2, n. 1, p. 1-23, 2021.

JARDINE, Eric. The case against commercial antivirus software: Risk homeostasis and information problems in cybersecurity. Risk Analysis, v. 40, n. 8, p. 1571-1588, 2020.

GARBA, Faisal A. et al. Evaluating the state of the art antivirus evasion tools on windows and android platform. In: 2019 2nd International Conference of the IEEE Nigeria Computer Chapter (NigeriaComputConf). IEEE, 2019. p. 1-4.

HULL, Gavin; JOHN, Henna; ARIEF, Budi. Ransomware deployment methods and analysis: views from a predictive model and human responses. Crime Science, v. 8, n. 1, p. 1-22, 2019.

CONCONE, Federico et al. Twitter analysis for real-time malware discovery. In: 2017 AEIT International Annual Conference. IEEE, 2017. p. 1-6.

YE, Yanfang et al. A survey on malware detection using data mining techniques. ACM Computing Surveys (CSUR), v. 50, n. 3, p. 1-40, 2017.

Blake Anderson, Daniel Quist, Joshua Neil, Curtis Storlie, and Terran Lane. 2011. Graph based malware detection using dynamic analysis. Journal in Computer Virology 4, 2011.

Sem autor: 2015-2016 Internet Security Research Report in China, Kingsoft, 2016. Disponível em: http://cn.cmcm.com/ news/media/2016-01-14/60.html. Acesso em: 06 de junho de 2022.

ZHANG, Yang; YAN, W.; NARAYANAN, Ajit. A virtual keyboard implementation based on finger recognition. In: 2017 International Conference on Image and Vision Computing New Zealand (IVCNZ). IEEE, 2017. p. 1-6.

KONDAVEETI, Hari Kishan et al. A systematic literature review on prototyping with Arduino: Applications, challenges, advantages, and limitations. Computer Science Review, v. 40, p. 100364, 2021.

ZHAO, Songyin; WANG, Xu An. A Survey of Malicious HID Devices. In: International Conference on Broadband and Wireless Computing, Communication and Applications. Springer, Cham, 2019. p. 777-786.

Sem autor: USBHost, Arduino, 2015, Disponível em: https://www.arduino.cc/reference/en/libraries/usbhost/, Acesso em: 06 de junho de 2022.

SUNYAEV, Ali. Middleware. In: Internet Computing. Springer, Cham, 2020. p. 125-154.

W.A. Stapleton, Microcontroller Fundamentals for Embedded Systems Education, in: Frontiers in Education (FIE) Conference, 2010.

Güven Y., Coşgun E., Kocaoğlu S., Gezici H., Yilmazlar E.
Understanding the concept of microcontroller based systems to choose the best hardware for applications, Res. Inventy Int. J. Eng. Sci., 7 (38) (2017)

PEOPLE, Healthy. Internet. Washington, DC: US Department of Health and Human Services, Office of Disease Prevention and Health Promotion, 2020.

PEREIRA, Bruno Venturini; SEABRA, Isadora Garcez; QUINTANA, Igor Messias Herzer. A INTERNET. ANAIS CONGREGA MIC-ISBN 978-65-86471-05-2, n. 12, p. 8, 2017.

Internet. In: Oxford Advanced Learner's Dictionary, 10th edition. Disponível em: https://www.oxfordlearnersdictionaries.com/us/definition/english/internet?q=internet. Acesso em: 07 de junho de 2022.

3. ASSINATURAS

ALUNO:	DATA:
PROFESSOR ORIENTADOR:	DATA:
PROFESSOR CO - ORIENTADOR:	DATA: