

TESIS
ANALISIS KEAMANAN DATA PENGGUNA PADA APLIKASI SOSIAL MEDIA
DAN WEB BROWSER



I WAYAN SINDIA GRIYA DANIKA

No Mhs : 145302288/PS/MTF

PROGRAM STUDI MEGISTER TEKNIK INFORMATIKA

PROGRAM PASCA SARJANA

UNIVERSITAS ATMA JAYA YOGYAKARTA

2018

THESIS
USER DATA SECURITY ANALYSIS ON APPLICATION OF SOCIAL MEDIA AND
WEB BROWSER



I WAYAN SINDIA GRIYA DANIKA

No Mhs : 145302288/PS/MTF

PROGRAM STUDI MEGISTER TEKNIK INFORMATIKA

PROGRAM PASCA SARJANA

UNIVERSITAS ATMA JAYA YOGYAKARTA

2018



UNIVERSITAS ATMA JAYA YOGYAKARTA
PROGRAM PASCASARJANA
PROGRAM STUDI MAGISTER TEKNIK INFORMATIKA

PENGESAHAN TESIS

Nama : I Wayan Sindia Griya Danika
Nomor Mahasiswa : 145302288
Konsentrasi : Mobile
Judu Tesis : Analisis Keamanan Data Pengguna pada Aplikasi Sosial Media dan
Web Browser

Nama Pembimbing
Prof. Ir. Suyoto, MSc., Ph.D
(Ketua)

Tanggal

Tanda Tangan

30-10-2018

Dr. Ir. Alb. Joko Santoso, MT.
(Sekretaris)

30-10-2018

Ir. A. Djoko Budiyanto, M.Eng., Ph.D.
(Anggota)

30-10-2018

Ketua Program Studi



Prof. Ir. Suyoto, MSc., Ph.D

PERNYATAAN

Nama : I Wayan Sindia Griya Danika
Nomor Mahasiswa : 145302288/PS/MTF
Konsentrasi : Mobile Computing
Judul Tesis : ANALISIS KEAMANAN DATA PENGGUNA PADA
APLIKASI SOSIAL MEDIA DAN WEB BROWSER

Menyatakan bahwa penelitian ini adalah hasil karya pribadi dan bukan duplikasi dari karya tulis yang telah ada sebelumnya. Karya tulis yang telah ada sebelumnya dijadikan penulis sebagai acuan dan referensi untuk melengkapi penelitian dan dinyatakan secara tertulis dalam penulisan acuan dan daftar pustaka.

Demikian pernyataan ini dibuat untuk digunakan sebagaimana mestinya.

Yogyakarta, Oktober 2018

I Wayan Sindia Griya Danika

INTISARI

Sosial media merupakan suatu identitas baru bagi masyarakat umum untuk saat ini dan merupakan gaya hidup (*life style*) yang tidak bisa di lupakan. Seiring perkembangan jaman ada begitu banyak sosial media yang tersebar di dunia maya atau internet setiap pengguna bebas memilih atau menggunakan sosial media yang mereka inginkan bahkan setiap orang bisa memiliki lebih dari satu sosial media. Dari banyaknya sosial media yang ada *facebook* dan *twitter* merupakan sosial media yang paling banyak digunakan oleh pengguna.

Facebook dan *twitter* sendiri merupakan sosial media yang bisa dijalankan di *smartphone* android dan iOS dan juga memiliki aplikasi natif yang bisa di *download* di masing-masing *smartphone* bisa melalui *play store* untuk android dan *Apple store* untuk iOS. Bisa juga kita menjalankan di *web browser* dari *smartphone* tersebut. Dari penggunaan aplikasi natif dan *web browser* perlu dianalisis keamanan data dari para pengguna sosial media.

Penelitian dilakukan untuk menganalisis keamanan data dari pengguna sosial media. Penelitian dilakukan di jaringan *wireless LAN* dan dilakukan penyadapan data dengan menggunakan berbagai macam teknik serangan untuk mengetahui keamanan data dari aplikasi sosial media dan juga *web browser*. Hasil dari penelitian membandingkan keamanan dari penggunaan sosial media pada aplikasi natif dan juga *web browser*.

Kata kunci : *Smartphone*, Sosial Media, *Facebook*, *Twitter*, *Wireless LAN*

ABSTRACT

Social media is a new identity for the general public for the time being and a way of life (life style) that can not be forgotten. Along the changing times there are so many social media that spread in cyberspace or the internet every user is free to choose or use soasial media they want even every person can have more than one social media. Of the many existing social media facebook and twitter social media is the most widely used by the user.

Facebook and twitter itself is social media that can run on android and iOS smartphones and also have native apps that can be downloaded on each smartphone could via the play store for android and Apple store for iOS. Can also run inside the web browser of the smartphone. From the use of native applications and web browser security to be analyzed data from the social media user.

The study was conducted to analyze security of data from social media users. The study was conducted in the wireless LAN network and do the tapping of data using a variety of attack techniques to determine the safety data from social media and the web browser. The results of the study compared the safety of the use of social media in native applications and web browsers.

Keywords: Social Media, Facebook, Twitter, Wireless LAN

Sloka 9.27

यत्करोषि यदश्नासि यज्जुहोषि ददासि यत् ।
यत्तपस्यसि कौन्तेय तत्कुरुष्व मदर्पणम् ॥ २७ ॥

*yat karoṣi yad aśnāsi yaj juhoṣi dadāsi yat
yat tapasyasi kaunteya tat kuruṣva mad-arpaṇam*

***O son of Kunti, all that you do, all that you eat, all that you offer and give away,
as well as all austerities that you may perform, should be done as an offering
unto Me.***

I Dedicated to ...

- ** Personality of Godhead***
- ** My Spiritual Master***
- ** My Family***
- ** My University***
- ** And for all Devotees***

KATA PENGANTAR

Puji dan syukur penulis ucapkan kepada Tuhan Yang Maha Esa, karena atas berkat dan rahmat-Nya penulis dapat menyelesaikan tesis yang berjudul **“Analisis Keamanan Data Pengguna Pada Aplikasi Sosial Media dan Web Browser ”**.

Penulis mengucapkan banyak terima kasih kepada semua pihak yang turut memberikan motivasi, semangat dan bantuan dalam bentuk apapun sehingga tesis ini dapat terselesaikan dengan baik :

1. Sri Krshna Kepribadian Tuhan Yang Maha Esa yang selalu memberikan saya kesempatan untuk melakukan pelayanan bhakti kepadanya.
2. H.H Bhakti Ragava Svami, guru spiritual saya yang memberikan kesempatan berbhakti dan mendukung saya menyelesaikan tugas akhir saya.
3. Bapak Prof. Ir. Suyoto, MSc., Ph.D selaku Ketua Prodi Megister Teknik Informatika dan dosen pembimbing I yang telah memberikan senyum dan sabar membantu dalam menyelesaikan tesis .
4. Bapak Dr.Ir Alb. Joko Santoso, MT., selaku dosen pembimbing II yang telah membantu membimbing hingga selesai tesis.
5. Bapak Ir. A. Djoko Budiyanto, M.Eng., Ph.D. selaku dosen penguji yang memberikan kritik dan saran terhadap tesis ini.
6. Seluruh dosen yang telah mendidik dan memberikan ilmu pengetahuan selama penulis menempuh studi di Universitas Atma Jaya Yogyakarta.
7. Staff sekretariat dan laboratorium komputer yang membantu dalam menyelesaikan tesis.

8. Chandra Pati das adikari, Gajha Gamini Devi dasi, dan Candra Vali devi dasi. Bapak, Ibu dan Adik yang telah mendukung dan selalu menyemangati untuk menyelesaikan tesis ini.
9. Ni Putu Novita Puspa Dewi yang selalu menemani dan membantu dalam penulisan tugas akhir ini. “ Semangat Bli...” .
10. Keluarga besar Narayana Smriti Ashram, yang selalu mendukung dan memberikan motivasi baut penulis.
11. Pihak-pihak lain yang turut membantu penulis dalam menyelesaikan tugas akhir ini, yang tidak dapat disebutkan satu persatu.

Penulis menyadari bahwa tesis ini masih memiliki banyak kekurangan. Oleh karena itu diperlukan saran dan kritik yang penulis harapkan dalam memperbaiki tesis ini. Akhir kata, penulis berharap semoga tesis ini bisa memberikan manfaat bagi semua pihak di masa yang akan datang. Terima Kasih.

Yogyakarta, ... Oktober 2018

I Wayan Sindia Griya Danika

DAFTAR ISI

PERNYATAAN	ii
INTISARI	iii
ABSTRACT.....	iv
HALAMAN PERSEMBAHAN	v
KATA PENGANTAR	vi
DAFTAR ISI.....	viii
DAFTAR GAMBAR.....	x
DAFTAR TABEL.....	xiii
1 PENDAHULUAN	1
1.1 LATAR BELAKANG.....	1
1.2 RUMUSAN MASALAH	3
1.3 BATASAN MASALAH	3
1.4 TUJUAN PENELITIAN	3
1.5 HALAMAN PERNYATAAN	3
BAB II.....	4
2 STUDI LITERATUR	4
2.1 TINJAUAN PUSTAKA.....	4
2.1.1 Tinjauan Pustaka.....	4
2.1.2 Pembahasan Pustaka	4
2.2 LANDASAN TEORI	6
2.2.1 Android	6
2.2.2 iOS	7
2.2.3 Sosial Media.....	9
2.2.4 Wireless.....	10
2.2.5 Teknik Serangan	11
BAB III	15
3 METODOLOGI PENELITIAN	15
3.1 TAHAPAN PENELITIAN	15
3.1.1 PERANCANGAN JARINGAN	15
3.1.2 ALAT-ALAT	16
3.1.3 ANALISIS DATA	17
3.1.4 LANGKAH-LANGKAH PENGUJIAN.....	19

3.2	DIAGRAM ALIR	21
BAB IV		22
4	PEMBAHASAN.....	22
4.1	INSTALASI	22
4.1.1	Instalasi Jaringan.....	22
4.1.2	<i>Device</i> Pengguna Jaringan	24
4.1.3	<i>Software</i> untuk <i>sniffing</i>	26
4.2	HASIL PENGUJIAN	29
4.2.1	Android	29
4.2.2	iOS	55
4.3	ANALISI PENGUJIAN.....	70
4.3.1	<i>Login</i>	70
4.3.2	Aktivitas sosial media	72
4.3.3	Tabel keseluruhan	74
4.4	ANALISIS AKHIR.....	75
4.4.1	<i>Metasploit</i>	75
4.4.2	Tingkat Keamanan	79
BAB 5		83
5	KESIMPULAN	83
5.1	KESIMPULAN	83
5.2	SARAN	84
6	DAFTAR PUSTAKA.....	85

DAFTAR GAMBAR

Gambar 2.1. Browser masing-masing platform (Virvilis et al. 2015)	5
Gambar 2.2. Phishing protection test dan malicious site test (Virvilis et al. 2015).....	5
Gambar 2.3. Android Architecture (Gronli et al. 2014)	7
Gambar 2.4. iOS Architecture (Gronli et al. 2014).....	8
Gambar 2.5. Deauthentication Attack (Noman et al. 2015)	13
Gambar 3.1. Arsitektur rancangan jaringan	15
Gambar 3.2. Diagram alir	21
Gambar 4.1. Status Wireless LAN.....	22
Gambar 4.2. Wireless settings	23
Gambar 4.3. Wireless security	24
Gambar 4.4. Android versi 5.1.1 dan android versi 8.1.0.....	25
Gambar 4.5. iPad dan iPhone.....	26
Gambar 4.6. wireshark.....	27
Gambar 4.7. Ettercap	27
Gambar 4.8. Sslstrip.....	28
Gambar 4.9. Login pada facebook aplikasi, messenger facebook, dan twitter aplikasi	30
Gambar 4.10. Login di google chrome untuk android.....	31
Gambar 4.11 Login di mozilla firefox untuk android.....	31
Gambar 4.12. Login di Opera untuk android	32
Gambar 4.13. Login di UC Browser untuk android.....	33
Gambar 4.14. Capture login facebook aplikasi.....	34
Gambar 4.15. Capture login messenger facebook aplikasi.....	35
Gambar 4.16. Capture login twitter aplikasi	35
Gambar 4.17. Capture login facebook dan twitter di mozilla firefox.....	36
Gambar 4.18. Capture login facebook dan witter di google chrome	37
Gambar 4.19. Capture login facebook dan twitter di opera	38
Gambar 4.20. Capture login facebook dan fwitter di UC Browser	39
Gambar 4.21. Capture ettercap secara keseluruhan	40
Gambar 4.22. Capture sslstrip Secara keseluruhan.....	41
Gambar 4.23. Login pada facebook aplikasi, messenger facebook dan twitter aplikasi	43

Gambar 4.24. Login di google chrome	44
Gambar 4.25. Login di mozilla firefox	45
Gambar 4.26. Login di opera	46
Gambar 4.27. Login di UC browser.....	47
Gambar 4.28. Capture login facebook aplikasi.....	48
Gambar 4.29. Capture login messenger aplikasi	49
Gambar 4.30. Capture login facebook dan twitter di Mozilla firefox	50
Gambar 4.31. Capture login facebook dan twitter di google chrome.....	50
Gambar 4.32. Capture login facebook dan twitter di opera	51
Gambar 4.33. Capture login facebook dan twitter di UC browser	52
Gambar 4.34. Capture ettercap secara keseluruhan	53
Gambar 4.35. Capture sslstrip secara keseluruhan	53
Gambar 4.36. Login di Aplikasi facebook.....	55
Gambar 4.37. Login faceook di google chrome	56
Gambar 4.38. Login faceook di Safari.....	56
Gambar 4.39. Login twitter menggunakan browser safari	57
Gambar 4.40. Capture wireshark	58
Gambar 4.41. Capture Ettercap.....	59
Gambar 4.42. Capture sslstrip.....	59
Gambar 4.43. Login aplikasi di iPhone	61
Gambar 4.44. Login facebook dan twitter di google chrome	63
Gambar 4.45. Login facebook dan twitter di safari	64
Gambar 4.46. Login facebook aplikasi	65
Gambar 4.47. Login messenger facebook aplikasi	66
Gambar 4.48. Login twitter aplikasi	66
Gambar 4.49. Login facebook dan twitter pada safari browser	67
Gambar 4.50. Login facebook dan twitter pada google chrome.....	68
Gambar 4.51. Capture ettercap secara keseluruhan	69
Gambar 4.52. Capture sslstrip untuk iPhone	69
Gambar 4.53. Login menggunakan UC browser	71
Gambar 4.54. Data UC browser.....	72
Gambar 4.55. Aktivitas pengguna di messenger facebook.....	73
Gambar 4.56. Data post messenger.....	73
Gambar 4.57. Metasploit.....	76

Gambar 4.58. Metasploit remote	77
Gambar 4.59. Ettercap metasploit remote.....	78
Gambar 4.60. Confidentiality	79
Gambar 4.61. Integrity.....	80
Gambar 4.62. Autentication.....	80



DAFTAR TABEL

Tabel 3.1 Contoh analisis data	20
Tabel 4.1. android versi 5.1.1	42
Tabel 4.2. Android versi 8.1.0	54
Tabel 4.3. iPad mini versi 9	60
Tabel 4.4. Tabel iPhone7 versi 11	70
Tabel 4.5. Android keseluruhan.....	74
Tabel 4.6. iOS Keseluruhan.....	75
Tabel 4.7 Metasploit	78
Tabel 4.8. Tingkat keamanan.....	81

