Sistemasi: Jurnal Sistem Informasi
Volume 13, Nomor 5, 2024: 1902-1913
ISSN:2302-8149
e-ISSN:2540-9719

Rekayasa Sosial dan Penyadapan Antar Perangkat Menggunakan SCRCPY untuk *Spoofing* dan *Sniffing*

Social Engineering and Inter-Device Eavesdropping Using SCRCPY for Spoofing and Sniffing

[1]Anne Ivena Wijaya, [2]Yeni Rosa Damayanti, [3]Dwi Indah Lestiani*, [4]Adinda Ayu Putri Sugiono, [5]Sherissa Callista Huanggino, [6]Demas Muhammad Rijal, [7]Renny Sari Dewi
[1,2,3,4,5,6,7]Bisnis Digital, Fakultas Ekonomika dan Bisnis, Universitas Negeri Surabaya
[1,2,3,4,5,6,7]Jl. Ketintang No.2, Ketintang, Kec. Gayungan, Kota Surabaya, Jawa Timur Indonesia 60231
*e-mail: dwiindah.22066@mhs.unesa.ac.id

(***received*:** 7 June 2024, ***revised*:** 24 June 2024, ***accepted*:** 17 August 2024)

Abstrak

Perkembangan teknologi yang pesat membuka celah baru bagi penjahat siber untuk melancarkan aksi rekayasa sosial dan penyadapan antar perangkat. Rekayasa sosial merujuk pada manipulasi, pengaruh, atau penipuan yang dilakukan untuk mendapatkan kendali atas sistem komputer. Teknik ini dimanfaatkan oleh para penjahat siber untuk mencuri informasi sensitif dari korbannya. Penelitian ini berfokus pada analisis teknik rekayasa sosial dan penyadapan antar perangkat menggunakan SCRCPY, sebuah alat kontrol layar Android yang memungkinkan kontrol jarak jauh perangkat Android dari komputer. SCRCPY menghadirkan peluang baru bagi penjahat siber untuk melancarkan serangan *spoofing* dan *sniffing*, dua teknik umum yang digunakan dalam serangan rekayasa sosial. Penelitian ini mengeksplorasi berbagai skenario penyadapan, menganalisis interaksi antara perangkat dan pengguna, serta respons sistem keamanan terhadap aktivitas mencurigakan. Hasil penelitian menunjukkan bahwa SCRCPY dapat digunakan untuk berbagai serangan rekayasa sosial dan penyadapan. Penjahat siber dapat menggunakan SCRCPY untuk mendapatkan kontrol perangkat Android korban melalui komputer desktop pelaku. Temuan ini menunjukkan bahwa serangan rekayasa sosial dan penyadapan antar perangkat menjadi semakin canggih dan sulit dideteksi. Oleh karena itu, pengguna perlu meningkatkan kesadaran mereka tentang risiko ini dan mengambil langkah-langkah untuk melindungi diri mereka sendiri.

Kata kunci: rekayasa sosial, SCRCPY, spoofing, sniffing, keamanan perangkat

Abstract

The rapid development of technology opens up new avenues for cybercriminals to carry out acts of social engineering and eavesdropping between devices. Social engineering refers to manipulation, influence, or deception used to gain control of a computer system. This technique is utilized by cybercriminals to steal sensitive information from their victims. This research focuses on analyzing social engineering and eavesdropping techniques between devices using SCRCPY, an Android screen control tool that allows remote control of Android devices from a computer. SCRCPY presents new opportunities for cybercriminals to launch spoofing and sniffing attacks, two common techniques used in social engineering attacks. This research explores various eavesdropping scenarios, analyzing interactions between devices and users, as well as security system responses to suspicious activity. The results show that SCRCPY can be used for various social engineering and eavesdropping attacks. Cybercriminals can use SCRCPY to gain control of a victim's Android device through the perpetrator's desktop computer. These findings indicate that social engineering attacks and eavesdropping between devices are becoming increasingly sophisticated and difficult to detect. Therefore, users need to increase their awareness of these risks and take steps to protect themselves.

Keywords: *social engineering, SCRCPY, spoofing, sniffing, device security*

 ISSN:2302-8149
e-ISSN:2540-9719

1 Pendahuluan

Perkembangan teknologi yang pesat membawa dampak positif dan negatif dalam kehidupan manusia. Di satu sisi, teknologi memudahkan berbagai aspek kehidupan, seperti komunikasi, informasi, dan aktivitas ekonomi. Di sisi lain, perkembangan teknologi juga membuka celah baru bagi berbagai tindak kejahatan, termasuk rekayasa sosial dan penyadapan antar perangkat. Salah satu aspek yang kerap menjadi sorotan adalah rekayasa sosial dan penyadapan antar perangkat, dua metode seperti *spoofing* dan *sniffing* sering digunakan oleh pelaku siber untuk memperoleh akses tidak sah ke dalam sistem atau data pribadi. Rekayasa sosial [1][2] adalah seni mengelabui korban untuk mengungkapkan identitas mereka dan kemudian menggunakannya untuk mendapatkan akses ke jaringan atau akun. Kemudian penyadapan antar perangkat sendiri adalah tindakan untuk memantau atau mencegat komunikasi antara dua perangkat elektronik.

Salah satu alat yang kini banyak diperbincangkan dalam dunia keamanan informasi adalah SCRCPY, sebuah aplikasi yang memungkinkan kontrol dan tampilan perangkat Android melalui komputer. Awalnya, SCRCPY dikembangkan untuk keperluan sah seperti pengujian aplikasi dan manajemen perangkat Android, namun potensi penyalahgunaannya dalam kegiatan *spoofing* dan *sniffing* tidak dapat diabaikan. SCRCPY sendiri merupakan sebuah aplikasi *open-source* yang memungkinkan kontrol dan pencerminan layar perangkat Android menggunakan USB dan mengatur jaringan melalui *TCP/IP* dengan mengaktifkan *debugging* nirkabel. Penyerang juga dapat mengawasi aktivitas pengguna dan mengontrol perangkat target dari jarak jauh. Aplikasi ini telah mendapatkan perhatian luas karena fungsionalitas dan efisiensinya. Aplikasi ini kini juga dipelajari dalam konteks keamanan siber, terutama dalam penerapannya untuk *spoofing* dan *sniffing*. *Spoofing* yang melibatkan penyamaran sebagai entitas yang sah untuk mengelabui target, dan [3] sniffing yang digunakan untuk pencurian atau intersepsi data dengan mengumpulkan lalu lintas jaringan yang memerlukan pemantauan komunikasi antar perangkat dengan memanfaatkan kemampuan SCRCPY dalam mengakses dan mengontrol perangkat dari jarak jauh.

Teknik *spoofing* dan *sniffing* memiliki kelebihan yang signifikan, terutama dalam mengeksploitasi kerentanan pada sistem Android yang sering kali minim perlindungan. Para pelaku siber dapat dengan mudah melihat dan mengontrol layar perangkat Android target melalui jaringan *Wi-Fi* yang sama. Dengan menggunakan USB dan mengatur jaringan melalui *TCP/IP*, para pelaku siber dapat mengaktifkan *debugging* nirkabel sehingga tidak terdeteksi oleh target. Dalam jaringan TCP/IP, *header* IP mengandung alamat IP sumber, alamat IP tujuan, *port* sumber, dan *port* tujuan. Alamat IP sumber mengidentifikasi *host* pengirim dan alamat IP tujuan mengidentifikasi host penerima. *Host* penerima menggunakan alamat IP sumber untuk mengarahkan balasan ke pengirim. Namun, IP *host* penerima tidak memiliki cara untuk memverifikasi keaslian alamat IP sumber paket[4]**.**

Dengan kemampuan ini, informasi sensitif seperti data pengguna dan informasi keuangan bisa diakses, menjadi sasaran yang sangat berharga bagi penyerang. Meskipun begitu, teknik ini juga memiliki kekurangan yang perlu diperhatikan. Misalnya, implementasi penyerangan menggunakan SCRCPY hanya memungkinkan pada perangkat yang terhubung dalam jaringan *Wi-Fi* yang sama. Selain itu, dampak dari serangan *spoofing* dan *sniffing* bisa sangat merusak, mengakibatkan kehilangan data, kerusakan reputasi, dan kerugian finansial yang signifikan. Dalam konteks ini, penggunaan alat seperti SCRCPY memainkan peran penting dalam mencapai tujuan serangan ini. Dengan kemampuannya untuk mengontrol dan memonitor perangkat dari jarak jauh, SCRCPY memberikan fleksibilitas yang lebih besar bagi penyerang untuk mengeksploitasi kerentanan dan menghindari deteksi yang mungkin dilakukan oleh pihak yang bersangkutan.

Dari penjelasan di atas terhadap rekayasa sosial dan penyadapan antar perangkat dengan penerapan SCRCPY dalam upaya *spoofing* dan *sniffing*, serangan yang berhasil dapat memberikan dampak yang merugikan bagi individu yang menjadi korban. Kebocoran data pribadi sensitif dapat menyebabkan kerugian finansial yang serius, merusak reputasi individu, dan menghilangkan kepercayaan dari pihak yang terlibat. Selain itu, serangan semacam ini juga dapat mengganggu operasional kehidupan pribadi, menghambat kemajuan karier, dan memerlukan upaya pemulihan yang memakan waktu dan biaya [5]. Oleh karena itu, penting bagi individu untuk memahami risiko yang terkait dengan praktik rekayasa sosial dan penyadapan antar perangkat, serta mengambil langkah-

 ISSN:2302-8149
e-ISSN:2540-9719

langkah pencegahan yang efektif guna melindungi diri dari ancaman siber yang semakin kompleks [6].

2 Tinjauan Literatur

Penelitian terkait teknik rekayasa sosial dan penyadapan antar perangkat telah banyak dilakukan dalam beberapa tahun terakhir. Penelitian yang dilakukan oleh Salahdine [7] mengungkapkan dengan adanya kemajuan teknologi digital, sistem komunikasi juga rentan dan dapat ditembus oleh pengguna siber yang tidak bertanggungjawab dan memiliki niat jahat melalui serangan rekayasa sosial. Rekayasa sosial [3] adalah metode manipulatif yang digunakan oleh penjahat siber untuk mendapatkan informasi atau akses melalui eksploitasi kelemahan psikologis manusia. Salah satu studi mengungkapkan bahwa rekayasa sosial merupakan tantangan besar bagi keamanan jaringan karena memanfaatkan kecenderungan manusia untuk mempercayai orang lain secara alami [7].

Serangan rekayasa sosial melibatkan beberapa tahap. Empat tahap umum dari serangan ini melibatkan "pengumpulan informasi, pengembangan hubungan, eksploitasi, dan eksekusi", yang merupakan bagian dari siklus serangan rekayasa sosial. Investigasi dimulai dengan mengidentifikasi korban, mengumpulkan informasi, dan menetapkan strategi serangan. Selanjutnya, penyerang melibatkan korban, mendapatkan informasi dari mereka selama periode waktu tertentu, dan kemudian pergi tanpa meninggalkan jejak [8]. Metode ini sering kali tidak dapat dicegah hanya dengan perangkat keras atau lunak, sehingga pelatihan pengguna menjadi penting untuk melawan serangan ini [9].

Rekayasa sosial dan penyadapan menggunakan aplikasi SCRCPY telah menunjukkan berbagai kerentanan dalam sistem keamanan digital. SCRCPY, sebagai alat untuk kontrol jarak jauh dan pencerminan layar perangkat Android, telah diidentifikasi memiliki potensi besar untuk disalahgunakan. Dengan SCRCPY, pelaku dapat mengaktifkan *debugging* nirkabel, yang memungkinkan akses tanpa terdeteksi oleh pemilik perangkat. Selain itu, kemampuan SCRCPY untuk mengakses dan mengontrol perangkat dari jaringan yang sama mempermudah pelaku untuk melakukan serangan *spoofing* dan *sniffing* [10]. *Spoofing*, yang melibatkan penyamaran sebagai entitas yang sah untuk mengelabui target, dan *sniffing*, yang digunakan untuk mengintersepsi data, adalah dua teknik yang sering digunakan dalam serangan rekayasa sosial. SCRCPY memungkinkan pelaku untuk melihat dan mengontrol layar perangkat Android target, menjadikannya alat yang efektif untuk kedua teknik ini [11].

Kerentanan USB *debugging* pada perangkat Android juga menjadi titik kritis yang dapat dieksploitasi oleh penyerang, terutama ketika *debugging* diaktifkan secara otomatis atau oleh *malware*. Contohnya adalah Salaxy, sebuah aplikasi yang dikembangkan untuk memungkinkan mode *debugging* USB diaktifkan secara otomatis untuk mengontrol perangkat Android [12]. Kerentanan ini menambah risiko ketika *debugging* USB tidak aman diaktifkan secara tidak sengaja atau oleh *malware* [13]. Lebih lanjut, analisis keamanan *debugging* Android menekankan pentingnya langkah-langkah keamanan yang lebih ketat untuk mencegah akses tidak sah. Kerentanan ini dapat digunakan untuk melewati keamanan layar kunci dan mendapatkan akses tidak sah ke data pribadi pengguna [14].

IP Spoofing dapat terjadi melalui celah *wireless debugging.* Penyerang memalsukan alamat IP sumber secara acak dalam paket serangan dengan metode Ran*dom Spoofed Source Address*. Ini dapat dicapai dengan membuat angka acak 32-bit dan *stamping packets*. *Route-based filtering* dapat dipengaruhi oleh teknik *spoofing*. Penyerang melakukan serangan reflektor pada *Fixed Spoofed Source Address* untuk menyalahkan serangan pada mesin tertentu. *Spoofed IP* mengandung alamat sumber yang dipilih dari daftar alamat IP yang konsisten. Metode *spoofing* acak yang sama masih digunakan untuk *Fixed Spoofing.* Pada *Subnet Spoofed Source Address,* penyerang memalsukan alamat acak dari ruang alamat yang diberikan ke subnet mesin penyerang. Sebuah mesin yang terhubung ke jaringan 192.170.186.0/24/ dapat memalsukan alamat apa pun di antara 192.170.186.0 dan 192.170.186.255 [4].

Berdasarkan literatur terbaru, penggunaan SCRCPY dapat dimanfaatkan secara efektif untuk melakukan serangan rekayasa sosial dan penyadapan antar perangkat melalui teknik *spoofing* dan *sniffing*. Penggunaan SCRCPY akan meningkatkan efektivitas serangan dengan memanfaatkan kemampuan kontrol secara *wireless*, sehingga memberikan ancaman signifikan terhadap keamanan

 ISSN:2302-8149
e-ISSN:2540-9719

perangkat Android. Analisis terhadap literatur menunjukkan bahwa kombinasi antara SCRCPY dan teknik rekayasa sosial mampu menghasilkan serangan yang lebih sulit dideteksi dan lebih berbahaya.

3 Metode Penelitian

Penelitian ini mengadopsi pendekatan kualitatif dengan fokus pada studi kasus mendalam terhadap proses penyadapan satu akun menggunakan SCRCPY. Penelitian akan mengeksplorasi berbagai skenario penyadapan, menganalisis interaksi antara perangkat dan pengguna, serta respons sistem keamanan terhadap aktivitas mencurigakan.

Data yang dikumpulkan berfokus pada *log* interaksi pengguna yakni dengan mendokumentasikan semua aktivitas yang dilakukan melalui SCRCPY pada perangkat target. Serta respons sistem keamanan dengan mencatat *feedback* dari sistem keamanan perangkat seperti notifikasi keamanan atau *log* aktivitas mencurigakan. Alat Penelitian yang digunakan dalam penelitian ini adalah alat SCRCPY untuk akses dan kontrol perangkat dan kamera atau perekam video (*screen record*) untuk mendokumentasikan interaksi secara visual jika diperlukan.

3.1 Pendekatan Penelitian

Penelitian ini mengadopsi pendekatan kualitatif dengan fokus pada observasi eksperimental. Observasi eksperimental [15] merupakan pengumpulan data dengan cara melakukan manipulasi terhadap variabel untuk melakukan pengamatan. Rancangan eksperimen ini dibagi menjadi tiga level intensitas: tinggi, sedang, dan rendah. Berikut penjelasan rinci dari setiap tingkatan tersebut:

1) Skenario pertama, untuk percobaan tingkat tinggi adalah ketika tools SCRCPY diterapkan pada perangkat laptop dan dihubungkan dengan *handphone* milik orang lain (hanya 1 unit). Kemudian melakukan pengaturan USB *debugging* di hp korban dan mengatur IP untuk *wireless debugging* ke aplikasi SCRCPY (*screencopy*). Dengan perangkat tersebut, pelaku mengakses laman dengan sekuritas level tinggi dengan mengakses aplikasi galeri, TikTok, Twitter, dan Lazada langsung dari laptop dengan *password* yang didapatkan, serta menyembunyikan aplikasi pengaturan pada perangkat korban.
2) Skenario kedua, pada percobaan tingkat sedang yaitu alat SCRCPY digunakan untuk melihat *password* dan mendengar suara yang dikeluarkan oleh perangkat korban.
3) Skenario ketiga yaitu eksperimen pada komputer lokal dengan memantau perangkat saat dioperasikan oleh korban.

3.2 Teknik Pengumpulan Data

Dalam penelitian ini, pengumpulan data dilakukan melalui pengamatan eksperimental intensitas tinggi, sedang, dan rendah untuk dapat menggunakan SCRCPY pada target telepon genggam android korban kemudian mengakses dan mengumpulkan data dari perangkat korban. Langkah pertama yang dilakukan adalah mencari target korban yang memiliki *handphone* android dan setuju untuk menjadi subjek penelitian. Setelah memperoleh persetujuan, perangkat Android milik subjek disiapkan dengan mengaktifkan mode *debugging* USB dan koneksi jaringan nirkabel yang diperlukan untuk SCRCPY. Pengaturan ini memungkinkan akses jarak jauh ke perangkat melalui laptop, yang kemudian digunakan untuk menyimulasikan skenario serangan dengan berbagai intensitas.

Eksperimen intensitas tinggi melibatkan pengaturan lanjutan dan akses ke aplikasi dengan tingkat keamanan yang tinggi seperti media sosial, aplikasi perbankan, dan *e-commerce*. Pada tahap ini, peneliti mengamati sejauh mana SCRCPY dapat mengontrol perangkat target, termasuk melihat dan mengakses data pribadi serta aplikasi yang ada. Untuk intensitas sedang, fokusnya adalah pada pengamatan interaksi dan aktivitas sehari-hari pengguna melalui SCRCPY, termasuk akses ke pesan teks, riwayat panggilan, dan penggunaan aplikasi umum. Pada tingkat rendah, peneliti mengamati aktivitas yang lebih terbatas, seperti pemantauan layar dan kontrol dasar tanpa melakukan perubahan signifikan pada perangkat.

Data yang dikumpulkan selama eksperimen mencakup log aktivitas pengguna, respons perangkat terhadap perintah dari SCRCPY, serta setiap notifikasi atau peringatan keamanan yang muncul. Dokumentasi ini dilakukan secara menyeluruh untuk memastikan bahwa semua aspek interaksi antara SCRCPY dan perangkat Android tercatat dengan baik. Dengan demikian, penelitian ini tidak hanya mengidentifikasi potensi risiko keamanan yang ditimbulkan oleh penggunaan SCRCPY, tetapi juga

menguji efektivitas dan respons dari sistem keamanan perangkat dalam menghadapi serangan tersebut [16].

3.3 Objek Penelitian

Setelah dilakukan serangkaian teknik pengumpulan data, maka didapatkan objek untuk diteliti dengan data yang tersaji pada Tabel 1. Penelitian ini terbatas pada satu akun perangkat Android yang digunakan dalam berbagai pengaturan jaringan, dengan fokus pada interaksi manusia dan sistem.

Tabel 1. Objek penelitian

Objek Penelitian	Deskripsi	Parameter yang Diamati	Metode Pengumpulan Data
Perangkat Android	Perangkat yang menjadi target penyadapan.	Versi Android OS 11, aplikasi yang terpasang, aktivitas jaringan.	Log perangkat, observasi langsung.

4 Hasil dan Pembahasan

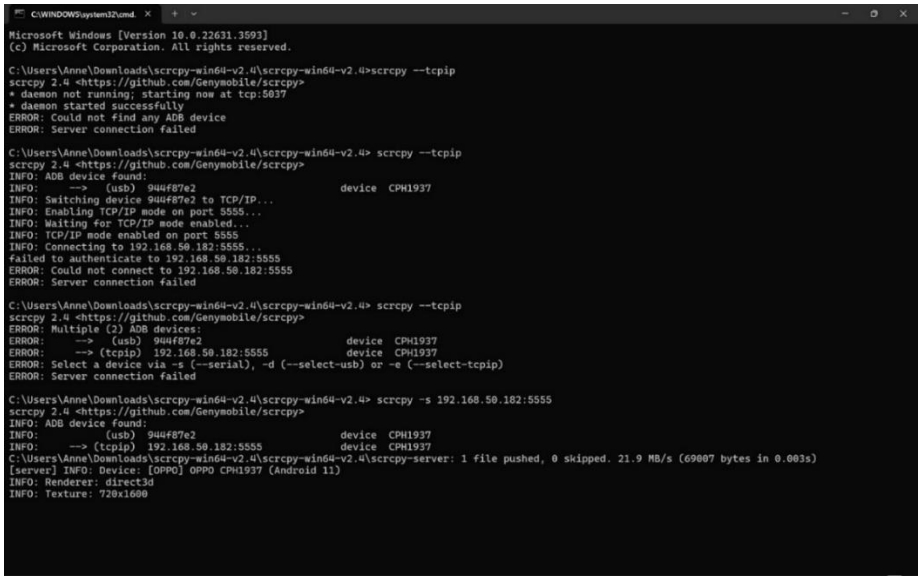
4.1 Hasil

Hasil yang diperoleh pada penerapan ketiga skenario (Subbab 3.2) dijelaskan secara rinci sebagai berikut.

Skenario pertama: Eksperimen tingkat tinggi adalah tools SCRCPY diterapkan pada perangkat *handphone* milik orang lain (hanya 1 unit). Kemudian sambungkan *handphone* korban ke komputer melalui USB terlebih dahulu lalu aktifkan pengaturan USB *Debugging* dan *wireless debugging*. Pastikan antara perangkat *handphone* terhubung di jaringan yang sama dengan perangkat komputer. Untuk melaksanakan percobaan pada skenario tersebut, beberapa tahapan yang harus dilakukan adalah:

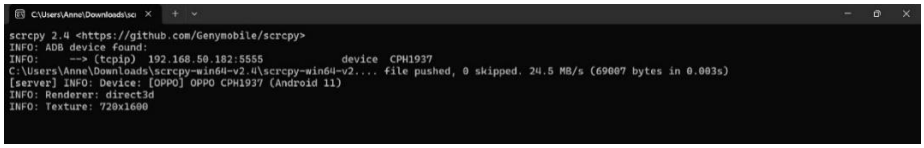
1) Pasang SCRCPY sampai dengan komputer berhasil menampilkan Gambar 1.

Gambar 1. Tampilan *software* SCRCPY yang berhasil terpasang



Gambar 2. Tampilan terminal untuk melihat perangkat yang terhubung

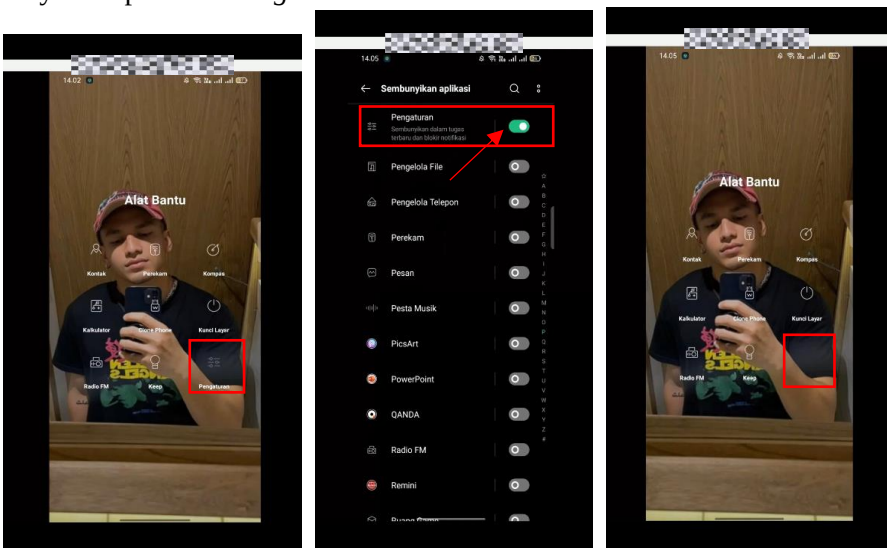
 ISSN:2302-8149
e-ISSN:2540-9719



Gambar 3. Tampilan *file scrcpy.exe* saat dijalankan

Gambar 1 menunjukkan *software* SCRCPY yang sudah terpasang dengan baik. Terdapat 2 *file* yang kita butuhkan yaitu *file scrcpy.exe* (gambar 1) dan file TCP/IP di open_a_terminal_here.bat (gambar 2) yang digunakan untuk memulai serangan pada *handphone* korban. *File* open_a_terminal_here.bat digunakan untuk melihat apakah perangkat korban sudah terhubung dengan SCRPCY dengan mengetikkan perintah "scrcpy --tcpip". Jika perangkat korban sudah terhubung maka kita dapat mengetahui IP dan *device* apa yang terhubung dengan SCRCPY pada komputer. Untuk mulai melakukan *screen mirroring* buka *file scrcpy.exe* maka akan terbuka tampilan seperti gambar 3. Tunggu beberapa saat, akan terbuka windows baru pada komputer yang menampilkan *screen copy* dari *handphone* korban.

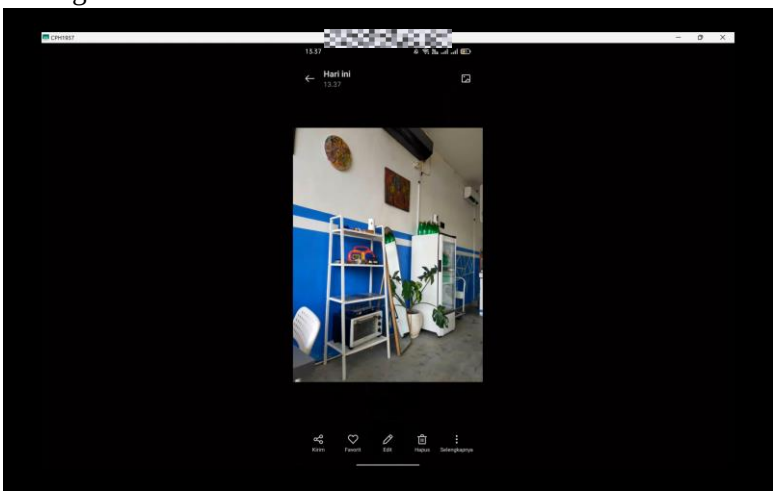
2) Menyembunyikan aplikasi *setting.*



Gambar 4. Tampilan saat menyembunyikan aplikasi *setting* korban

Pada gambar 4 tersebut menggambarkan setelah layar perangkat sudah ditampilkan pada komputer, kami mencoba menyembunyikan aplikasi pengaturan. Cara ini digunakan untuk meminimalisasi korban akan membuka pengaturan dan menonaktifkan USB *debugging*. Sehingga dapat lebih maksimal dalam mengeksploitasi *handphone* milik korban karena perangkat akan tetap terhubung dengan SCRCPY.

3) Mengakses aplikasi galeri.

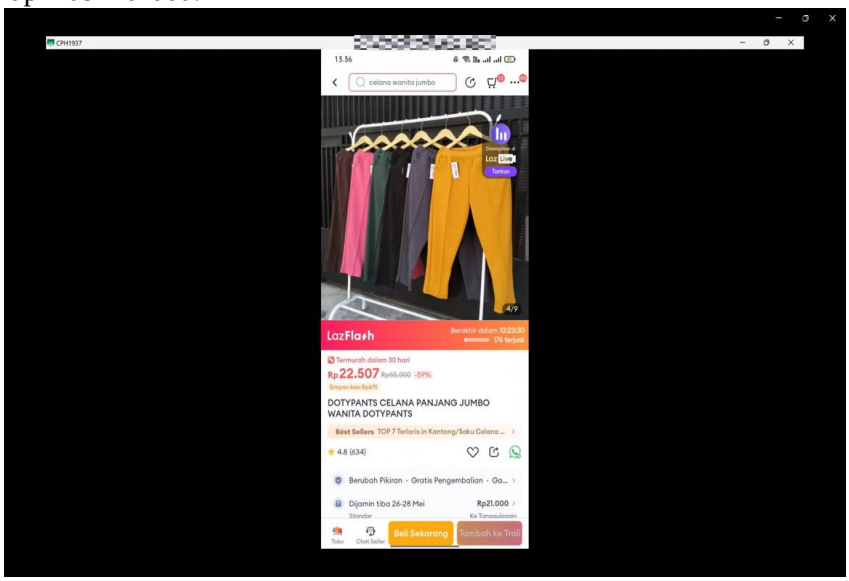


Gambar 5. Tampilan saat mengakses gallery korban

 ISSN:2302-8149
e-ISSN:2540-9719

Gambar 5 adalah saat mencoba mengakses galeri korban dari *password* yang didapat saat memantau kegiatan korban sebelumnya. Dalam hal ini gambar privasi yang masih disimpan di galeri seperti foto-foto pribadi, *screenshots* yang berisi *password* dan *username* dari sebuah *website* atau aplikasi, dan lainnya akan lebih mudah diakses. Selain itu gambar mengenai informasi pribadi seperti Kartu Tanda Penduduk (KTP), Kartu Keluarga (KK) juga dapat dimungkinkan pencurian data.

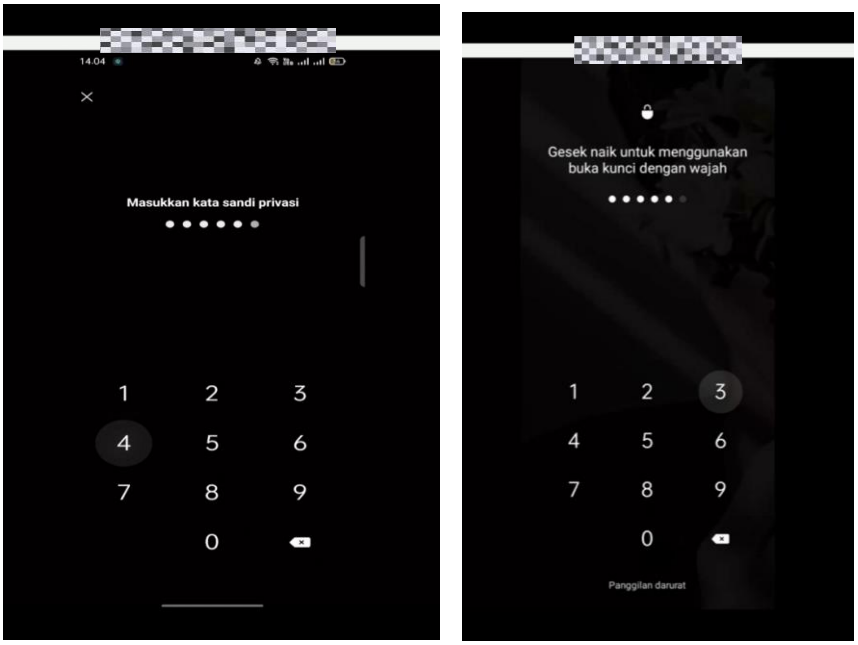
4) Mengakses aplikasi Lazada.



Gambar 6. Tampilan saat mengakses aplikasi lazada korban

Gambar 6 adalah tampilan saat memantau aktivitas korban dalam mengakses aplikasi Lazada. Melalui akses aplikasi ini dapat diketahui informasi pribadi seperti kata sandi aplikasi, informasi keuangan yang ditampilkan pada halaman *checkout*, dan informasi alamat pengiriman.

Skenario kedua: Eksperimen tingkat sedang yakni alat SCRCPY digunakan untuk melihat *password* dan mendengar suara yang dikeluarkan oleh perangkat korban.

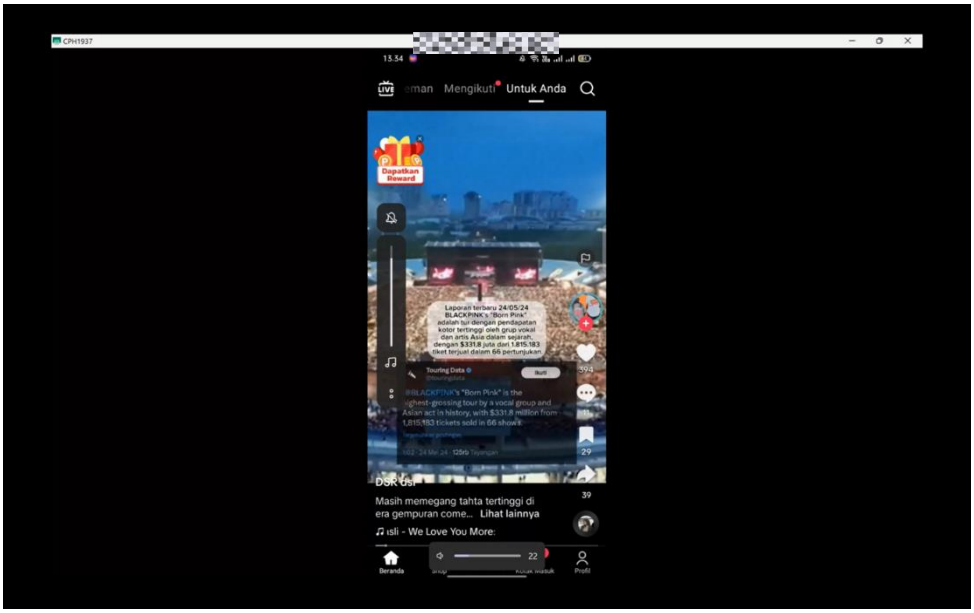


Gambar 7. Tampilan saat memantau *password handphone* korban

Gambar 7 adalah tampilan saat memantau aktivitas korban dalam memasukkan password dalam membuka perangkat dan membuka galeri. *Password* yang diketikkan akan terlihat jelas pada layar

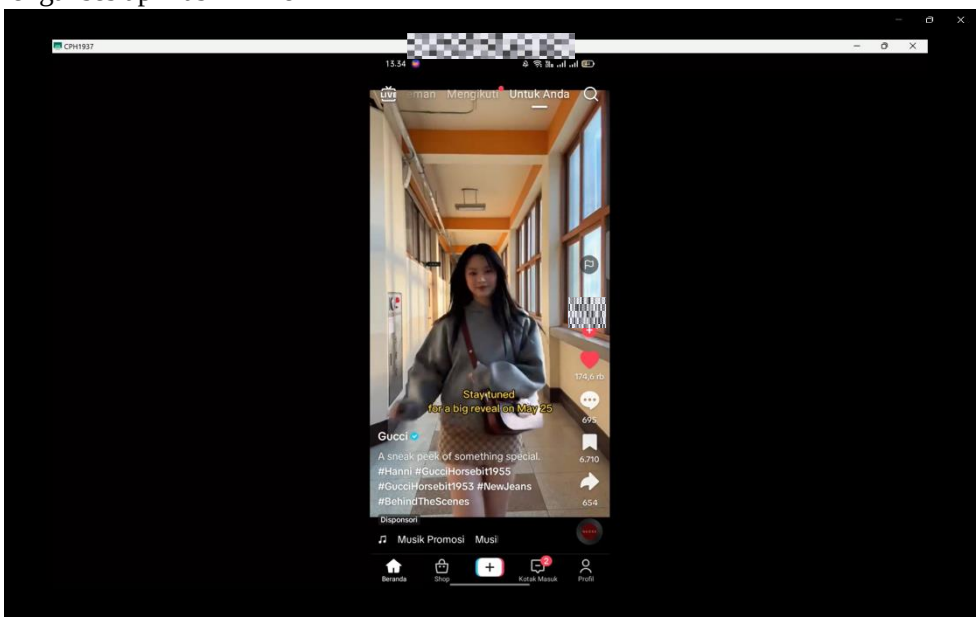
 ISSN:2302-8149
e-ISSN:2540-9719

komputer. Hal ini dapat digunakan untuk percobaan mengakses hal lain seperti log in sosial media, email, atau dalam sebuah *website*, mengingat biasanya *password* yang digunakan seseorang akan tidak jauh berbeda satu sama lain.



Gambar 8. Tampilan saat mengatur volume pada *device* korban

5) Mengakses aplikasi TikTok



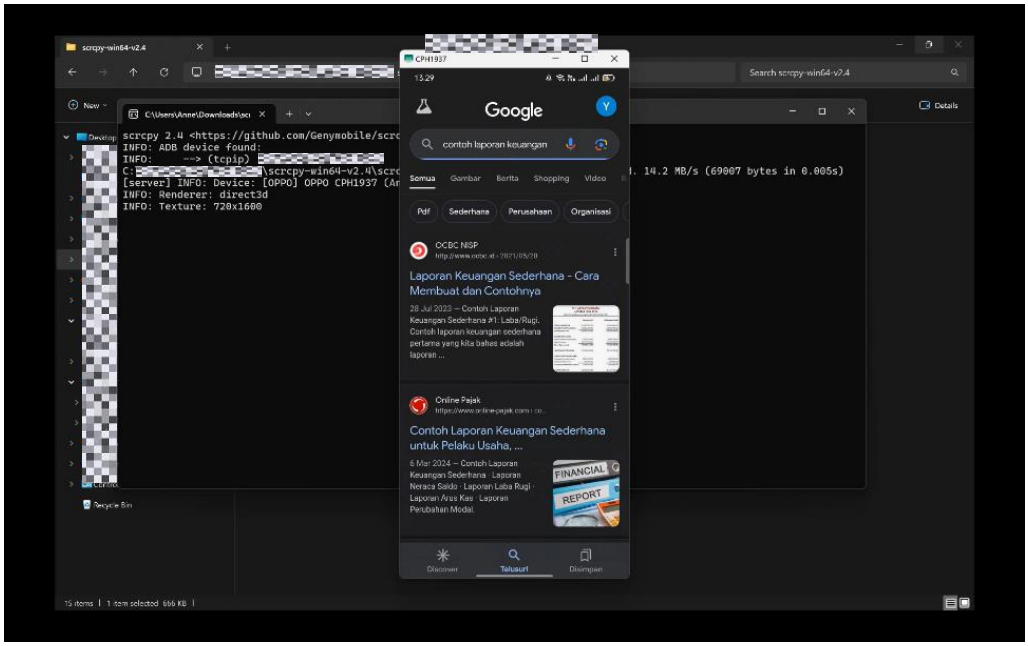
Gambar 9. Tampilan saat mengakses aplikasi tiktok korban

Gambar 9 menampilkan korban yang sedang mengakses aplikasi TikTok. Melalui aplikasi TikTok, penyusup dapat mengetahui informasi pribadi seperti alamat email yang didaftarkan, nomor *handphone*, informasi kontak tersimpan, dan informasi pembayaran pada TikTok Shop.

Skenario ketiga: Eksperimen tingkat rendah yakni eksperimen pada komputer lokal dengan memantau perangkat saat dioperasikan oleh korban. Memantau kegiatan korban yang sedang mengakses pencarian pada Google dan membuka Twitter.

6) Memantau saat user membuka google

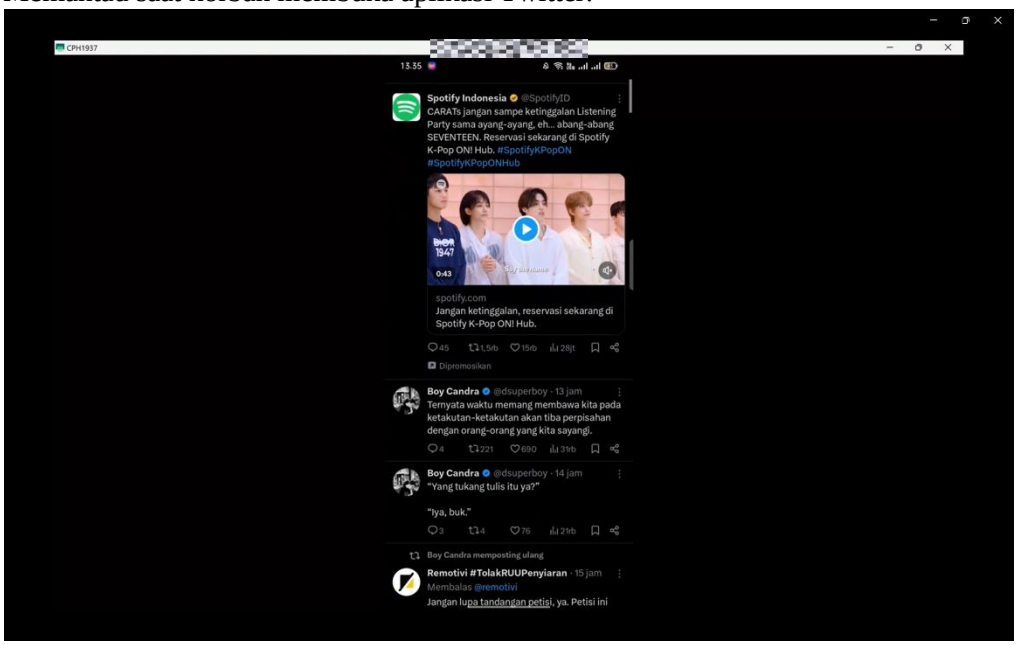
 ISSN:2302-8149
e-ISSN:2540-9719



Gambar 10. Tampilan korban yang sedang mengakses *search* pada google

Pada gambar 10 menunjukkan saat korban mengakses Google penyusup dapat mengetahui histori pencarian korban, saat akan memasukkan kata pada *search bar*. Histori ini dapat digunakan untuk mengetahui apa *website* yang terakhir kali korban buka. Hal ini dapat dimanfaatkan penyusup untuk secara *real-time* memantau minat dan kegiatan *online* korban, yang dapat digunakan untuk membuat profil lebih lanjut tentang korban, mendapatkan informasi sensitif, dan bahkan memanipulasi perilaku korban.

7) Memantau saat korban membuka aplikasi Twitter.



Gambar 11. Tampilan saat korban mengakses aplikasi twitter

Pada gambar 11 menampilkan tampilan saat korban mengakses laman Twitter. Penyusup dapat mengetahui laman Twitter yang sedang dilihat oleh korban. Penyusup dapat memantau kegiatan bersosial media korban melalui Twitter korban. Hal tersebut bisa dimanfaatkan oleh penyusup untuk mengetahui kebiasaan korban yang nantinya bisa disalahgunakan untuk kepentingan lain yang merugikan.

 ISSN:2302-8149
e-ISSN:2540-9719

4.2 Pembahasan

Penelitian ini mengeksplorasi penggunaan alat SCRCPY untuk pengawasan dan manipulasi perangkat seluler melalui tiga skenario berbeda. Pada skenario tingkat tinggi, SCRCPY digunakan untuk mengakses berbagai aplikasi di perangkat korban seperti Galeri, TikTok, Twitter, dan Lazada setelah melakukan pengaturan USB *debugging* dan konfigurasi IP untuk *debugging* nirkabel. Hasil eksperimen menunjukkan bahwa alat ini dapat dengan mudah mengakses aplikasi-aplikasi tersebut dan bahkan menyembunyikan aplikasi pengaturan untuk menghindari deteksi, menyoroti potensi risiko keamanan yang serius.

Skenario tingkat sedang berfokus pada penggunaan SCRCPY untuk melihat *password* dan mendengar suara dari perangkat korban. Eksperimen ini menunjukkan bahwa SCRCPY dapat digunakan untuk memantau *input password* dan mengatur volume perangkat dari jarak jauh, menegaskan potensi alat ini sebagai ancaman privasi dan keamanan. Kemampuan untuk mengakses informasi sensitif seperti *password* dan kontrol terhadap pengaturan perangkat memberikan gambaran tentang betapa rentannya perangkat seluler terhadap serangan semacam ini jika tidak dilindungi dengan baik.

Skenario tingkat rendah melibatkan pemantauan aktivitas korban secara lokal saat mengakses pencarian di Google. Hasil dari eksperimen ini menunjukkan bahwa aktivitas korban dapat dipantau secara efektif, memberikan wawasan tentang bagaimana pemantauan *real-time* dapat dilakukan melalui alat pencerminan layar. Ketiga skenario ini secara keseluruhan menggambarkan berbagai tingkat kerentanan yang dapat dieksploitasi melalui SCRCPY, menekankan pentingnya peningkatan keamanan pada perangkat seluler dan fitur-fitur *debugging* untuk melindungi privasi pengguna dan integritas data mereka.

Dibandingkan dengan penelitian lain di bidang ini, hasil yang diperoleh menunjukkan konsistensi dalam hal risiko yang ditimbulkan oleh penggunaan alat pencerminan layar seperti SCRCPY. Studi-studi sebelumnya juga mengindikasikan bahwa alat-alat semacam ini bisa digunakan untuk eksploitasi, terutama dalam skenario *social engineering* di mana penyerang berusaha mendekati korban dan memanipulasi mereka untuk memberikan izin akses. Misalnya, riset dari komunitas keamanan siber telah menunjukkan bahwa teknik *social engineering* yang efektif dapat mengelabui pengguna untuk mengaktifkan fitur *debugging* atau memberikan akses *remote*, yang kemudian dieksploitasi oleh penyerang untuk mengambil alih perangkat.

5 Kesimpulan

Penelitian ini menunjukkan bahwa SCRCPY sebagai alat kontrol dan pencerminan layar perangkat Android, dapat dimanfaatkan oleh penjahat siber untuk melakukan berbagai serangan rekayasa sosial dan penyadapan antar perangkat. Melalui tiga skenario eksperimen yang berbeda, ditemukan bahwa SCRCPY mampu mengakses dan mengendalikan perangkat Android dari jarak jauh dengan tingkat kerentanan yang signifikan. Berikut ini adalah hasil yang dapat disimpulkan dari penelitian di atas:

1. Pada skenario pertama tingkat tinggi, SCRCPY berhasil digunakan untuk mengakses aplikasi-aplikasi pada perangkat korban, serta menyembunyikan aplikasi pengaturan untuk menghindari deteksi.
2. Skenario kedua tingkat sedang, berhasil menunjukkan kemampuan alat ini untuk melihat *password* dan mengatur volume suara perangkat korban.
3. Sementara skenario ketiga tingkat rendah, berhasil menyoroti potensi pemantauan aktivitas korban saat melakukan pencarian di Google.

Hasil penelitian ini menegaskan bahwa SCRCPY dapat digunakan untuk berbagai serangan yang berpotensi merugikan, seperti *spoofing* dan *sniffing*, yang dapat menyebabkan kebocoran informasi sensitif dan kerugian finansial bagi korban. Kerentanan pada perangkat Android, terutama dalam pengaturan USB *debugging* dan *debugging* nirkabel, membuka peluang bagi penjahat siber untuk mengeksploitasi dan mendapatkan akses tidak sah. Oleh karena itu, penting bagi pengguna perangkat Android untuk meningkatkan kesadaran mereka tentang risiko ini dan mengambil langkah-langkah pencegahan yang efektif, seperti menonaktifkan *debugging* USB ketika tidak digunakan dan menghindari penggunaan jaringan *Wi-Fi* publik yang tidak aman.

 ISSN:2302-8149
e-ISSN:2540-9719

Referensi

[1] N. Y. Conteh and P. J. Schmick, "*Cybersecurity Risks, Vulnerabilities, and Countermeasures to Prevent Social Engineering Attacks*," in *Ethical Hacking Techniques and Countermeasures for Cybercrime Prevention*, N. Conteh, Ed., IGI Global, 2021, pp. 19–31. doi: 10.4018/978-1-7998-6504-9.ch002.

[2] Z. Wang, L. Sun, and H. Zhu, "*Defining Social Engineering in Cybersecurity*," *IEEE Access*, vol. 8, pp. 85094–85115, 2020, doi: 10.1109/ACCESS.2020.2992807.

[3] D. GlĂVan, C. RĂCuciu, R. Moinescu, and S. Eftimie, "*Sniffing attacks on computer networks," Scientific Bulletin of Naval Academy*, vol. 23, no. 1, pp. 202–207, 2020, doi: 10.21279/1454-864X-20-I1-027.

[4] N. Arumugam, "*A Novel Method for Detecting and Preventing IP Spoofing Attack in Data Network*," Aug. 2018.

[5] R. Tuli, "*Packet Sniffing and Sniffing Detection*," *International Journal of Innovations in Engineering and Technology*, vol. 16, no. 1, pp. 22–32, Apr. 2020, doi: 10.21172/ijiet.161.04.

[6] J. R. van der Merwe, X. Zubizarreta, I. Lukčin, A. Rügamer, and W. Felber, "*Classification of Spoofing Attack Types*," in *2018 European Navigation Conference (ENC)*, 2018, pp. 91–99. doi: 10.1109/EURONAV.2018.8433227.

[7] F. Salahdine and N. Kaabouch, "*Social Engineering Attacks: A Survey*," *Future Internet*, vol. 11, p. 89, 2019, doi: 10.3390/FI11040089.

[8] U. N. and S. T. and H. S. and R. S. Mashtalyar Nikol and Ntaganzwa, "*Social Engineering Attacks: Recent Advances and Challenges*," in *HCI for Cybersecurity, Privacy and Trust*, A. Moallem, Ed., Cham: Springer International Publishing, 2021, pp. 417–431.

[9] A. Koyun, "*Social Engineering Attacks*," 2020, doi: 10.1002/9781119672357.ch12.

[10] D. Xu and H. Zhu, "*Proactive Eavesdropping for Wireless Information Surveillance Under Suspicious Communication Quality-of-Service Constraint*," *IEEE Trans Wirel Commun*, vol. PP, p. 1, 2022, doi: 10.1109/TWC.2021.3138446.

[11] J. H. Anajemba, Y. Tang, C. Iwendi, A. Ohwoekevwo, G. Srivastava, and O. Jo, "*Realizing Efficient Security and Privacy in IoT Networks*," *Sensors (Basel)*, vol. 20, 2020, doi: 10.3390/s20092609.

[12] H. Lu, X. Helu, C. Jin, Y. Sun, M. Zhang, and Z. Tian, "*Salaxy: Enabling USB Debugging Mode Automatically to Control Android Devices*," *IEEE Access*, vol. 7, pp. 178321–178330, 2019, doi: 10.1109/ACCESS.2019.2958837.

[13] J. Amarante and J. P. Barros, "*Exploring USB connection vulnerabilities on android devices breaches using the android debug bridge*," in *ICETE 2017 - Proceedings of the 14th International Joint Conference on e-Business and Telecommunications*, SciTePress, 2017, pp. 572–577. doi: 10.5220/0006475905720577.

[14] K. Opasiak and W. Mazurczyk, *"(In)Secure Android Debugging: Security analysis and lessons learned*," *Comput Secur*, vol. 82, pp. 80–98, 2019, doi: https://doi.org/10.1016/j.cose.2018.12.010.

[15] H. Hasanah, "TEKNIK-TEKNIK OBSERVASI (Sebuah Alternatif Metode Pengumpulan Data Kualitatif Ilmu-ilmu Sosial)," *At-Taqaddum*, vol. 8, no. 1, pp. 21–46, 2017, doi: 10.21580/at.v8i1.1163.

[16] R. S. Dewi and Y. S. Dharmawan, "*A Proposed Model for Embedding Risk Proportion in Software Development Effort Estimation," Procedia Comput Sci*, vol. 234, pp. 1777–1784, 2024, doi: *https://doi.org/10.1016/j.procs.2024.03.185*.