ANCAMAN BUG “STAGEFRIGHT” PADA SISTEM OPERASI ANDROID

Miftahul Fadli Muttaqin (23215026)
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung
Bandung, Indonesia
miftahul.fadli@s.itb.ac.id

A. Sistem Operasi Android

Saat ini sistem operasi android sudah menjadi salah satu sistem operasi terbesar yang menguasai pangsa pasar *smartphone*, sistem operasi ini adalah sistem operasi berbasis linux yang khusus dirancang untuk perangkat *smartphone* dengan layar sentuh. Android awalnya dikembangkan oleh Android, Inc., dengan dukungan finansial dari Google, yang kemudian membelinya pada tahun 2005. Sistem operasi ini dirilis secara resmi pada tahun 2007, bersamaan dengan didirikannya *Open Handset Alliance*, sebuah konsorsium dari perusahaan – perusahaan perangkat keras, perangkat lunak dan telekomunikasi.

a. Sejarah

Android, Inc. didirikan di Palo Alto, California, pada bulan Oktober 2003 oleh Andy Rubin, Rich Miner, Nick Sears dan Chris White dengan tujuan untuk semakin mengembangkan perangkat *smartphone* yang lebih sadar akan lokasi dan preferensi penggunanya. Tujuan awal pengembangan sistem operasi android ini adalah untuk mencoba mengembangkan sebuah sistem operasi yang diperuntukkan untuk kamera digital, namun kemudian disadari bahwa pasar unuk perangkat tersebut tidak cukup besar dan pengembangan android kemudian dialihkan bagi pasar *smartphone* untuk menyaingi Symbian dan Windows Mobile.

Meskipun pengembang sistem operasi android ini adalah pakar – pakar teknologi yang sudah berpengalaman, Android, Inc. ternyata dioperasikan secara diam – diam, hanya diungkapkan bahwa para pengembang sedang mempersiapkan sebuah sistem operasi yang diperuntukkan bagi *smartphone*.

Google secara resmi mengakuisisi Andorid, Inc. pada tanggal 17 Agustus 2005 silam, menjadikannya sebagai anak perusahaan yang sepenuhnya dimiliki oleh Google. Pendiri android sendiri tetap bekerja di perusahaan setelah diakuisisi oleh Google. Di Google, tim yagn dipimpin oleh Rubin mulai mengembangkan *platform smartphone* dengan menggunakan kernel linux. Google memasarkan *platform* tersebut kepada produsen perangkat seluler dan operator telekomunikasi dengan janji bahwa mereka akan menyediakan sistem yang fleksibel dan bisa diperbarui. Google telah memilih beberapa mitra perusahaan perangkat lunak dan perangkat keras, serta mengisyaratkan kepada operator telekomunikasi bahwa kerja sama ini terbuka bagi siapapun yang ingin berpartisipasi.

Beberapa spekulasi kemudian muncul dan berkembang tentang niat Google untuk memasuki pasar komunikasi seluler terus berkembang hingga bulan Desember 2006. BBC dan Wall Street Journal melaporkan bahwa Google sedang bekerja keras

untuk menyertakan aplikasi dan mesin pencarinya di perangkat seluler. Berbagai media cetak dan media *online* mengabarkan bahwa Google sedang mengembangkan perangkat seluler dengan merek Google. Beberapa di antaranya berspekulasi bahwa Google telah menentukan spesifikasi teknisnya, termasuk produsen telepon seluler dan operator jaringan. Pada bulan Desember 2007, *InformationWeek* melaporkan bahwa Google telah mengajukan beberapa aplikasi paten di bidang telepon seluler.

Pada tanggal 5 November 2007, Open Handset Alliance (OHA) didirikan. OHA adalah konsorsium dari perusahaan-perusahaan teknologi seperti Google, produsen perangkat seluler seperti HTC, Sony dan Samsung, operator nirkabel seperti Sprint Nextel dan T-Mobile, serta produsen chipset seperti Qualcomm dan Texas Instruments. OHA sendiri bertujuan untuk mengembangkan standar terbuka bagi perangkat seluler. Saat itu, Android diresmikan sebagai produk pertamanya; sebuah platform perangkat seluler yang menggunakan kernel Linux versi 2.6. Telepon seluler komersial pertama yang menggunakan sistem operasi Android adalah HTC Dream, yang diluncurkan pada 22 Oktober 2008.

Pada tahun 2010, Google merilis seri Nexus; perangkat telepon pintar dan tablet dengan sistem operasi Android yang diproduksi oleh mitra produsen telepon seluler seperti HTC, LG, dan Samsung. HTC bekerja sama dengan Google dalam merilis produk telepon pintar Nexus pertama, yakni Nexus One. Seri ini telah diperbarui dengan perangkat yang lebih baru, misalnya telepon pintar Nexus 4 dan tablet Nexus 10 yang diproduksi oleh LG dan Samsung. Pada 15 Oktober 2014, Google mengumumkan Nexus 6 dan Nexus 9 yang diproduksi oleh Motorola dan HTC. Pada 13 Maret 2013, Larry Page mengumumkan dalam postingan blognya bahwa Andy Rubin telah pindah dari divisi Android untuk mengerjakan proyek-proyek baru di Google. Ia digantikan oleh Sundar Pichai, yang sebelumnya menjabat sebagai kepala divisi Google Chrome, yang mengembangkan Chrome OS.

b. Versi Android

Versi android diawali dengan dirilisnya Android beta pada bulan November 2007. Versi komersial pertama, android 1.0 dirilis pada September 2008. Android dikembangkan secara terus menerus oleh Google dan Open Handset Alliance, yang telah merilis sejumlah pembaruan sistem operasi ini sejak dirilis di versi awal.

Sejak April 2009, versi android dikembangkan dengan nama kode yang dinamai berdasarkan makanan pencuci mulut dan panganan manis. Masing masing versi dirilis sesuai urutan alfabet, yakni

1. Android Versi 1.0 (Astro)
   Android 1.0 atau dikenal dengan Astro (API level 1) adalah versi komersial pertama dari sistem operasi android, dirilis pada tanggal 23 September 2008. Perangkat android pertama yang tersedia secara komersial adalah HTC Dream.
2. Android Versi 1.1 (Bender)
   Android 1.1 atau dikenal dengan Bender (API level 2) adalah versi yang dirilis pada tanggal 9 Februari 2009. Seri ini awalnya hanya dirilis untuk HTC Dream. Android 1.1 juga dikenal dengan nama lain yaitu “Petit Four”

meskipun nama ini tidak digunakan secara resmi. Versi ini memperbaiki beberapa bug, mengubah API android dan menambahkan beberapa fitur pada sistem operasi android.

3. Android Versi 1.5 (Cupcake)
   Android 1.5 atau dikenal dengan Cupcake (API level 3) adalah penerus dari versi android pendahulunya. Seri android ini diperkenalkan pada akhir bulan April 2009. Seri ini dirilis menggunakan versi kernel linux 2.6.27. Versi ini adalah rilis pertama yang secara resmi menggunakan nama kode berdasarkan nama – nama makanan pencuci mulut ("Cupcake").
4. Android Versi 1.6 (Donut)
   Android 1.6 atau dikenal dengan Donut (API level 4) adalah versi selanjutnya dari sistem operasi android. Seri ini sudah menggunakan versi kernel linux yang lebih tinggi dari sebelumnya yaitu seri 2.6.29. Selain mengupdate kernelnya seri ini juga melakukan beberapa penambahan fitur dari sistem operasi android itu sendiri.
5. Android Versi 2.0/2.1 (Éclair)
   Android 2.0 / 2.1 yang lebih dikenal dengan Éclair (API level 5) merupakan seri sistem operasi android yang masih sama – sama menggunakan versi kernel linux 2.6.29. Seri ini dirilis pada tanggal 26 Oktober 2009. Seri android ini sendiri terdapat beberapa update walau masih dalam nama yang sama yaitu Éclair. Diantaranya adalah android 2.0.1 (API level 6) dan Android 2.1 (API level 7).
6. Android Versi 2.2 (Froyo)
   Versi selanjutnya dari Éclair adalah seri android 2.1 atau yang biasa disebut dengan Froyo atau *Frozen Yogurt* (API level 8). Seri selanjutnya dari Éclair ini sudah menggunakan seri kernel baru dari linux yaitu 2.6.32. Seri ini diperkenalkan pada 20 Mei 2010.
7. Android Versi 2.3 (Gingerbread)
   Versi android selanjutnya yaitu Gingerbread yang memiliki beberapa varian dari seri 2.3 – 2.3.7. Android ini sudah dibekali dengan versi kernel terbaru dari linux yaitu versi 2.6.35. Seri ini diperkenalkan pertama kali pada tanggal 6 Desember 2010. Seri android 2.3 – 2.3.2 dikenal juga dengan API level 9) sedangkan android 2.3.3 – 2.3.7 dikenal juga dengan API level 10
8. Android Versi 3.0/3.1 (Honeycomb)
   Android 3.0 dikenal dengan sebutan Honeycomb (API Level 11) adalah sistem operasi android pertama yang ditujukan hanya untuk komputer tablet. Seri ini dirilis berdasarkan seri kernel linux 2.6.36. Seri ini diperkenalkan pada tanggal 22 Februari 2011. Perangkat pertama yang menggunakan versi ini adalah table Motorola Xoom yang dirilis pada 24 Februari 2011. Seri lain yang juga menggunakan nama Honeycomb antara lain adalah versi android 3.1 (API level 12) dan android 3.2 (API level 13). Google TV generasi pertama dan kedua menggunakan Honeycomb 3.2.
9. Android Versi 4.0 (ICS : Ice Cream Sandwich)
   Seri android selanjutnya dari Honeycomb adalah seri android 4.0 – 4.0.2 atau yang biasa dikenal dengan Ice Cream Sandwich (API level 14). Seri ini dibangun menggunakan kernel linux 3.0.1. Diperkenalkan pertama kali

pada tanggal 19 Oktober 2011. Petinggi Google, Gabe Cohen menyatakan bahwa Android 4.0 secara teoritis kompatibel dengan perangkat android 2.3x yang diproduksi saat itu. Seri selanjutnya yang juga menggunakan nama ICS adalah seri android 4.0.3 – 4.0.4 (API level 15). Seri terakhir dari ICS ini sudah mendukung Flash Player yang disediakan oleh Adobe Systems. Seri ini dirilis pada tanggal 16 Desember 2011.

10. Android Versi 4.1 (Jelly Bean)
    Untuk seri android selanjutnya adalah android 4.1 atau yang biasa dikenal dengan sebutan Jelly Bean (API level 16). Google secara resmi mengumumkan android 4.1 ini pada acara konfrensi Google I/O pada tanggal 27 Juni 2012. Seri ini dibangun menggunakan kernel linux 3.0.31, seri jelly bean ini di usung – usung menjadi salah satu pembaruan terpenting karena tujuannya yang meningkatkan fungsi dan kinerja dari UI. Pembaruan ini diwujudkan melalui "Proyek Butter", perbaikan ini meliputi antisipasi sentuh, *triple buffering*, perpanjangan waktu *vsync* dan peningkatan frame rate hingga 60 fps untuk menciptakan UI yang lebih halus. Perangkat pertama yang menggunakan sistem operasi ini adalah tablet Nexus 7 yang dirilis pada 13 Juli 2012.
    Seri selanjutnya yang sama – sama menggunakan nama Jelly Bean adalah android versi 4.2 (API level 17). Jelly Bean 4.2 didasarkan pada kernel linux 3.4.0 dan pertama kali digunakan pada Nexus 4 LG dan Nexus 10 Samsung yang dirilis pada 13 November 2012.
    Masih dengan nama yang sama Jelly Bean, android versi 4.3 (API level 18) resmi dirilis pada tanggal 24 Juli 2013 di San Fransisco. Nexus 7 generasi kedua adalah perangkat pertama yang menggunakan sistem operasi android 4.3 ini.
11. Android Versi 4.4 (KitKat)
    Seri android 4.4 yang selanjutnya dikenal dengan nama Kitkat (API level 19) seri ini terlebih dahulu mendapatkan izin dari Nestle dan Hershey. Seri ini di rilis pada tanggal 31 Oktober 2013. Pada saat seri ini di umumkan sempat ada isu – isu bahwa google selanjutnya akan memberi nama untuk android 5.0 dengan nama "Key Lime Pie".
12. Android Versi 5.0 (Lollipop)
    Salah satu seri terbaru dari sistem operasi android adalah seri 5.0 – 5.1 atau yang biasa dikenal dengan Lollipop, seri ini secara resmi diperkenalkan oleh google pada acara Google I/O yang diselenggarakan pada bulan Juni 2014. Hingga Februari 2016 lalu statistik google menunjukkan bahwa 34,1% *smartphone* yang mengakses Google Play menggunakan sistem operasi Android Lollipop ini.
13. Android Versi 6.0 (Marshmallow)
    Android 6.0 atau yang biasa dikenal dengan M atau Marshmalow ini pertama kali diperkenalkan pada acara Google I/O yang digelar pada bulan Mei 2015 dan secara resmi dirilis pada bulan Oktober 2015. Tujuan utama seri Marshmalow ini dibangun adalah untuk penyempurnaan UI dari seri sebelumnya yaitu Lollipop, seri ini juga memperkenalkan arsitektur perizinan yang baru dan juga sistem *power management* yang diperbarui.

c. Keamanan dan Privasi

Aplikasi android berjalan di atas sistem *sandbox*, sistem *sandbox* adalah sebuah area yang terisolasi yang tidak memiliki akses pada sistem, kecuali izin akses yang secara eksplisit diberikan oleh pengguna ketika memasang aplikasi. Sebelum memasang aplikasi, Play Store akan menampilkan semua izin yang diperlukan, misalnya : sebuah aplasi perlu mengaktifkan camera atau menyimpan data pada memori internal atau *sd card* tapi tidak memerlukan izin untuk membaca sms atau mengakses *phone book*. Setelah meninjau ijin yang diperlukan, pengguna dapat memilik untuk menerima atau menolaknya, dan bisa memasang aplikasi hanya jika mereka menerimanya.

Sistem sandbox dan perizinan pada Android bisa mengurangi dampak kerentanan terhadap bug pada aplikasi, namun ketidaktahuan pengembang dan terbatasnya dokumentasi telah menghasilkan aplikasi yang secara rutin meminta izin yang tidak perlu, sehingga mengurangi efektivitasnya. Beberapa perusahaan keamanan perangkat lunak seperti Avast, Lookout Mobile Security, AVG Technologies dan McAfee, telah merilis perangkat lunak antivirus ciptaan mereka untuk perangkat Android. Perangkat lunak ini sebenarnya tidak bekerja secara efektif karena sandbox juga bekerja pada aplikasi tersebut, sehingga membatasi kemampuannya untuk memindai sistem secara lebih mendalam.

Hasil penelitian perusahaan keamanan Trend Micro menunjukkan bahwa penyalahgunaan layanan premium adalah tipe perangkat perusak (malware) paling umum yang menyerang Android; pesan teks akan dikirim dari ponsel yang telah terinfeksi ke nomor telepon premium tanpa persetujuan atau sepengetahuan pengguna. Perangkat perusak lainnya akan menampilkan iklan yang tidak diinginkan pada perangkat, atau mengirim informasi pribadi pada pihak ketiga yang tak berwenang. Ancaman keamanan pada Android dilaporkan tumbuh secara bertahap, namun teknisi di Google menyatakan bahwa perangkat perusak dan ancaman virus pada Android hanya dibesar-besarkan oleh perusahaan antivirus untuk alasan komersial dan menuduh industri antivirus memanfaatkan situasi tersebut untuk menjual produknya kepada pengguna. Google menegaskan bahwa keberadaan perangkat perusak berbahaya pada Android sebenarnya sangat jarang dan survei yang dilakukan oleh F-Secure menunjukkan bahwa hanya 0,5% dari perangkat perusak Android yang berasal dari Google Play.

Google baru-baru ini menggunakan pemindai perangkat perusak atau yang lebih dikenal dengan sebutan Google Bouncer untuk mengawasi dan memindai aplikasi di Google Play. Tindakan ini bertujuan untuk menandai aplikasi yang mencurigakan dan memperingatkan pengguna atas potensi masalah pada aplikasi sebelum mereka mengunduh aplikasi tersebut dari Google Play. Android versi 4.2 Jelly Bean dirilis pada tahun 2012 dengan peningkatan yang cukup baik pada fitur keamanannya, termasuk pemindai perangkat perusak yang disertakan dalam sistem; pemindai ini tidak hanya memeriksa aplikasi yang dipasang dari Google Play, namun juga bisa memindai aplikasi yang diunduh dari situs-situs pihak ketiga. Sistem akan memberikan peringatan

yang memberitahukan pengguna ketika aplikasi mencoba mengirim pesan teks premium, dan memblokir pesan tersebut, kecuali jika pengguna mengizinkannya.

Telepon pintar Android memiliki kemampuan untuk melaporkan lokasi titik akses Wi-Fi, terutama jika pengguna sedang bepergian, untuk menciptakan basis data yang berisi lokasi fisik dari ratusan juta titik akses tersebut. Basis data ini membentuk peta elektronik yang bisa memosisikan lokasi telepon pintar. Hal ini memungkinkan pengguna untuk menjalankan aplikasi seperti Foursquare, Google Latitude, Facebook Places, dan untuk mengirimkan iklan berbasis lokasi.Beberapa perangkat lunak pemantau pihak ketiga juga bisa mendeteksi saat informasi pribadi dikirim dari aplikasi ke server jarak jauh. Sifat dari sistem operasi Android yaitu *open source* memungkinkan perusahaan keamanan untuk menyesuaikan perangkat dengan penggunaan yang sangat aman. Misalnya, Samsung bekerja sama dengan General Dynamics melalui proyek "Knox" Open Kernel Labs.

Pada September 2013, terungkap bahwa badan intelijen Amerika Serikat dan Britania; NSA dan Government Communications Headquarters (GCHQ), memiliki akses terhadap data pengguna pada perangkat iPhone, Blackberry, dan Android. Mereka bisa membaca hampir keseluruhan informasi pada telepon pintar, termasuk SMS, lokasi, surel, dan catatan.

B. Bug “Stagefright”

Bug “Stagefright” pertama kali ditemukan oleh Joshua Drake dari perusahaan Zimperium Security, bug ini secara resmi pertama kali diperkenalkan pada 27 Juli 2015 silam. Sebelum mengumumkan bug ini secara resmi Drake terlebih dahulu melaporkan bug ini pada google sekitar bulan April 2015, yang kemudian di tanggapi dengan dirilisnya *patch* untuk menutupi bug ini 2 hari setelah menerima laporan tersebut. Pada bulan Juli 2015 Evegeny Legerov seorang peneliti keamanan yang berbasis di Moscow mengumumkan bahwa dia menemukan 2 jenis serangan yang sejenis dengan yang dilaporkan Drage yang sama – sama memanfaatkan *heap overflow zero-day vulnerabilities* pada librari stagefright. Legerov juga menambahkan bahwa 2 bug yang ia temukan tersebut sudah tidak lagi dapat di exploit setelah melakukan *patch* yang Drake berikan pada Google.

a. Mengenali bug “stagefright”

“Stagefright” adalah sebuah nama yang diberikan pada sekumpulan bug yang ada pada sistem operasi android dengan memanfaatkan celah pada librari stagefright. Bug – bug ini mengancam hampir keseluruhan dari seri sistem operasi android, hal ini dikarenakan bug ini mengancam sistem operasi android dari mulai seri 2.2 atau yang lebih dikenal dengan froyo hingga sistem operasi terbaru yang dirilis oleh google yaitu seri 6.0 atau yang biasa disebut Android M (Marshmalow).

Joshua Drake, peneliti dari Zimperium Labs yang berhasil menemukan beberapa bug pada sistem operasi android dan melaporkannya pada google. Bug yang memungkinkan serangan hanya dengan mengirimkan 1 buah MMS untuk melakukan *hacking* terhadap hampir 950 juta *smartphone*, mungkin saja bisa menjadi lebih kaya dari kondisinya saat ini. Jika ia menjualnya pada pemerintah atau pada “pedagang” *exploit* dia bisa mendapatkan $100.000 atau setara dengan sekitar 133 milyar rupiah

bahkan lebih. Salah satu dari “pedagang” *exploit* yaitu Zerodium menyatakan berani menawarkan harga sampai $100.000 untuk nya agar memberikan bug tersebut kepada mereka.

Gambar 1 Penawaran Zerodium untuk bug Stagefright

Tapi sayangnya Drake ternyata menjadi salah seorang yang masih memegang teguh prinsip bahwa bug yang ia temukan haruslah di berikan pada pengembangnya, sehingga ia kemudian memberikan bugs dan patch pada google yang hanya membayarnya dengan $1.337 saja.

b. CVE “stagefright”

CVE atau *Common Vulnerabilities and Exposures* adalah sebuah *Standard for Information Security Vulnerabilites Names* yang dikelola oleh MITRE. Bug – bug stagefright pun mendapatkan nomor khusus pada CVE diantaranya adalah :

1. CVE-2015-1538
   Serangan ini memanfaatkan integer overflow pada fungsi SampleTabe::setSampleToChunkParams di SampleTable.cpp yang ada pada library stagefright.
2. CVE-2015-1539
   Serangan ini memanfaatkan integer overflow pada ESDS::parseESDescriptor yang ada pada ESDS.cpp pada library stagefright.
3. CVE-2015-3824
   Serangan ini memanfaatkan fungsi MPEG4Extractor::parseChunk pada MPEG4Extractor.cpp yang bisa ditemukan pada library stagefright.
4. CVE-2015-3826
   Serangan ini memanfaatkan funsi dari MPEG4Extractor::parse3GPPMetaData pada MPEG4Extractor.cpp yang bisa ditemukan pada librari stagefright. Serangan ini mengakibatkan *denial of service* menggunakan metode *integer uderflow, buffer over-read,* dan *mediaserver process crash*.
5. CVE-2015-3827
   Serangan ini memanfaatkan fungsi MPEG4Extractor::parseChunk pada MPEG4Extractor.cpp yang bisa ditemukan pada librari stagefright. Serangan ini mengakibatkan *denial of service* menggunakan metode *integer underflow* dan *memory corruption.*

6. CVE-2015-3828
   Serangan ini memanfaatkan fungsi MPEG4Extractor::parse3GPPMetaData pada MPEG4Extractor.cpp yang bisa ditemukan pada librari stagefright. Serangan ini mengakibatkan *denial of servie* menggunakan metode *integer underflow* dan *memory corruption.*
7. CVE-2015-3829
   Serangan ini memanfaatkan *one-by-one error* yang ada pada fungsi MPEG4Extractor::parseChunk pada MPEG4Extractor.cpp yang bisa ditemukan pada librari stagefright. Serangan ini mengakibatkan *denial of service* menggunakan metode *integer underflow* dan *memory corruption.*
8. CVE-2015-3864
   Serangan ini memanfaatkan *integer underflow* yang ada pada fungsi MPEG4Extractor::parseChunk pada MPEG4Extractor.cpp yang bisa ditemukan pada librari stagefright.
9. CVE-2015-3876
   Serangan ini memanfaatkan librari stagefright yang memperbolehkan penyerang mengeksekusi *arbitary code*.
10. CVE-2015-6602
    Serangan ini memanfaatkan *libutils* yang memperbolehkan penyerang mengeksekusi *arbitary code*.
11. CVE-2015-6575-1
12. CVE-2015-6575-2
13. CVE-2015-6575-3
14. CVE-2016-0828
15. CVE-2016-0829

c. Bahaya “stagefright”

Dari banyaknya nomor CVE diatas sebenarnya cukup menunjukkan dampak besar yang ditimbulkan dari bug pada library stagefright ini. Bug stagefright ini pun banyak dibicarakan sebagai bug terbesar sepanjang sejarang sistem operasi android. Hal ini dikarenakan tidak seperti metode serangan lainnya yang membutuhkan interaksi dari user, bug “stagefright” sama sekali tidak membutuhkan hal terebut. Sebagai contoh serangan *spear phising* yang dikirmkan ke *smartphone* membutuhkan interaksi user untuk mendownload *attachment* yang disediakan penyerang. Hal ini sangat berbeda dengan serangan yang memanfaatkan bug stagefright, karena hal tersebut sama sekali tidak dibutuhkan, misalnya salah satu bug stagefright yang memanfaatkan media MMS dengan cara mengirimkan video yang sudah dimanipulasi terlebih dahulu struktur data dan codenya maka ketika mms tersebut diterima oleh *smartphone* target maka saat itu pula penyerang mendapatkan akses ke *smartphone* target. Hal ini dikarenakan secara *default* beberapa aplikasi pesan menlakukan download *content* secara otomatis dengan tujuan saat user ingin membukanya *content* sudah dalam keadaan siap. Kemungkinan terburuknya adalah serangan tersebut dilakukan pada malam hari saat target sedang beristirahat, setelah mendapatkan akses ke *smartphone* target maka penyerang hanya butuh menghapus bukti atau notifikasi dari *smartphone* target terebut. Maka secara otomatis target tidak merasa curiga sama sekali bahkan menggunakan *smartphone* yang sudah terjangkit virus tersebut dengan normal seperti biasanya.

d. Pendeteksi bug stagefright

Beberapa aplikasi pada google play store sebenarnya menawarkan fasilitas untuk melakukan pengecekan terhadap *smartphone* apakah bug – bug stagefright masih dapat dimanfaatkan (di *exploit*) atau tidak. Dari banyaknya aplikasi tersebut ada 2 aplikasi yang terlihat cukup menjanjikan untuk dapat melakukan pengecekan tersebut. 2 aplikasi tersebut adalah Lookout Mobile Stagefright Detector dan Zimperium Stagefright Detector.

e. Celah keamanan stagefright varian baru

Tahun 2016 ini kembali ditemukan varian baru dari celah keamanan stagefright yang pada tahun 2015 silam sudah banyak update dikerluarkan hanya untuk menambal celah – celah yang ada pada library tersebut. Hampir setiap bulan google mengeluarkan update untuk sistem operasi nya yang kemudian di susul oleh produsen – produsen *smartphone* yang menggunakan sistem operasi besutan google tersebut. Ketika sebuah update sudah dirilis, hanya sebagian kecil saja yang benar – benar melakukan update pada sistem operasinya. Google sendiri berencana untuk mencoba memperbaiki secara keseluruhan bug pada stagefright pada android seri N, tapi tentu saja hal itu membutuhkan waktu yang tidak sebentar bahkan bisa memakan waktu hingga bertahun – tahun sampai seluruh pengguna android menggunakan sistem operasi Android N+. Hal ini diperparah dengan banyaknya produsen *smartphone*, membuat update dengan begitu banyak produsen bukan lah sebuah proses yang mudah.

Satu hal yang mungkin saja terjadi adalah penyebaran worm dari satu *smartphone* ke *smartphone* lain menggunakan metode *social engineering*. Seperti worm yang akan menjangkit *smartphone* dengan cara mengirimkan link menggunakan

SMS, MMS, Instant Messages atau email. Jika user membuka file atau link yang diberikan maka *smartphone* yang digunakan akan langsung terkena serangan dengan menggunakan celah keamanan stagefright ini. Namun sebenarnya ada 2 metode serangan lain yang cukup berbahaya yang masih mungkin terjadi dan sama – sama tidak membutuhkan interaksi dengan usernya.

Kemungkinan pertama dari serangan ini adalah dengan menggunakan metode *watering hole attack*. Dengan cara ini penyerang mencoba menebak website yang paling sering di akses oleh sebuah grup atau instansi. Kemudian menginfeksi salah satu dari website tersebut dengan malware. Maka secara tidak langsung target akan mengunjungi website yang sudah disusupi malware tadi dan penyerang mendapatkan *smartphone* target.

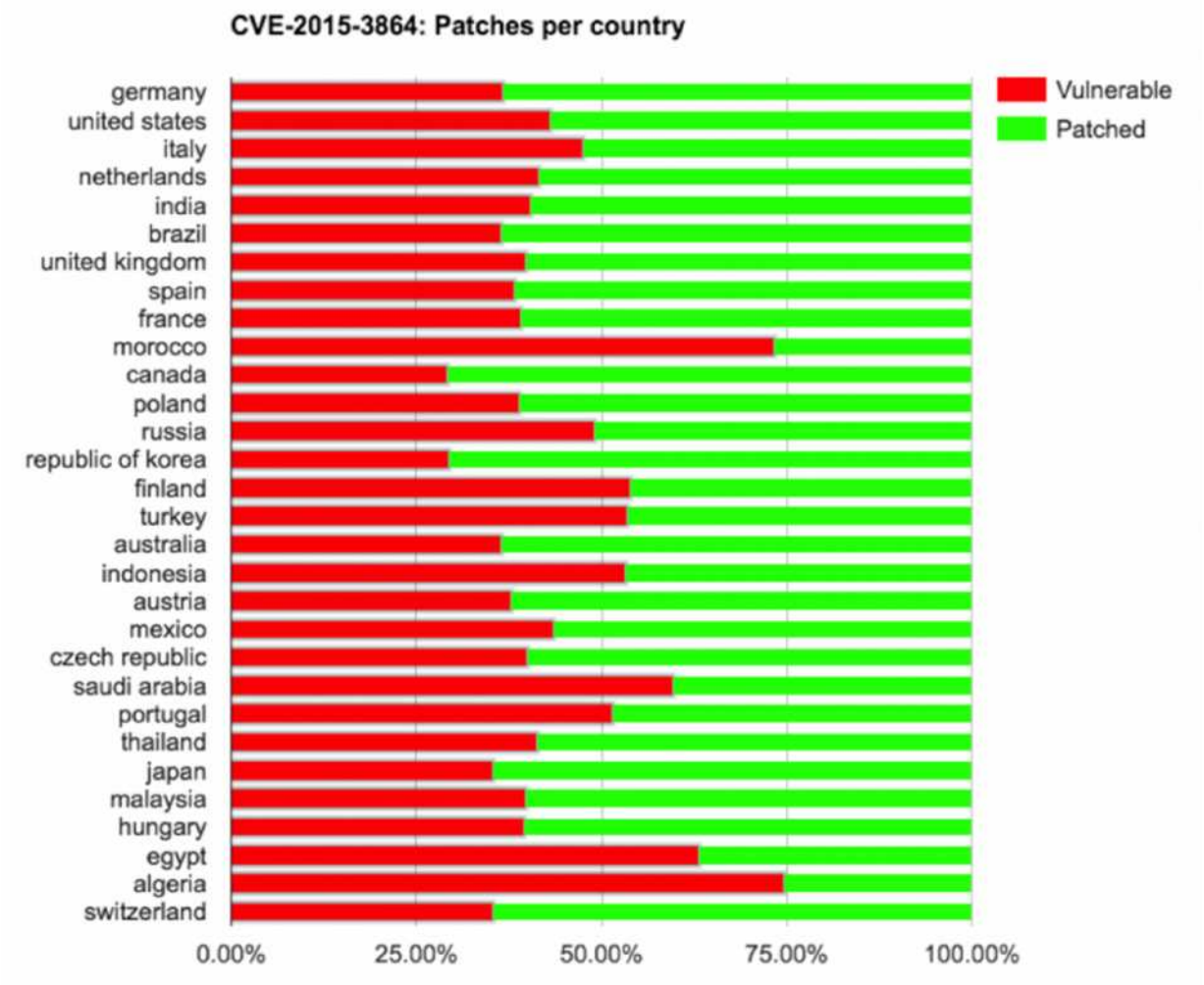
Kemungkinan kedua dari serangan ini adalah dengan menggunakan metode MITM (*Man in the Middle).* Serangan ini bisa dilakukan menggunakan media Wi-Fi *access point,* dengan membuat *rogue base station* atau dengan menggunakan bagian dari sistem yang memang sudah berhasil diserang.

C. Pencegahan

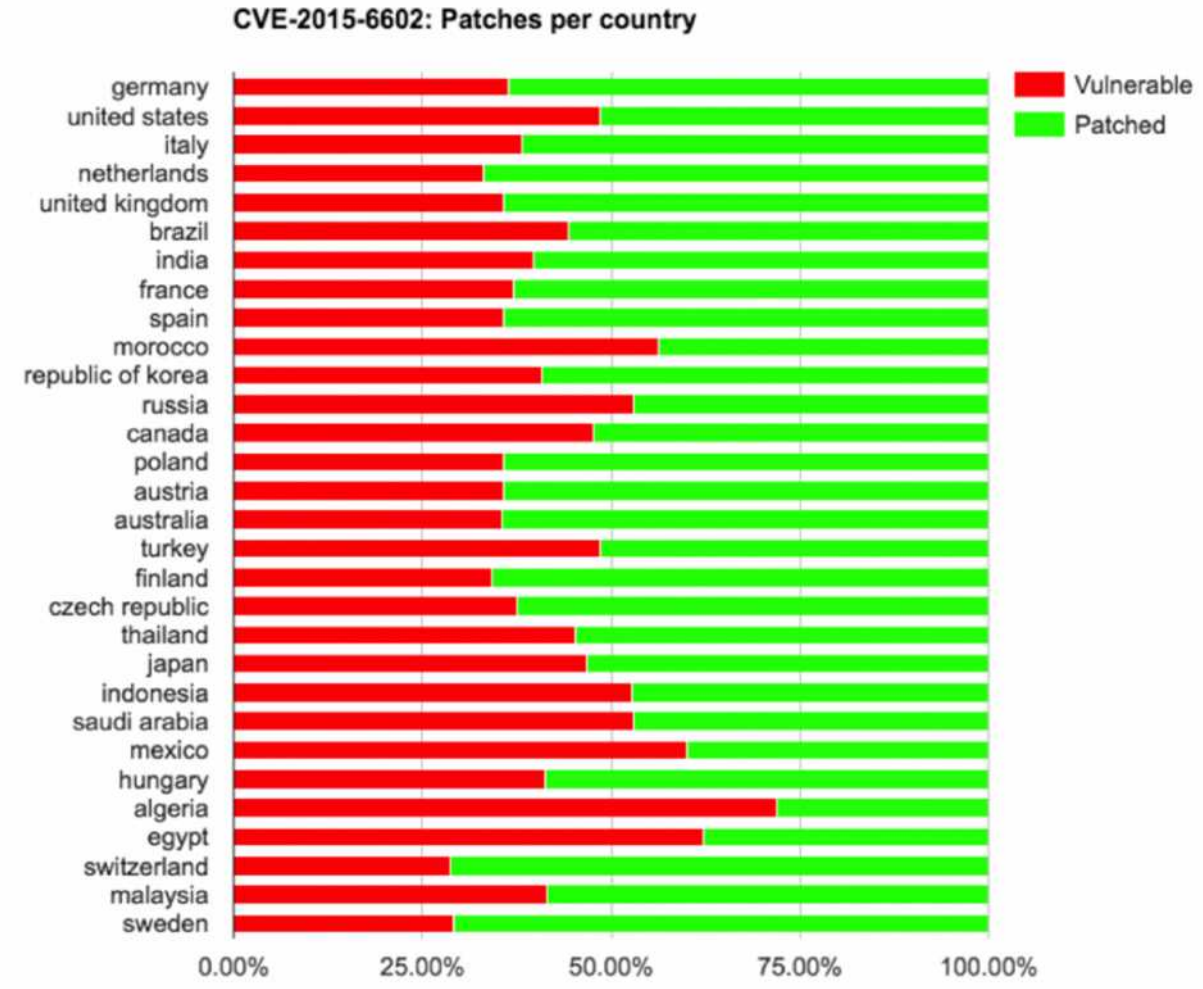
Cara yang paling baik untuk mencegah serangan ini agar tidak berhasil melakukan serangannya terhadap *smartphone* adalah dengan cara menonaktifkan *auto download* pesan – pesan MMS, hal ini guna meminimalisir kemungkinan serangan yang dilakukan penyerang dengan memanfaatkan bug pada *MediaServer* pada *smartphone*. Hal ini tentu saja menjadi tidak berlaku apabila penyerang menyembunyikan “media” yang digunakan untuk masuk ke *smartphone* target pada cara – cara yang lain seperti melalui *bluetooth*, website, maupun cara – cara yang lainnya. Saran lainnya untuk mencegah serangan ini adalah jangan pernah membuka website – website yang memiliki nama yang aneh atau membuka website yang dipandang memiliki *content* yang seperti menggiring pembacanya untuk membuka website tersebut. Untuk media *bluetooth* jangan pernah membiarkan perangkat *bluetooth* pada *smartphone* dibiarkan selalu menyala atau jangan sembarangan menerima file *trasfer* dari perangkat yang tidak benar – benar dikenal.

D. Penanganan

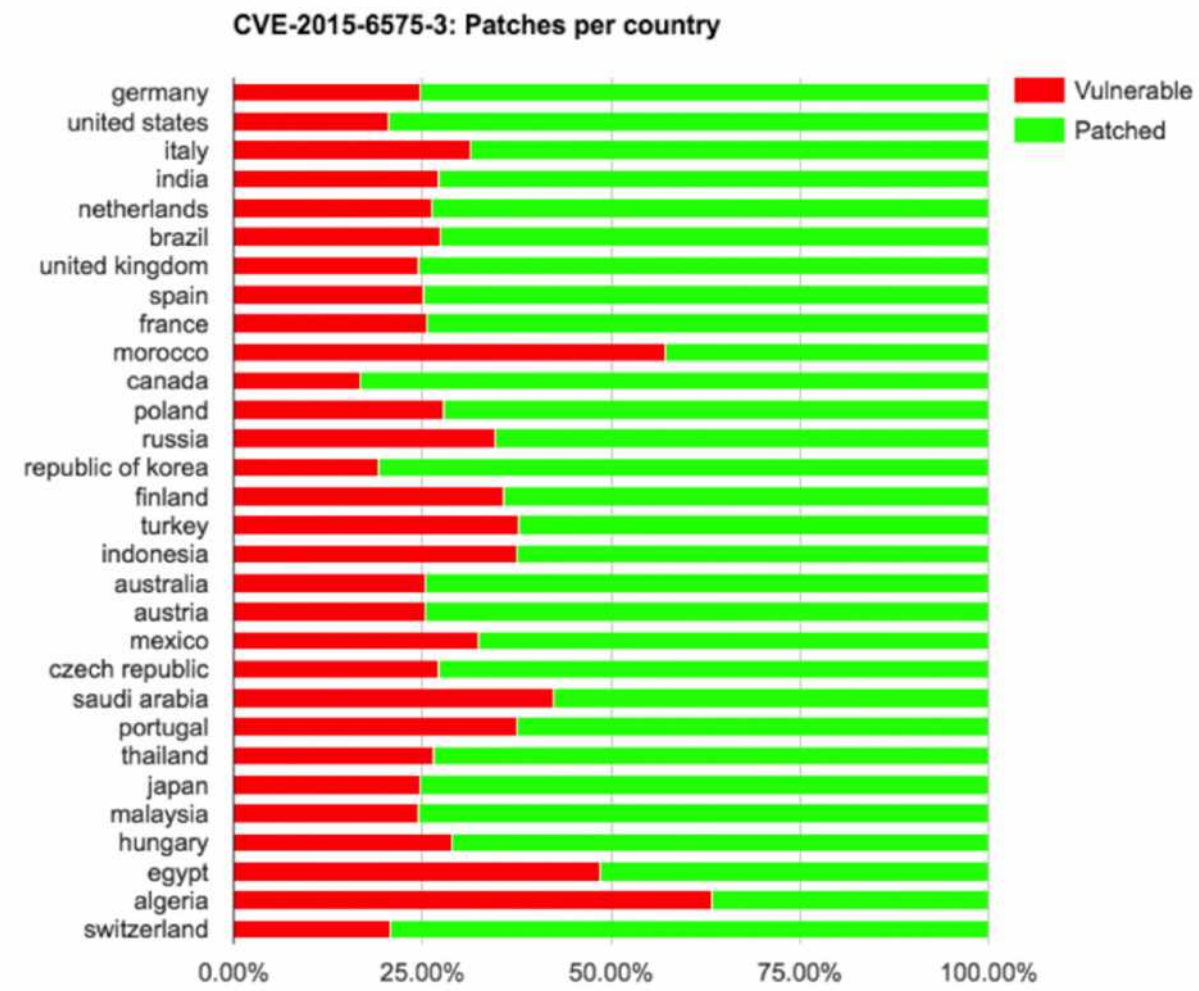
Sebagai penanganan dari seragan pada celah keamanan stagefright ini sebenarnya google sendiri sudah mengeluarkan beberapa patch untuk menutup setiap celah yang ditimbulkan. Namun, walaupun google dan beberapa produsen besar sudah mengeluarkan patch yang cukup banyak untuk menutupi semua celah keamanan tersebut, keputusan terakhir tentu saja kembali pada pengguna dari *smartphone* tersebut. Apakah pengguna selalu melakukan update terhadap sistem operasi android yang mereka miliki atau justru bersifat acuh terhadap update yang diberikan oleh google dan produsen *smartphone.* Dibawah ini beberapa gambar statistik dari beberapa CVE yang terkait dengan stagefright dan berapa presentase pengguna yang melakukan update dan yang tidak melakukan update pada beberapa negara besar di dunia.



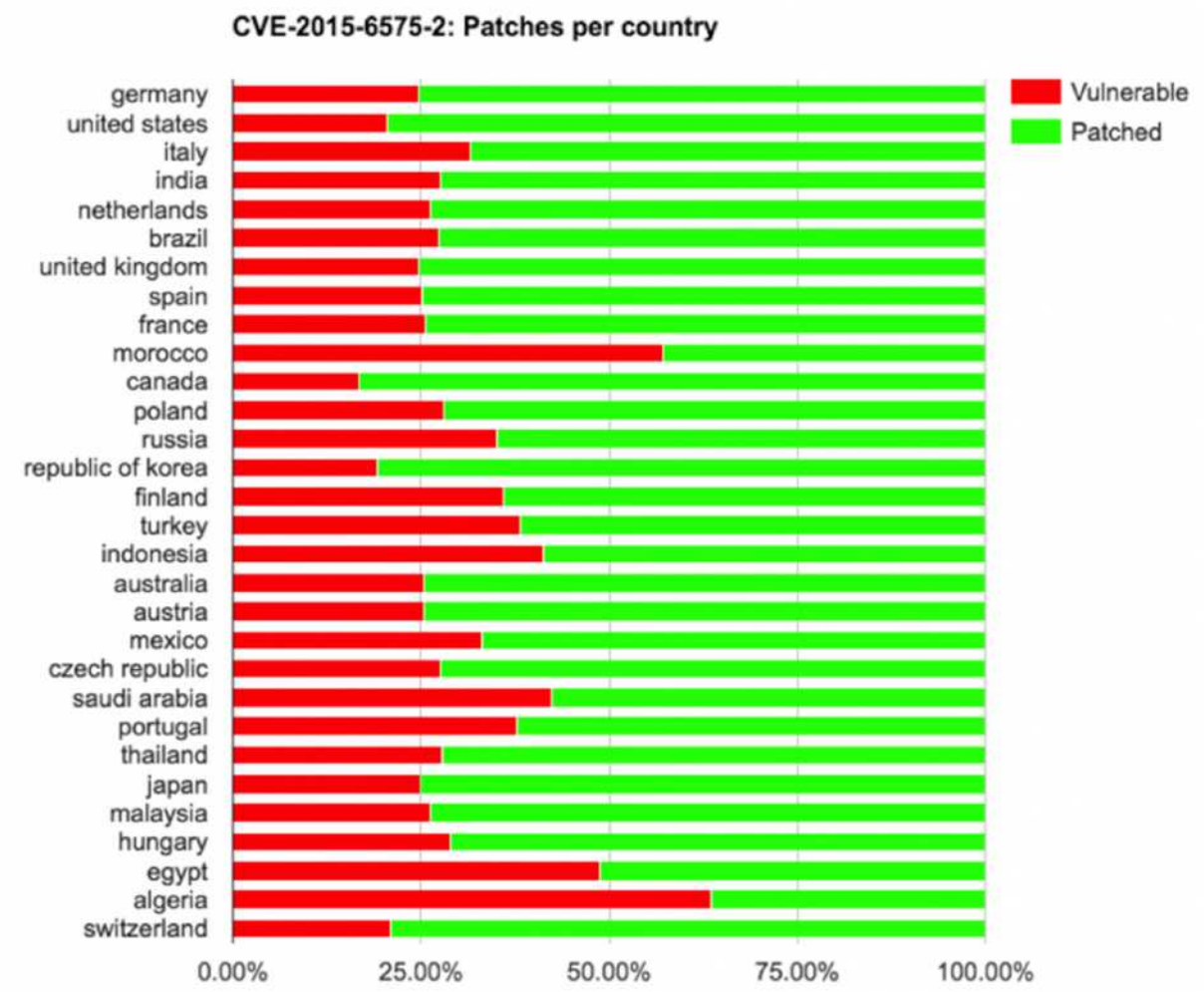
Gambar 2 Penggunaan patch CVE-2015-3864



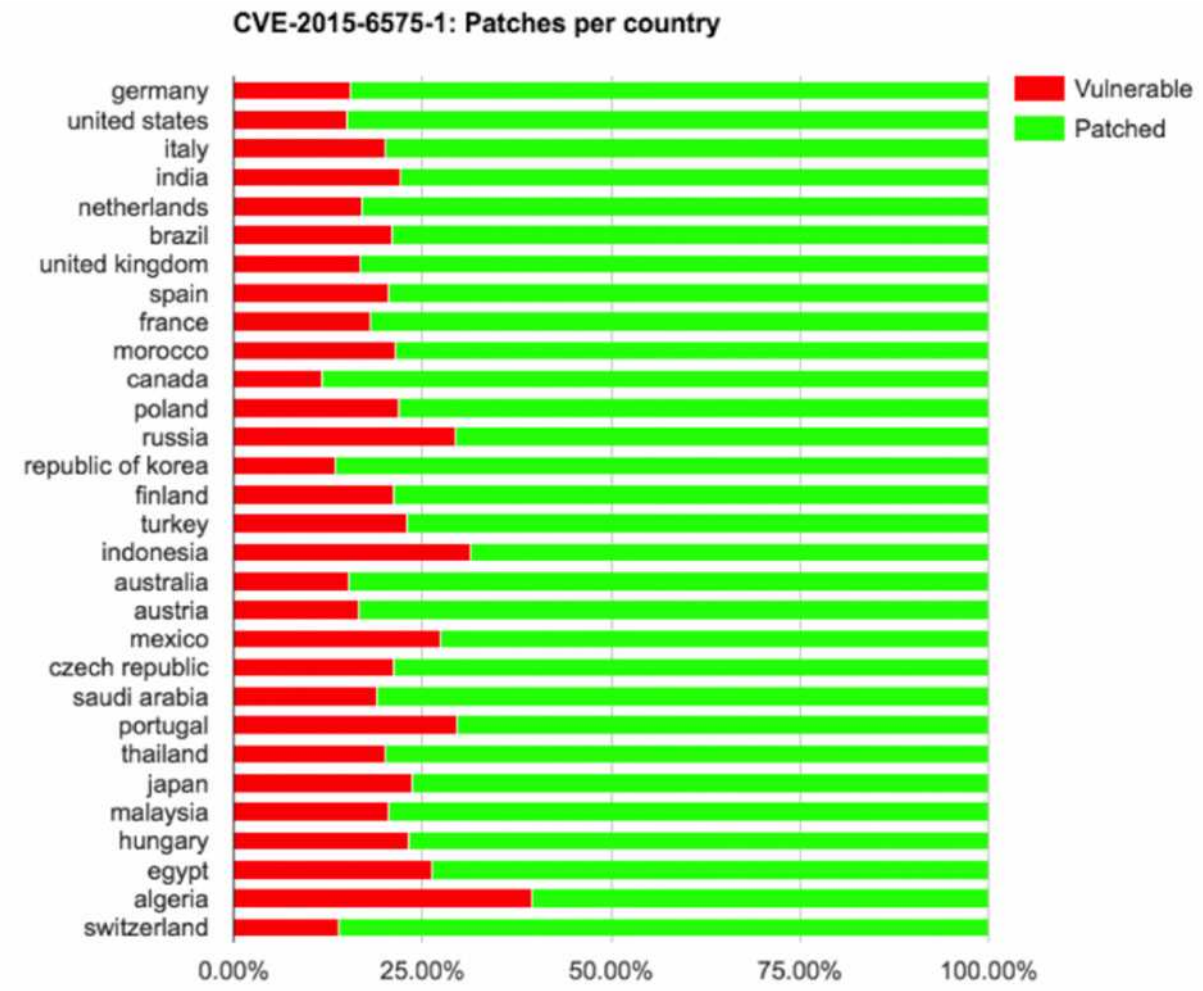
Gambar 3 Penggunaan patch CVE-2015-6602



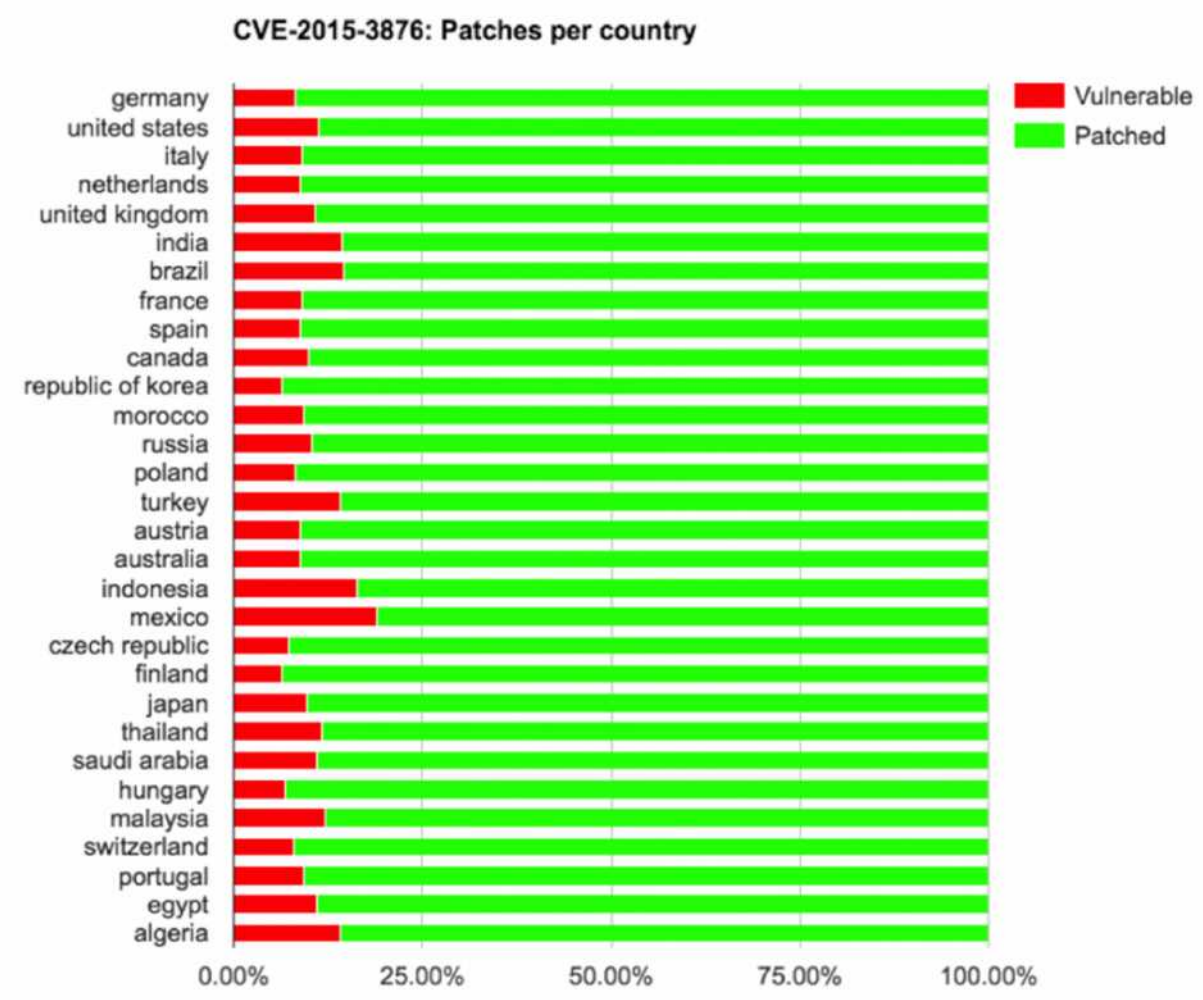
Gambar 4 Penggunaan patch CVE-2015-6575-3



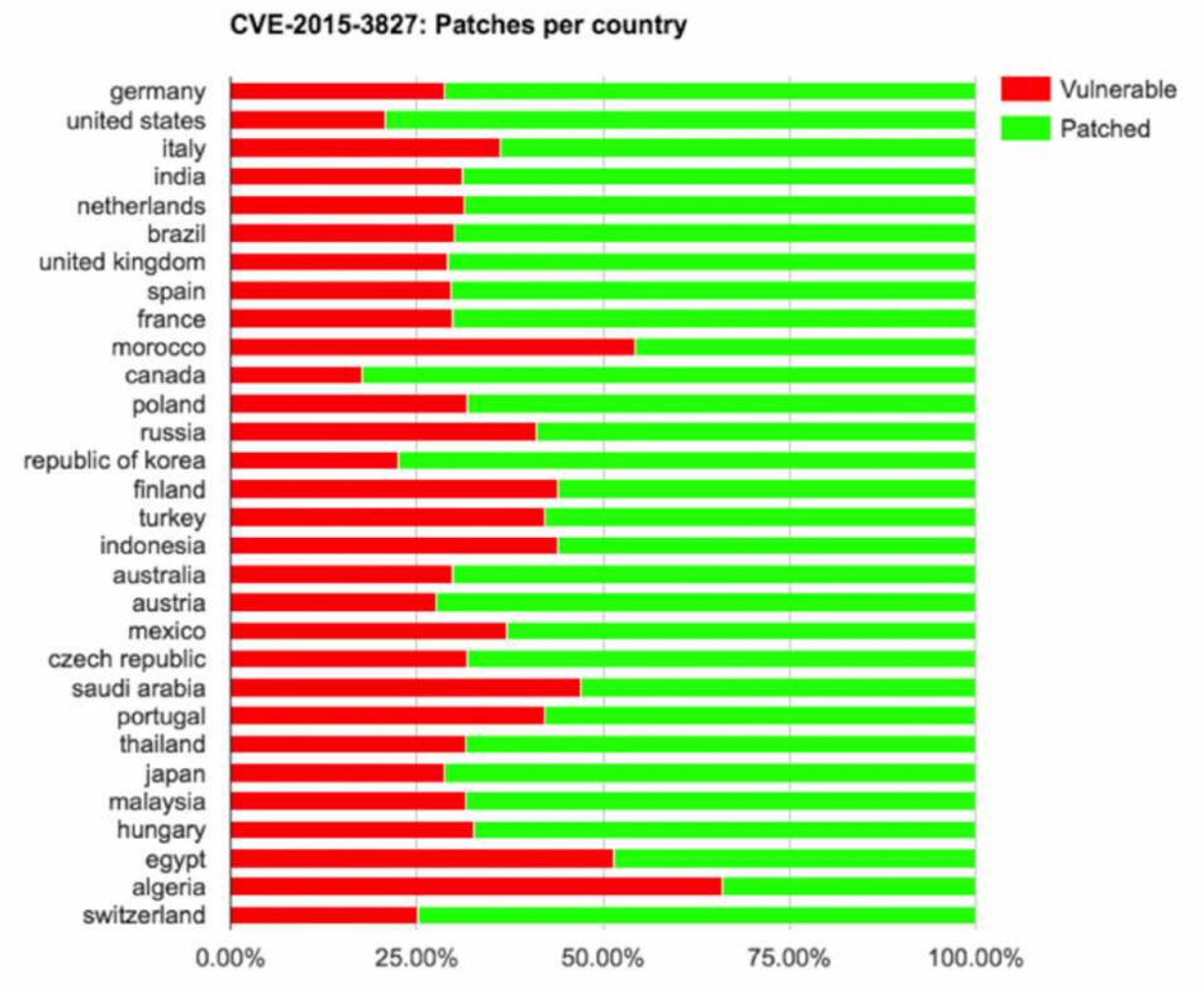
Gambar 5 Penggunaan patch CVE-2015-6575-2



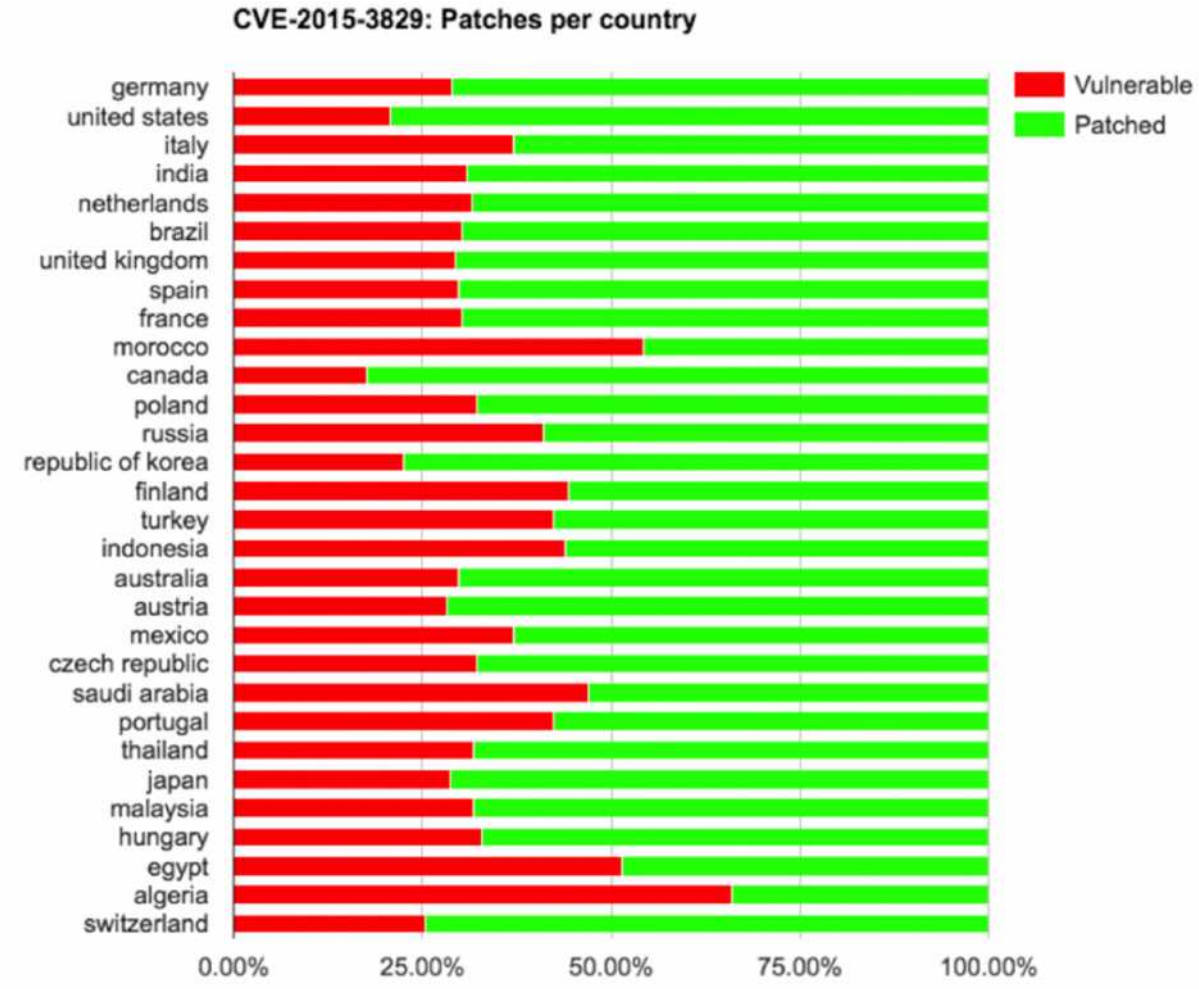
Gambar 6 Penggunaan patch CVE-2015-6575-1



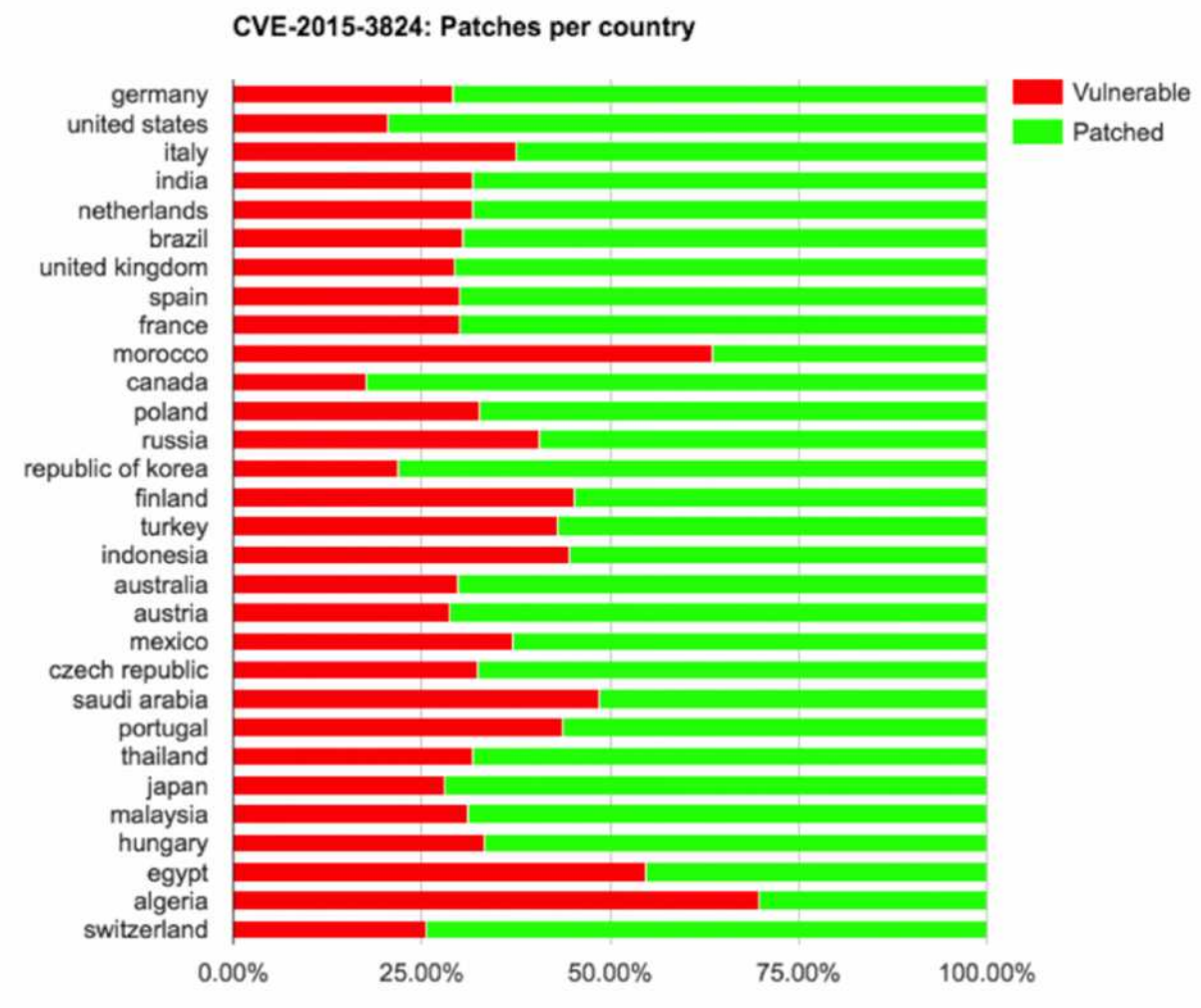
Gambar 7 Penggunaan patch CVE-2015-3876



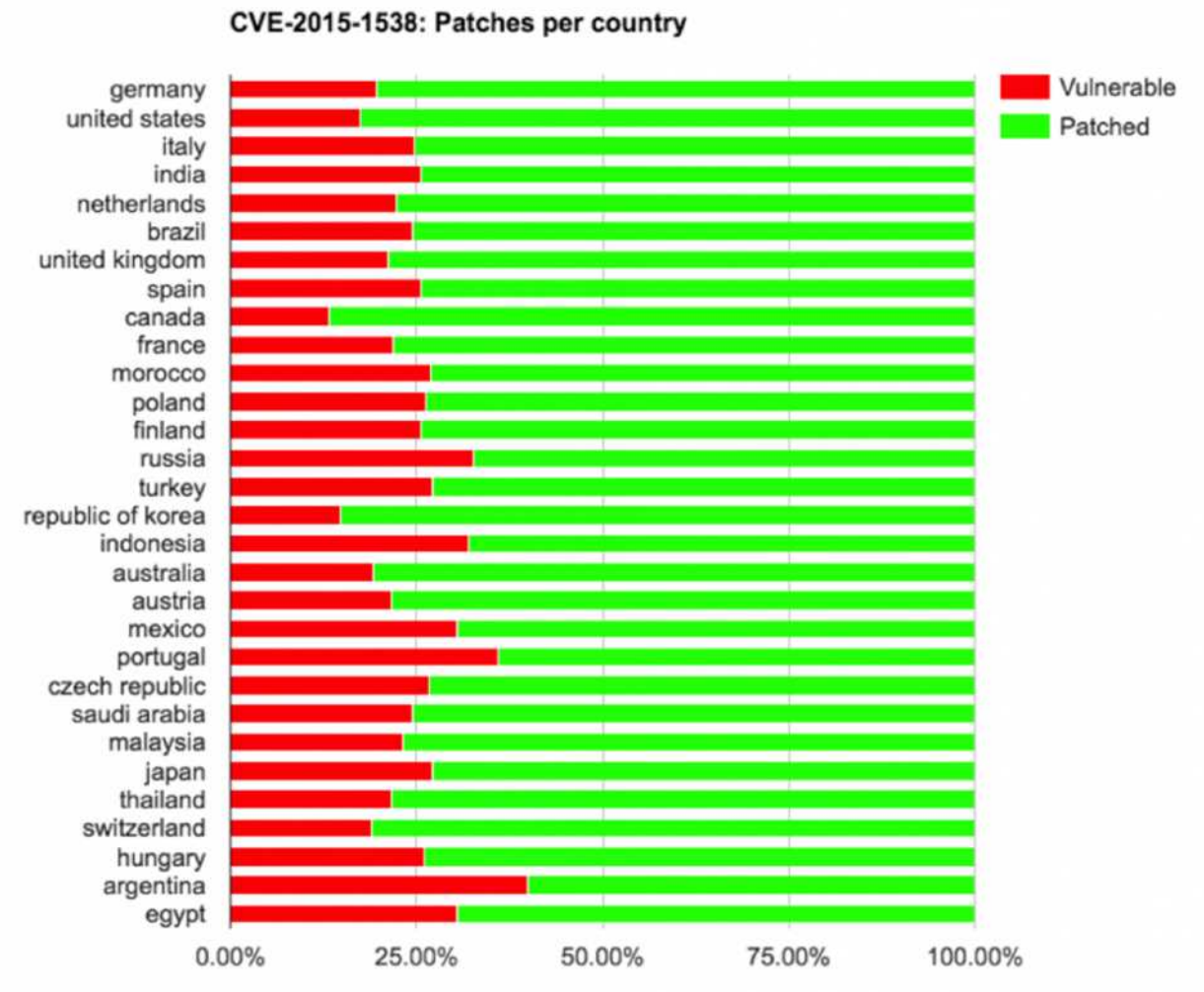
Gambar 8 Penggunaan patch CVE-2015-3827



Gambar 9 Penggunaan patch CVE-2015-3829



Gambar 10 Penggunaan patch CVE-2015-3824



Gambar 11 Penggunaan patch CVE-2015-1538

Bisa sedikit terlihat gambaran jelas dari banyaknya patch yang dikeluarkan baik itu oleh google maupun produsen – produsen *smartphone*. Pilihan terakhir terletak pada penggunanya sendiri, beberapa pengguna atau mungkin mayoritas dari pengguna sistem operasi android sendiri merasa acuh terhadap update sistem operasi yang diberikan. Hal ini bisa didasari oleh beberapa hal, salah satunya adalah cukup mahalnya harga yang harus di bayar oleh pengguna untuk mendapatkan akses internet yang cukup baik atau penyebaran akses internet yang masih tidak merata pada negara – negara berkembang terutama kita bisa lihat pada Indonesia. Hal lain yang tentu saja tidak kalah penting adalah kesadaran pengguna *smartphone* itu sendiri yang terkadang merasa tidak perlu atau bahkan sebenarnya tidak faham mengenai keamanan informasi yang seharusnya menjadi tanggung jawab bukan hanya produsen maupun pengembang sistem operasi android tapi juga penggunanya itu sendiri. Karena sekali lagi sebaik apapun sebuah sistem atau hardware jika penggunananya tidak memiliki *awarness* yang cukup baik mengenai keamanan informasi maka sudah bisa dipastikan *software* maupun *hardware* tersebut tetap saja dapat diserang oleh orang – orang yang tidak bertanggung jawab.

E. Kesimpulan dan Saran

1. Kesimpulan

Beberapa kesimpulan yang dapat diambil dari makalah ini antara lain adalah dalam proses pertukaran informasi di era yang canggih saat ini paling tidak ada 3 aspek penting yang berperan cukup besar yaitu *software* atau perangkat lunak dapat berupa sistem operasi maupun aplikasi,

hardware atau perangkat keras dapat berupa *handphone, smartphone, tablet* dan lain – lain. Dan yang terakhir adalah *brainware* atau yang biasa dikenal dengan pengguna. Ketika para pengguna menginginkan atau bahkan membutuhkan “keamanan” maka hal ini tentu saja tidak bisa dilakukan hanya oleh 2 atau bahkan salah 1 dari ketiga aspek diatas. Namun, untuk mewujudkan hal itu diperlukan aksi maupun peran serta dari ketiga aspek tersebut agar “keamanan” dapat terwujud.

2. Saran

Saran yang bisa diberikan terkait dengan masalah ini adalah agar pengguna mulai dapat lebih *aware* terhadap keamanan informasi. Baik itu yang terkait hanya untuk informasi dirinya sendiri maupun yang terkait instansi atau bahkan negara. Dengan adanya *awarness* dari pengguna sebenarnya sudah cukup mengurangi kemungkinan pemanfaatan celah keamanan baik itu dari sisi sistem operasi, aplikasi maupun *hardware*nya itu sendiri.

Referensi

1. https://id.wikipedia.org/wiki/Android_(sistem_operasi), diakses pada tanggal 4 Mei 2016.
2. https://id.wikipedia.org/wiki/Daftar_versi_Android, diakses pada tanggal 4 Mei 2016.
3. http://www.openhandsetalliance.com/android_overview.html, diakes pada tanggal 5 Mei 2016.
4. http://www.seputarit.com/sejarah-dan-perkembangan-sistem-operasi-android.html, diakses pada tanggal 5 Mei 2016.
5. http://www.techradar.com/reviews/pc-mac/software/operating-systems/android-5-0-lollipop-1271651/review, diakses pada tanggal 7 Mei 2016.
6. https://en.wikipedia.org/wiki/Android_Marshmallow, diakses pada tanggal 7 Mei 2016.
7. https://en.wikipedia.org/wiki/Stagefright_(bug), diakses pada tanggal 10 Mei 2016.
8. http://www.androidcentral.com/stagefright, diakses pada tanggal 10 Mei 2016.
9. http://www.wired.co.uk/news/archive/2016-03/16/stagefright-android-real-world-hack, diakses pada tanggal 11 Mei 2016.
10. http://www.wired.co.uk/news/archive/2015-07/27/stagefight-android-bug, diakses pada tanggal 11 Mei 2016.
11. http://www.infoworld.com/article/3045383/security/new-exploit-spotlights-androids-stagefright-vulnerability.html, diakses pada tanggal 12 Mei 2016.
12. https://blog.zimperium.com/zimperium-zlabs-is-raising-the-volume-new-vulnerability-processing-mp3mp4-media/, diakses pada tanggal 13 Mei 2016.
13. https://blog.zimperium.com/reflecting-on-stagefright-patches/, diakses pada tanggal 13 Mei 2016.
14. http://www.realita.co/index.php?news=Mengenal-Bugs-Mematikan-Android-Stagefright-2.0~3b1ca0a43b79bdfd9f9305b81298296216b28dda2fa71f38117835c30af9076b, diakses pada tanggal 13 Mei 2016.
15. http://www.merdeka.com/teknologi/malware-ini-menginfeksi-1-juta-pengguna-android-di-seluruh-dunia.html, diakses pada tanggal 13 Mei 2016.
16. http://www.forbes.com/sites/thomasbrewster/2015/07/30/stagefright-vulnerabilties-ready-for-testing/#785fd9033ef9, diakses pada tanggal 14 Mei 2016
17. https://blog.exodusintel.com/2015/08/13/stagefright-mission-accomplished/, diakses pada tanggal 14 Mei 2016.
18. https://blog.zimperium.com/reflecting-on-stagefright-patches/, diakses pada tanggal 14 Mei 2016
19. http://www.spiegel.de/international/world/privacy-scandal-nsa-can-spy-on-smart-phone-data-a-920971.html, diakses pada tanggal 14 Mei 2016.