DIAGRAM SITASI PAPER

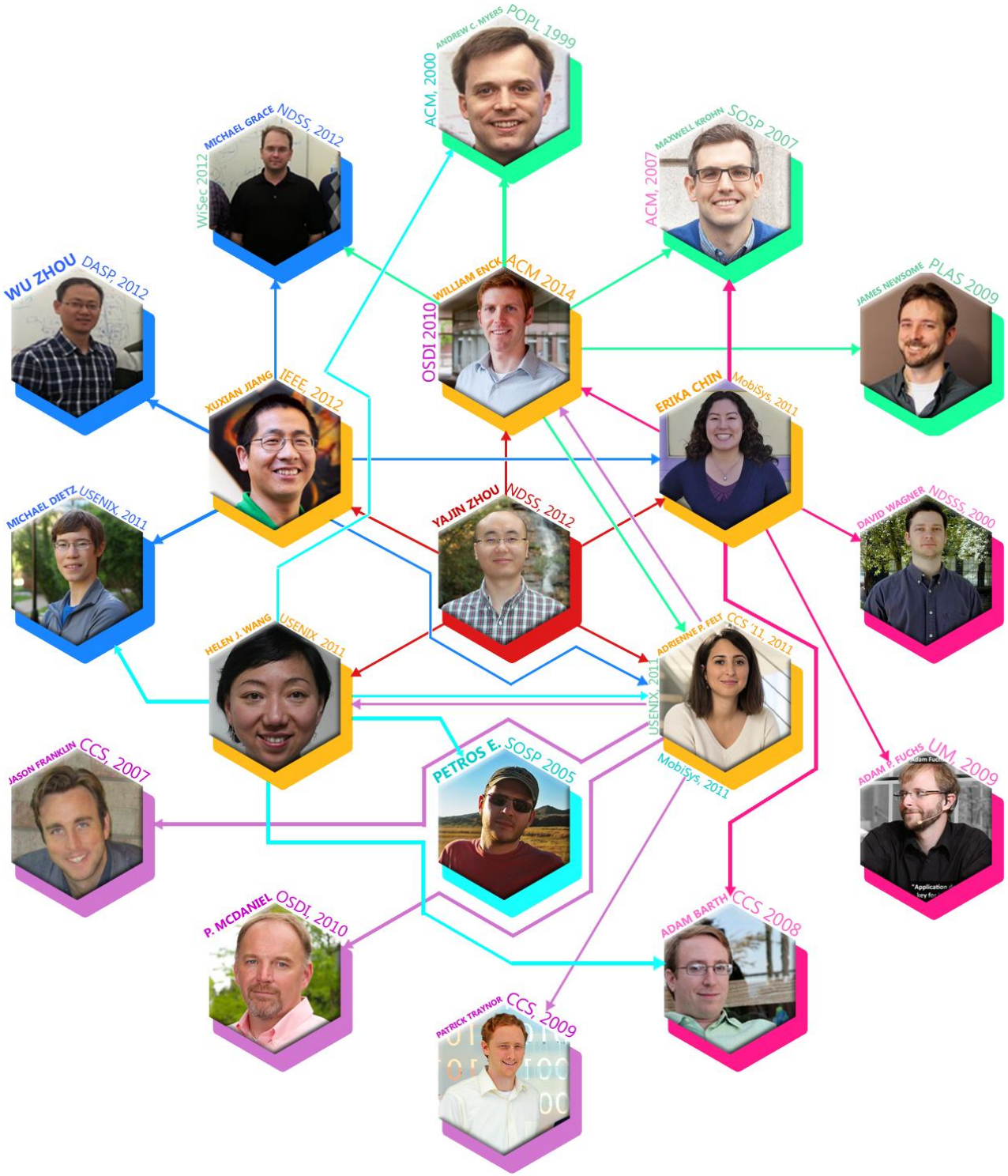
Disusun Oleh :

Tio Artha Nugraha

09011181520027

SK2A

PROGRAM STUDI SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA
2016


ANDREW C. MYERS POPL 1999
ACM, 2000
MICHAEL GRACE NDSS, 2012
WiSec 2012
MAXWELL KROHN SOSP 2007
ACM, 2007
WU ZHOU DASP, 2012
WILLIAM ENCK ACM 2014
OSDI 2010
JAMES NEWSOME PLAS 2009
XUXIAN JIANG IEEE, 2012
ERIKA CHIN MobiSys, 2011
MICHAEL DIETZ USENIX, 2011
YAJIN ZHOU NDSS, 2012
DAVID WAGNER NDSS, 2000
HELEN J. WANG USENIX 2011
ADRIENNE P. FELT CCS '11, 2011
USENIX, 2011
JASON FRANKLIN CCS, 2007
PETROS E. SOSP 2005
MobiSys, 2011
ADAM P. FUCHS UM, 2009
P. MCDANIEL OSDI, 2010
ADAM BARTH CCS 2008
PATRICK TRAYNOR CCS, 2009

Serangan Android Malware;

Mendeteksi Aplikasi Berbahaya pada Market Android Resmi dan Alternatifnya

[1] Dalam paper ini, kami telah menyajikan sebuah studi sistematis untuk mendeteksi aplikasi berbahaya pada Market Android yang bersifat resmi dan alternatifnya. Dalam studi yang kami lakukan, kami sudah mengumpulkan sekitar 204.040 aplikasi Android. Untuk menstabilkan dan mengefisienkan pendeteksian potensi terjadinya infeksi dari malware baik yang dikenal maupun yang tidak dikenal, kami telah sepakat mengusulkan dua skema yang berbeda, yaitu, *permission* yang didasarkan oleh tingkah laku dan satunya penyaringan berdasarkan heuristik. Kami telah menerapkan kedua skema di *Droid Ranger* dan hasil evaluasi berhasil mendeteksi 211 aplikasi berbahaya dan mengungkapkan dua *zero-day malware* di *Android Market* resmi dan tidak resmi (alternatif) dan hal ini menunjukkan kelayakan dan efektivitas hasil kerja kami. Dari perspektif lain, hasil kami juga secara tidak langsung maupun langsung menyerukan perlunya proses pemeriksaan ketat tiap aplikasi yang beredar pada Market Android yang resmi ataupun tidak resmi.

[2] Dalam paper ini, kami menyajikan karakterisasi sistematis malware Android yang ada. Pengkarakterisasian ini dimungkinkan bisa dipercaya atas usaha kami yang lebih dari satu tahun dalam mengumpulkan 1.260 sampel malware Android di 49 klasifikasi yang berbeda, yang meliputi sebagian besar malware Android yang ada, mulai dari debutnya pada bulan Agustus 2010 sampai yang baru-baru ini pada Oktober 2011. Dengan karakteristik sampel malware dari berbagai aspek tersebut, hasil kami menunjukkan bahwa (1) 86,0% adalah *repackage* dari aplikasi yang sudah komplit untuk dimasukkan muatan yang berbahaya; (2) 36,7% mengandung eksploitasi platform bertingkat; (3) 93,0% menunjukkan kemampuan seperti *bot*. Sebuah analisis evolusi lebih lanjut dan mendalam dari perwakilan beberapa malware Android menunjukkan perkembangan pesat dan peningkatan kecanggihan, Sayangnya, 107 evaluasi dengan empat ponsel software anti-virus yang ada menunjukkan bahwa kasus terbaik mendeteksi 79,6% dari mereka, sementara kasus terburuk mendeteksi hanya 20,2%. Hasil ini adalah panggilan untuk lebih mengembangkan generasi solusi anti-mobile-malware.

[3] Sementara beberapa sistem operasi ponsel memungkinkan pengguna untuk mengontrol akses aplikasi ke informasi yang lebih sensitif, seperti sensor lokasi, gambar kamera, dan daftar kontak, pengguna kurang jelas tentang bagaimana aplikasi tersebut menggunakan data pribadi mereka. Untuk mengatasi hal ini, kami menyajikan TaintDroid, sebuah arus informasi alat pelacakan yang efisien di seluruh sistem yang secara bersamaan dapat melacak berbagai sumber data yang bersifat sensitif. Tujuan desain kunci utama dari TaintDroid adalah efisiensi, dan TaintDroid mencapai hal tersebut dengan mengintegrasikan empat *granularities propagasi noda* (variabel-tingkat, message level, metode-tingkat, dan file-level) untuk mencapai overhead kinerja 14% pada *microbenchmark* CPU-terikat. Kami juga menggunakan implementasi TaintDroid kami untuk mempelajari perilaku dari 30 aplikasi pihak ketiga yang populer, yang dipilih secara acak dari Android Marketplace. Studi kami

menunjukkan bahwa dua pertiga dari aplikasi dalam penelitian kami menunjukkan penanganan yang mencurigakan dari data sensitif, dan bahwa 15 dari 30 aplikasi melaporkan lokasi pengguna ke server iklan terpencil. Temuan kami menunjukkan efektivitas dan nilai meningkatkan platform smartphone dengan alat monitor seperti TaintDroid.

[4] Kami telah menyajikan TaintDroid, yaitu sebuah informasi-aliran alat pelacakan efisien seluruh sistem yang secara bersamaan dapat melacak berbagai sumber data sensitif. TaintDroid mencapai efisiensi, kinerja biaya overhead 32% pada microbenchmark CPU-terikat, dengan mengintegrasikan empat granularities propagasi noda (variabel-tingkat, pesan-tingkat, metode-tingkat, dan file-level). Kami menggunakan implementasi TaintDroid kami untuk mempelajari perilaku dari 30 aplikasi *thirdparty* populer. Studi kami 2010 mengungkapkan bahwa dua pertiga dari aplikasi dalam penelitian kami menunjukkan penanganan yang mencurigakan dari data sensitif, dan bahwa 15 dari 30 aplikasi melaporkan lokasi pengguna ke server iklan terpencil. Sebuah fraksi yang sama dari aplikasi yang diuji dalam penelitian kami 2012 juga berpotensi disalahgunakan data sensitif pengguna. Temuan kami menunjukkan efektivitas dan nilai meningkatkan platform smartphone dengan TaintDroid. TaintDroid merupakan upaya berkelanjutan yang telah secara aktif digunakan oleh komunitas keamanan sistem. TaintDroid yang tersedia untuk Android versi 2.1, versi 2.3 (dan menambahkan dukungan JIT), versi 4.1, dan versi 4.3. Informasi untuk men-download dan bangunan TaintDroid dapat ditemukan di http://appanalysis.org.

[5] Sementara pesan Android melewati sistem pendorong terciptanya kekayaan, aplikasi kolaborasi, ia juga memperkenalkan potensi serangan jika sang *developer* tidak mengambil tindakan pencegahan. Kami memeriksa komunikasi antar aplikasi Android dan menyajikan beberapa kelas dari potensi serangan pada aplikasi. *Outgoing communication* dapat menempatkan aplikasi pada risiko pencurian (termasuk *eavesdropping* dan *denial of service*) siaran, pencurian data, hasil modifikasi, dan pembajakan kegiatan dan layanan. *Incoming communication* dapat menyebabkan aplikasi beresiko terkena *activity* dan *service* yang menyebarkan injeksi berbahaya. Kami menyediakan alat, ComDroid, yang dapat digunakan oleh *developer* untuk menemukan jenis kerentanan. Alat kami bergantung pada kode DEX, sehingga *third parties* atau pengulas untuk Android Market dapat menggunakannya untuk mengevaluasi aplikasi yang kode sumbernya tidak tersedia. Kami menganalisis 100 aplikasi dan memverifikasi temuan kami secara manual sebanyak 20 dari aplikasi tersebut. Dari 20 aplikasi tadi, kami mengidentifikasi 12 aplikasi dengan setidaknya satu kerentanan. Ini menunjukkan bahwa aplikasi dapat menjadi rentan untuk menyerang dan bahwa pengembang harus mengambil tindakan pencegahan untuk melindungi diri dari serangan ini.

[6] Kami membahas perizinan delegasi ulang sebagai sebuah masalah dengan sistem izin yang baru. Izin delegasi kembali terjadi ketika Deputi mendelegasi pengaturan izin untuk aplikasi unprivileged tanpa otorisasi pengguna. Ini adalah ancaman yang muncul untuk platform web dan smartphone. Kami menemukan bahwa banyak aplikasi Android berisiko memiliki kerentanan *re-delegation vulnerabilities*, dan kami membangun serangan yang mengeksploitasi 15 kerentanan dalam sistem aplikasi Android. Kami mengungkapkan temuan kami dan mengajukan laporan bug; beberapa kerentanan telah dikonfirmasi sebagai bug. Kami juga menyusun mekanisme pertahanan *runtime-independen*, inspeksi IPC, yang secara

transparan melindungi terhadap serangan pada *confused deputies*, dengan tanpa biaya kompatibilitas untuk *non-deputies* atau *confused deputies*. Namun, Deputi yang disengaja dan klien mereka perlu beberapa modifikasi untuk bekerja dengan inspeksi IPC. Secara khusus, aplikasi yang berinteraksi dengan Deputi mungkin perlu menambahkan izin bahwa jika mereka tidak menggunakannya. Kami merasa bahwa masalah *permission re-delegation* layak perhatian, dan kami berharap makalah ini akan mendorong masa depan bekerja pada masalah ini. Secara khusus, kami percaya analisis statis Deputi yang menjanjikan masa depan untuk analisis sisi server atau platform dengan paket-paket yang sudah diinstal.

[7] Mobile malware berkembang menjadi ekosistem yang kompleks yang akan berkemungkinan nantinya menjadi saingan *desktop malware landscape*. Dalam tulisan ini, kami menyurvei perilaku muatan *mobile malware* saat ini. Saat ini, mobile malware termotivasi terutama oleh keinginan untuk mengirim *premiumrate SMS* dan menjual informasi. Pembentuk motivasi dapat dikalahkan dengan *requiring user confirmation* untuk *premiumrate SMS* pesan (seperti halnya iOS), tetapi penelitian lebih lanjut diperlukan pada topik membela terhadap perangkat perusak yang mencuri data pengguna dan kredensial. Kami juga mengeksplorasi potensi kemana arah malware ini ke depannya; secara khusus, kami berpikir bahwa *credential theft*, pencurian kartu kredit melalui NFC, dan iklan klik penipuan yang paling mungkin untuk menjadi target penulis perangkat perusak masa depan. Sebagai bagian dari survei kami, kami memeriksa izin malware Android. Malware Android biasanya meminta kemampuan untuk langsung mengirim pesan SMS, yang merupakan tindakan yang sangat jarang antara *non-malicious applications*. Namun, kami tidak dapat mengidentifikasi setiap izin berbasis pola lain untuk klasifikasi malware. Classication izin berbasis akan meminta pertimbangan masa depan sebagai kumpulan pertumbuhan malware Android yang dikenal. Kami juga mengamati bahwa tidak satupun dari malware di set data kami telah disetujui oleh Apple App Store, yang menunjukkan bahwa manusia yang memberikan *review* mungkin efektif menjadi tolak ukur untuk menghapus malware. Symbian's otomatis memproses review dan tanda yang bernasib lebih buruk; hampir sepertiga dari malware Symbian dalam set data kami telah disetujui oleh atau menghindari proses ini. Saat ini, kedua penulis perangkat perusak dan pengguna smartphone insentif untuk menemukan akar eksploitasi. Komunitas homebrew menerbitkan akar eksploitasi untuk membantu pemilik smartphone menyesuaikan ponsel mereka. Namun, malware dapat menggunakan mengeksploitasi akar yang sama ini untuk menghindari mekanisme keamanan smartphone; Memang, 4 buah malware di set data kami melakukan hal ini. Kami mempertimbangkan dampak dari komunitas homebrew dan menemukan bahwa akar eksploitasi tersedia antara 74% dan 100% ponsel seumur hidup. Kami merekomendasikan bahwa produsen ponsel mendukung kustomisasi smartphone sehingga komunitas homebrew tidak perlu mencari akar eksploitasi.

Daftar Pustaka

[1] Y. Zhou, Z. Wang, W. Zhou, and X. Jiang, "Hey, You, Get Off of My Market: Detecting Malicious Apps in Official and Alternative Android Markets," *Proc. 19th Annu. Netw. Distrib. Syst. Secur. Symp.*, no. 2, pp. 5–8, 2012.

[2] Y. Zhou and X. Jiang, "Dissecting Android malware: Characterization and evolution," *Proc. - IEEE Symp. Secur. Priv.*, no. 4, pp. 95–109, 2012.

[3] W. Enck, P. Gilbert, B.-G. Chun, L. P. Cox, J. Jung, P. McDaniel, and A. N. Sheth, "TaintDroid: An Information-Flow Tracking System for Realtime Privacy Monitoring on Smartphones," *Osdi '10*, vol. 49, pp. 1–6, 2010.

[4] W. Enck, P. Gilbert, S. Han, V. Tendulkar, B.-G. Chun, L. P. Cox, J. Jung, P. McDaniel, and A. N. Sheth, "TaintDroid," *ACM Trans. Comput. Syst.*, vol. 32, no. 2, pp. 1–29, 2014.

[5] E. Chin, A. Felt, K. Greenwood, and D. Wagner, "Analyzing inter-application communication in Android," *Proc. 9th ...*, pp. 239–252, 2011.

[6] A. P. Felt, H. J. Wang, A. Moshchuk, S. Hanna, and E. Chin, "Permission Re-Delegation: Attacks and Defenses," *Proc. 20th USENIX Conf. Secur.*, pp. 22–22, 2011.

[7] A. P. Felt, M. Finifter, E. Chin, S. Hanna, and D. Wagner, "A survey of mobile malware in the wild," *Proc. 1st ACM Work. Secur. Priv. smartphones Mob. devices - SPSM '11*, pp. 3 – 14, 2011.