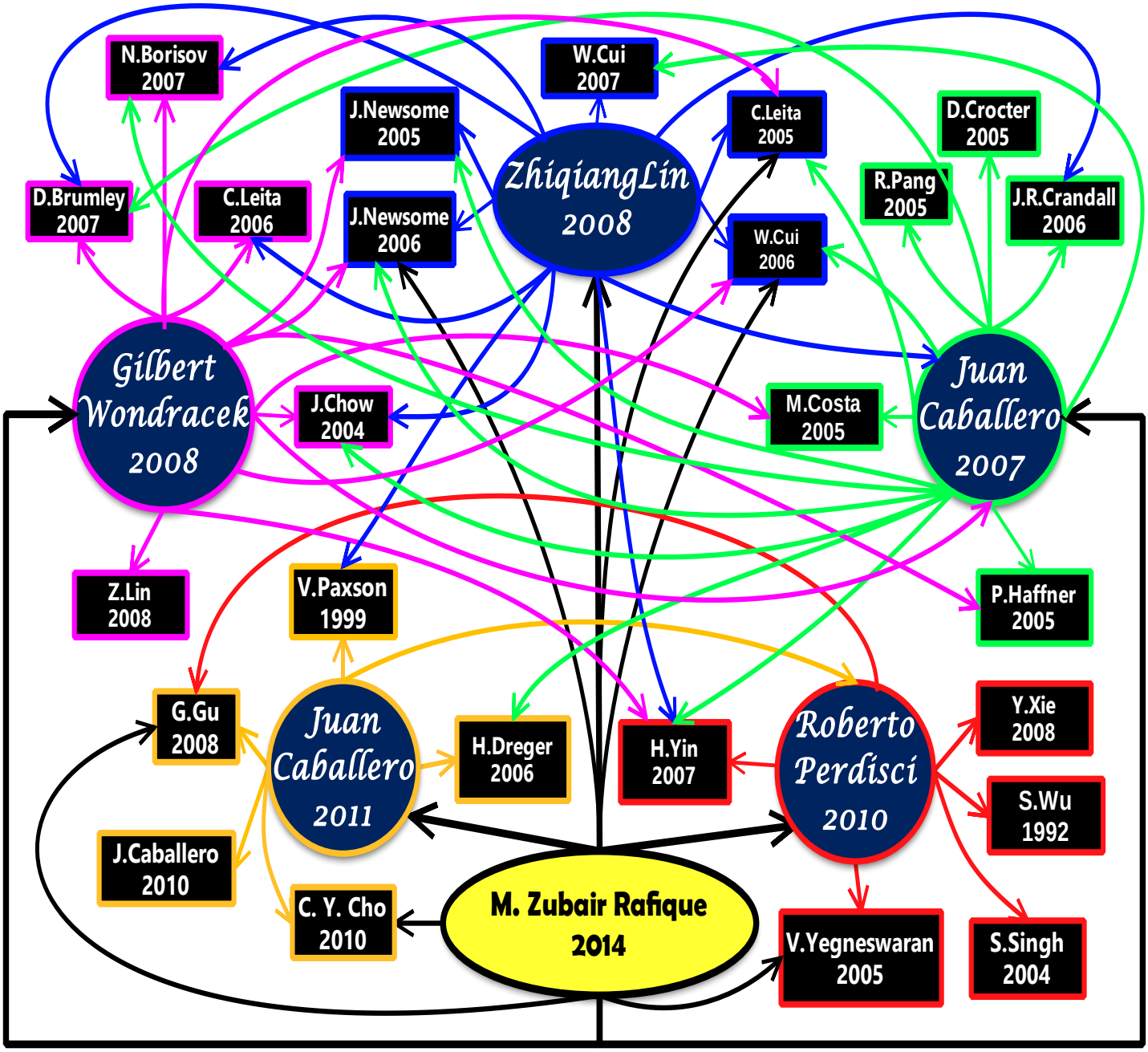
Tugas membuat Site map Citasi Paper
Teknik Penulisan Karya Ilmiah

Donny Giovana Karo-Karo
O9011181520011
SK 2a

Fakultas Ilmu Komputer
Universitas Sriwijaya

SITE MAP CITASI PAPER



Network Dialog Minimization and Network Dialog Diffing: Two Novel Primitives for Network Security Applications

Paper yang dibuat oleh *M. Zubair Rafique (2008)* menjelaskan tentang keamanan jaringan yaitu minimalisasi dialog jaringan dan membedakan dialog jaringan. Minimisasi dialog Network (NDM) menyederhanakan dialog asli sehubungan dengan tujuan, sehingga dialog diminimalkan ketika diputar masih mencapai tujuan, tetapi membutuhkan jaringan minimal komunikasi tion, mencapai waktu dan bandwidth penghematan yang signifikan. Sebuah jaringan terdiri atas dialog yang saling bertukar dalam lalu lintas jaringan menjadi rekan-rekan untuk mencapai suatu tujuan, contohnya bisa seperti mengunjungi situs favorit Anda atau men-download file dari suatu server , tetapi dapat juga berbahaya seperti jika anda memanfaatkan aplikasi jaringan. Misalnya, seperti anda ingin mengunjungi halaman Amazon.com, saat mengetik dan menekan enter maka akan menghasilkan dialog jaringan yang kompleks yang melibatkan beberapa server dan membutuhkan sebanyak 41 koneksi TCP dan bertukar hingga 330 pesan HTTP, yang masing-masing digunakan untuk men-download konten HTML , angka dari CDNs, melakukan analisa, dan tampilan iklan dari jaringan iklan *M. Zubair Rafique (2008).*

M. Zubair Rafique (2008) memperkenalkan masalah dialog jaringan imitasi mini (NDM) dan perbedaan dialog jaringan. Dialog jaringan imitasi mini adalah masalah yang diberi dialog asli yang memenuhi tujuan, menghasilkan dialog yang diminimalkan yang terdiri dari sub terkecil dari dialog asli yang ketika diputar masih mencapai tujuan yang sama seperti dialog asli. Pada dasarnya, dialog diminimalkan VIDES pada jalan pintas untuk tujuan, dan menghapus semua koneksi dan pesan dalam dialog asli yang tidak terkait dengan tujuan. Sebuah dialog diminimalkan diharapkan dapat memahami apa bagian dari dialog dan tujuannya, agar dapat menentukan pesan dan bidang yang benar-benar diperlukan untuk mengeksploitasi server jaringan tanpa analisis kode yang rumit. Untuk membuat kedua sistem keaman jaringan tersebut maka dibutuhkan pula sebuah proses penggalian protokol agar keaman jaringan yang dibuat dapat tersistem dengan baik dan tidak merugikan sebuah instansi yang akan menggunakan sistem keaman jaringan tersebut. Dalam paper *Juan Caballero (2007)* dia menggunakan analisis biner dinamis dan berdasarkan pada intuisi unik, bahwa implementasi dari protokol memproses data aplikasi yang diterima mengungkapkan banyak informasi tentang format pesan protokol. Mereka juga telah menerapkan pendekatan dalam sistem yang disebut Polyglotand yang telah dievaluasi secara ekstensif menggunakan implementasi dunia nyata mengunakan lima protokol yang berbeda: DNS, HTTP, IRC, SAMBA dan ICQ.

Untuk mengaktifkan analisis dinamis protokol, arsitektur Polyglot memiliki dua fase. Pertama, kita mengawasi program eksekusi karena proses pesan yang diberikan. Fase ini menghasilkan rekor pengolahan program, yang berisi semua informasi tentang eksekusi. Kedua, kita menganalisis catatan pengolahan program dan ekstrak keterangan tentang batas-batas lapangan dan kata kunci yang membentuk dasar untuk format pesan. Dibutuhkan sebuah input biner dan aplikasi data program dan monitor untuk mengetahui bagaimana

program akan memproses data aplikasi tersebut, Output dari monitor eksekusi adalah jejak eksekusi yang berisi catatan semua petunjuk yang dilakukan oleh program. Jejak eksekusi menjadi masukan untuk analisis pada tahap kedua. Pada pembuatan suatu sistem keaman jaringan maka akan banyak sekali virus yang akan mengganggu suatu perangkan komputer yang menggunakan keaman jaringan tersebut. Contoh dari virus yang paling sering menggangu suatu perangkat adalah malware. Malware adalah aplikasi yang paling jahat. Malware bertindak sebagai penyerang, pencuri data dan berusaha menyebarkan aplikasi-aplikasi kedalam komputer yang lain di dalam jaringan komputer. Intinya malware adalah program yang mengumpulkan informasi tentang pengguna komputer tanpa izin. Semua aplikasi pengganggu yang saya sebutkan diatas menjalankan aksinya tanpa diketahui yang punya komputer atau laptop. Program ini Ia bisa disebarkan dengan berbagai cara.

Dalam paper *Roberto Perdiscia (2010)* menyajikan suatu sistem pengelompokan malware berdasarkan perilaku jaringan tingkat baru. Kami fokus pada analisis kesamaan struktural di antara jejak lalu lintas HTTP yang berbahaya yang dapat diciptakan dengan mengeksekusi malware berbasis HTTP. Dia juga telah menerapkan konsep sistem pengelompokan malware jaringan dan melakukan percobaan dengan lebih dari 25.000 sampel malware yang berbeda. Dalam penelitian yang telah dilakukan oleh *M. Zubair Rafique (2014)* dia menemukan dari 14.000 sampel malware berjalan dari satu perangkat. Cara mengatasi hal tersebut maka *M. Zubair Rafique (2014)* telah membangun pengamanan sebanyak 9 buah untuk mengeksploitasi dan telah terintegrasi ke dalam infrastruktur yang telah dikumpulkan lebih dari 14.000 malware. Sebuah pengamanan mencapai pengurangan waktu ulangan 34 kali dan penggunaannya memungkinkan mengurangi infrastruktur koleksi malware dari sebuah host. Kedua dapat menerapkan NDM untuk mengukur status masalah ulangan yang terkenal di situs web-populer Penggunaan NDM mencapai pengurangan waktu ulangan 71 kali, menghemat lebih dari 20 jam dari pengolahan setiap hari. Pengukuran kami menunjukkan bahwa meskipun tahun penelitian pada topik 31% dari 100 Alexa domain tidak menghancurkan negara server-side ketika pengguna mengklik link logout. Dengan demikian, pengguna tetap secara efektif login.

Dari semua data yang telah didapat maka dapat ditarik kesimpulan ada dua buah sistem keamanan jaringan yang yaitu dialog jaringan minimisasi dan membedakan dialog jaringan, juga telah di perkenalkan jaringan menulusuri delta , teknik pertama untuk memecahkan dialog jaringan minimalisasi.Paper *Gilbert Wondracek (2008)* membahas tentang protokol reverse. Protokol reverse engineering adalah proses spesifikasi aplikasi-tingkat membagi-bagikan brosur mantan untuk jaringan tocols pro. Spesifikasi tersebut sangat membantu dalam berbagai konteks yang berhubungan dengan keamanan. Misalnya, mereka dibutuhkan oleh sistem deteksi intrusi untuk melakukan paket yang mendalam di- spection, dan mereka memungkinkan pelaksanaan alat memperjelas kotak hitam. Sayangnya, pengguna reverse engineering adalah memakan waktu dan tugas yang membosankan. Untuk mengatasi lem prob ini, peneliti baru-baru ini mengusulkan sistem yang membantu untuk mengotomatisasi proses. Sistem ini beroperasi dengan ana jejak lyzing lalu lintas jaringan. Namun, ada informasi terbatas yang tersedia di jaringan-tingkat, dan dengan demikian, keakuratan hasil terbatas. Pendekatan kami bekerja dengan dy- namically

memantau pelaksanaan aplikasi, an- alyzing bagaimana program sedang memproses bijak protokol-pesan yang diterima. Hal ini dilatarbelakangi oleh pemahaman bahwa aplikasi mengkodekan protokol lengkap dan sebenarnya merupakan spesifikasi otoritatif input yang dapat menerima. Dalam langkah pertama, kita mengekstrak informasi tentang bidang pesan individu. Kemudian, kami mengumpulkan in- formasi ini untuk menentukan spesifikasi yang lebih umum dari format pesan, yang dapat mencakup bidang opsional atau alternatif, dan pengulangan.

Dalam Protokol reverse engineering paper *Zhiqiang Lin (2008)* menyajikan pendapat baru yaitu sistem yang disebut AutoFormat yang bertujuan tidak hanya penggalian bidang protokol dengan akurasi yang tinggi, struktur hirarkis pesan protokol. AutoFormat didasarkan pada wawasan kunci yang bidang protokol yang berbeda dalam pesan yang sama yang ditangani dalam konteks eksekusi yang berbeda (misalnya,waktu berjalan panggilan gagal). Dengan demikian, dengan memantau program eksekusi, kita dapat mengumpulkan informasi konteks eksekusi untuk setiap byte pesan (dijelaskan di seluruh pesan) dan kelas mereka untuk mendapatkan format protokol. Kami telah mengevaluasi sistem kami dengan bijak lebih dari 30 protokol pesan dari tujuh protokol, termasuk dua protokol berbasis teks (HTTP dan SIP), tiga berdasarkan binary-protokol (DHCP, RIP, dan OSPF), salah satu protocol hybrid (CIFS / SMB), serta satu protokol yang tidak diketahui digunakan oleh malware dunia nyata. Hasil kami menunjukkan bahwa AutoFormat tidak hanya dapat mengidentifikasi bidang pesan individual secara otomatis dan dengan akurasi yang tinggi (sebuah 93,4% rasio pertandingan rata-rata dibandingkan dengan Wireshark), tetapi juga mengungkap struktur dari format protokol dengan hubungan re- vealing mungkin (misalnya, sekuensial , paralel, dan erarchical hi) antara bidang pesan.

Site map ini memaparkan 31 Autors atau pembuat paper ilimiah dimana memiliki tujuan untuk mengetahui bagaimana urutan atau rangkaian pencitasian dalam satu judul paper karya ilimiah. Dalam site map ini memiliki urutan atau susunan yang berada paling bawah yang berwarna kuning itu adalah paper yang urutannya paling pertama yang akan menjadi titik awalnya, yang berbentuk bulat berwarna biru tua itu urutan kedua dan yang berbentuk kotak itu urutan ketiga. Bergerak dari paper yang urutan pertama akan mencitasi lima paper, setelah itu kelima paper tadi akan mencitasi masing masing lima paper juga. Didalam site map ini adanya saling mencitasi tidak hanya dalam susunan urutan tadi atau adanya saling citasi diantara tiga pulah satu paper diluar konteks urutannya. Paper M.Zubair Rafique,2014" Network Dialog Minimization and Network Dialog Diffing: Two Novel Primitives for Network Security Applications" dalam site map ini tidak hanya mencitasi 5 paper yang dipaparkan di urutan kedua namun Ia juga mencitasi paper di urutan ke 3 yaitu paper yang juga didicitasi oleh paper Roberto Perdisci,2010 yaitu paper V.Yegnewaran,2005"An architecture for generating semantics-aware signatures", paper yang dicitasi oleh Juan caballero,2011 yaitu paper G.Gu,2008" Botminer: Clustering analysis of network traffic for protocol andstructure independent botnet detection, paper yang dicitasi oleh Zhiqiang Lin,2008 yaitu paper C.Leita,2005" scriptgen: An automated script generation tool for honeyd", W.Cui,2006" Protocol-independent adaptive replay of application dialog", J.Newsome,2006" Replayer: Automatic protocol replay by binary analysis".

Begitu juga diurutan kedua tidak hanya mencitasi 5 papernya masing masing namun mencitasasi bebarapa paper diurutan 3 juga. Selain mencitasi 5 paper yang menjadi bagiannya, paper Roberto Perdisci,2010 mencitasi paper yang juga dicitasi oleh paper Juan Caballero,2011 yaitu paper G.Gu,2008" Botminer: Clustering analysis of network traffic for protocol andstructure independent botnet detection". Begitu juga dengan paper Juan Caballero,2007, Ia mencitasi semua paper yang menjadi bagian Zhiqiang Lin,2008 di site map tersebut yaitu paperC.Leita,2005"Botminer: Clustering analysis of network traffic for protocol andstructure independent botnet detection", paper W.Cui,2006"Protocol-IndependentAdaptive Replay of Application Dialog" paper W.Cui,2007"Discoverer: Automatic Protocol Description Generation from Network Traces" paper J.newsome,2005" Dynamic Taint Analysis for Automatic Detection, Analysis, and Signature Generation of Exploits on Commodity Software" paper J.Newsome,2006" Replayer: Automatic Protocol Replay By Binary Analysis", yang dicitasi paper Gilbert Wondracek,2008 yaitu paper D.Brumley,2007"Towards Automatic Discovery of Deviations in Binary Implementations with Applications to Error Detection and Fingerprint Generation", paper N.Borisov,2007 "A generic application-level protocol analyzer and its language", paper J.Chow,2004 "Understanding Data Lifetime via Whole System Simulation", yang dicitasi paper Roberto Perdisci,2010 yaitu paper H.Yin,2007 "Panorama: capturing system-wide information flow for malware detection andanalysis" yang dicitasi paper Juan Caballero,2011 yaitu paper H.Dreger,2006 "Dynamic Application-Layer Protocol Analysis for Network Intrusion Detection". Paper Zhingqiang Lin,2008 mencitasi paper yang dicitasi paper Roberto Perdisci,2010 yaitu paper H.Yin,2007 "Panorama: capturing system-wide information flow for malware detection and analysis".