DIAGRAM SITASI PAPER

Disusun Oleh :

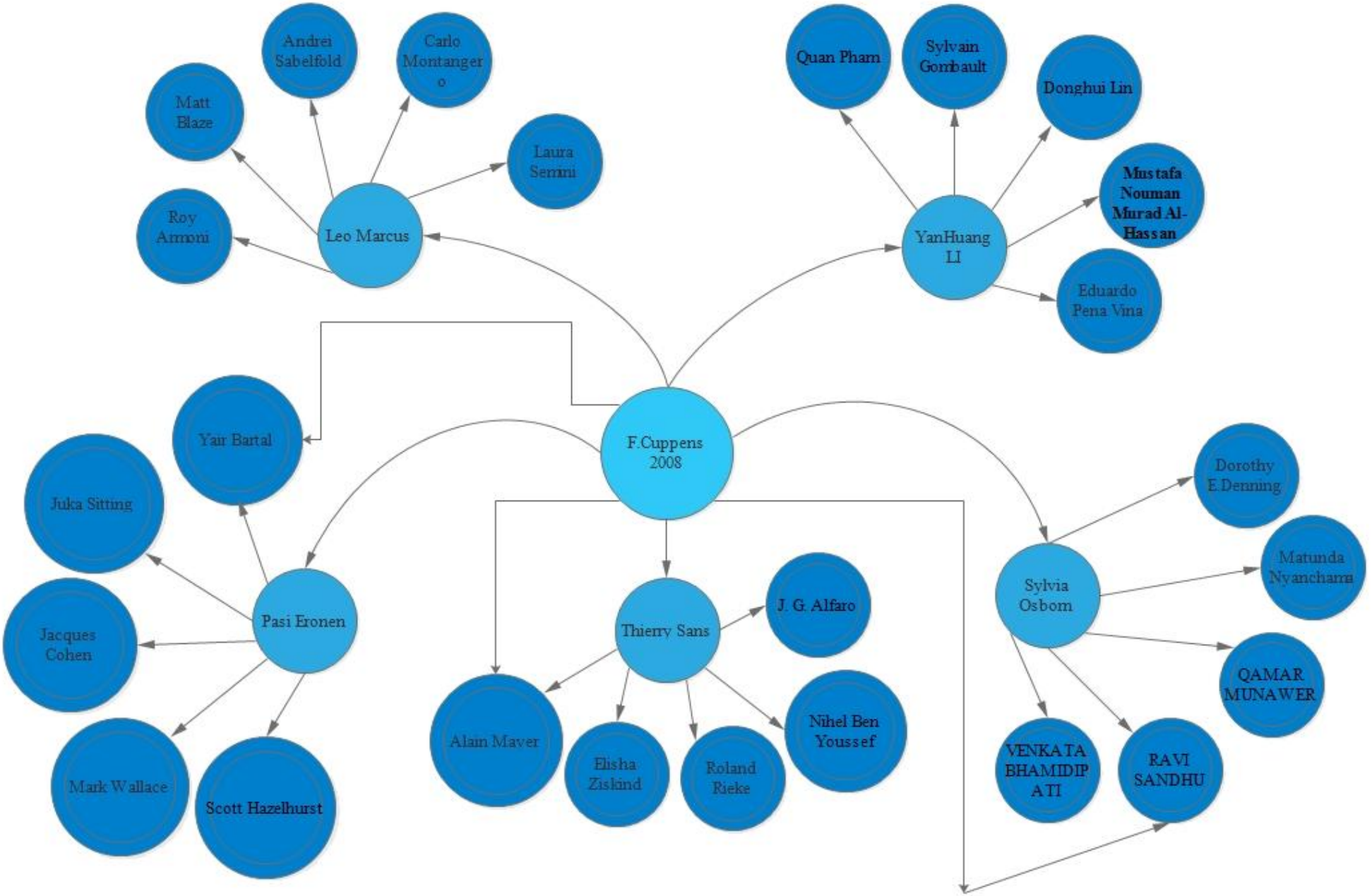
Nama : Stevanus Christivan Panjaitan
NIM : 09011181520030
Kelas : SK2A

PROGRAM STUDI SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2015/2016


F.Cuppens 2008
Leo Marcus
Andrei Sabelfold
Carlo Montangero
Matt Blaze
Laura Semini
Roy Armoni
YanHuang LI
Quan Pham
Sylvain Gombault
Donghui Lin
Mustafa Nouman Murad Al-Hassan
Eduardo Pena Vina
Yair Bartal
Juka Sitting
Pasi Eronen
Jacques Cohen
Mark Wallace
Scott Hazelhurst
Thierry Sans
J. G. Alfaro
Alain Maver
Elisha Ziskind
Roland Rieke
Nihel Ben Youssef
Sylvia Osborn
Dorothy E.Denning
Matunda Nyanchama
QAMAR MUNAWER
VENKATA BHAMIDIPATI
RAVI SANDHU

Pendekatan Formal yang Ditentukan Dengan Menggunakan Kebijakan Keamanan Jaringan

Bahasa konfigurasi firewall saat ini telah ada baik didirikan oleh semantik.Setiap firewall mengimplementasikan algoritma sendiri yang mem-parsing bahasa proprietary tertentu. Konsekuensi utama adalah bahwa kebijakan kontrol akses jaringan sulit untuk mengelola dan firewall yang paling benar-benar salah dikonfigurasi.Kami menyajikan bahasa kontrol akses berdasarkan sintaks XML yang semantik ditafsirkan dalam model kontrol akses Atau-BAC (Berdasarkan Organisasi AksesKontrol). Dalam beberapa file pdf ini menunjukkan bagaimana menggunakan bahasa ini untuk menentukan akses jaringan tingkat tinggi kebijakan kontrol dan kemudian secara otomatis mendapatkan kontrol akses beton aturan untuk mengkonfigurasi firewall tertentu melalui proses penerjemahan. Pendekatan kita memberikan semantik yang jelas untuk jaringan spesifikasi kebijakan keamanan, membuat manajemen kebijakan tersebut lebih mudah bagi administrator dan jaminan portabilitas antara firewall. Hal ini juga dikenal di komunitas keamanan komputer yang menentukan dan mengelola aturan kontrol akses adalah tugas yang sulit apapun tingkat abstraksi dipertimbangkan. aturan kontrol akses ini sebetulnya merupakan bagian dari satu set yang lebih global aturan yang disebut kebijakan organisasi. Kami berpendapat bahwa kebijakan organisasi ini telah harus membuka untuk mendapatkan paket aturan kontrol akses. Setiap paket aturan ditangani oleh komponen keamanan. Misalnya, keamanan lingkungan paket, paket keamanan fisik, paket keamanan sistem operasi, staf paket dan paket keamanan jaringan. Firewall adalah komponen-komponen yang berurusan dengan paket keamanan jaringan. Mereka digunakan untuk memblokir sampai batas tertentu komunikasi yang mencurigakan dari Internet ke jaringan area lokal swasta (LAN) dan mengingkari anggota LAN swasta mengakses semua berbahaya godaan internet. Salah satu masalah yang dihadapi dengan firewall adalah kesulitan administrator harus juga mengkonfigurasi mereka. Ada benar-benar kekurangan suatu metodologi dan sesuai alat pendukung untuk membantu mereka dalam menetapkan keamanan jaringan bagian kebijakan, dan menghasilkan dan menggunakan aturan yang diturunkan dari kebijakan ini. Sebenarnya tidak ada tingkat perantara antara kebijakan persyaratan dirumuskan sebagai sebuah kalimat bahasa Inggris dan set setara dari firewall aturan, mengatakan kode. Bahkan jika administrator firewall mahir dalam banyak bahasa konfigurasi dan alat-alat, keahlian ini tidak menghindari dari membuat kesalahan. Tanpa metodologi yang jelas dan beberapa alat pendukung yang sesuai, ini dapat

menyebabkan untuk generasi aturan konfigurasi yang tidak konsisten dengan yang dimaksudkan jaringan kebijakan keamanan. Kami mengklaim bahwa penggunaan bahasa tingkat tinggi untuk menentukan kebijakan keamanan jaringan akan menghindari kesalahan tersebut dan akan membantu untuk secara konsisten mengubah aturan firewall bila diperlukan. Selain itu, ini tinggi bahasa tingkat harus memungkinkan administrator untuk menentukan persyaratan keamanan dan harus cukup ekspresif untuk menentukan setiap kebijakan keamanan jaringan. Kami juga melihat bahwa tidak ada spesifikasi kebijakan keamanan global sehingga hipotesis yang mendasari selalu dilakukan: komponen keamanan tunggal digunakan, mengatakan firewall tunggal. Sekarang, kadang-kadang lebih mudah untuk menyebarkan keamanan aturan pada beberapa komponen keamanan. Secara khusus, aturan keamanan akses dapat dipisahkan ke dalam paket yang relevan dan ditegakkan oleh lebih dari satu firewall pada LAN yang sama. Selanjutnya, di sebagian besar firewall, administrator menggunakan kebijakan keamanan ganda. Yang mereka tentukan baik izin dan larangan aturan. Dalam hal ini, Temukan oleh firewall aturan yang sesuai didasarkan pada pencocokan pertama atau prosedur pencocokan lalu. Dalam kedua kasus, keputusan tergantung pada bagaimana aturan keamanan diurutkan. Oleh karena itu, administrator harus mengetahui yang benar dan Agar efisien aturan, agar tergantung pada prosedur penyaringan. Ini adalah tugas yang kompleks untuk mengelola terutama ketika kebijakan keamanan harus diperbarui. Selain itu, dalam beberapa kasus, bahkan tidak selalu mungkin untuk menyortir aturan. Jadi, kebijakan kontrol akses tertutup yang hanya mencakup izin mungkin sebuah alternatif. Untuk menangani kebijakan keamanan jaringan, beberapa topologi dari organisasi jaringan area lokal harus ditegakkan. Oleh karena itu, LAN dibagi-ke zona. Kontrol akses terdiri aman mengelola komunikasi antara zona ini. Kami menunjukkan dalam makalah ini yang melihat dan definisi peran Atau Untuk menangani kebijakan keamanan jaringan, beberapa topologi organisasi ini jaringan area lokal harus ditegakkan. Oleh karena itu, LAN dibagi-ke zona. Kontrol akses terdiri aman mengelola komunikasi antara zona ini. Kami menunjukkan dalam makalah ini yang melihat dan definisi peran Atau .Dalam hubungan ini, kami juga menyelidiki apakah mungkin untuk menentukan kebijakan keamanan jaringan dengan memanfaatkan izin saja. Itu kontribusi yang besar dari kebijakan tertutup ini untuk menghindari harus memilah aturan firewall yang diturunkan untuk menegakkan kebijakan ini. Menyortir aturan sebenarnya kompleks untuk mengelola dan merupakan sumber utama dari kesalahan. Ini adalah salah satu kelemahan utama banyak firewall languages. Proses penalaran pada akses kebijakan pengendalian tidak dianggap. Oleh karena itu, ada kurangnya semantik akurat yang memungkinkan administrator keamanan untuk menghindari firewall

mis-konfigurasi.Sisa dari makalah ini disusun sebagai berikut. Bagian 2 menyajikan konsep utama Atau-BAC menggunakan sintaks XML di harapan terjemahannya menjadi platform target yang diberikan. Kami jelaskan di bagian 3 cara menentukan kebijakan keamanan jaringan di Atau-BAC dan mitranya di XML. Kami menggambarkan pendekatan ini dengan contoh arsitektur keamanan berbasis pada dua firewall. Kami kemudian merancang sebuah proses penerjemahan di XSLT untuk menghasilkan aturan konfigurasi filtering firewall tertentu. Pendekatan ini telah diterapkan untuk firewall Netfilter. Keaslian proposal kami adalah bahwa ia menyediakan link semantik yang jelas antara model abstrak kontrol akses, yaitu Atau-BAC, dan pelaksanaannya menjadi komponen-komponen keamanan tertentu, yaitu firewall. Pendekatan kami menyediakan tingkat tinggi abstraksi dibandingkan dengan aturan keamanan final yang digunakan untuk mengkonfigurasi firewall. Ini harus menyederhanakan manajemen aturan keamanan seperti dan menjamin portabilitas antara firewall.