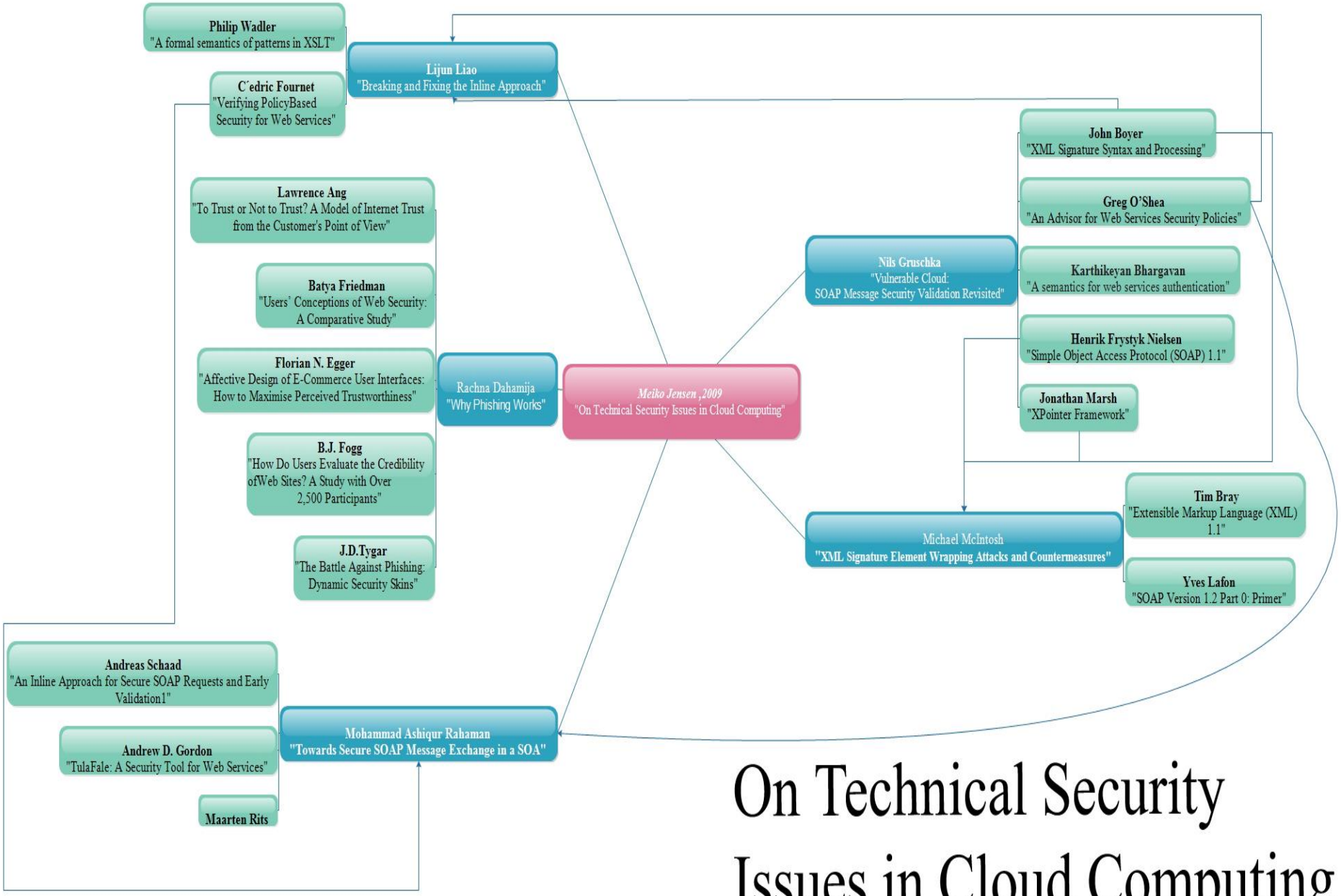

On Technical Security Issues in Cloud Computing

KESIMPULAN

Meiko Jensen ,mempresentasikan mengenai masalah didalam cloud computing security. Meiko Jensen menggunakan aplikasi XML Signature dan the Web
Services security frameworks (untuk menyerang cloud computing security itu sendiri). mendiskusikan kepentingan dan kemampuan dari keamanan browser di cloud computing context. Tingginya perhatian terhadap kejujuran pelayanan cloud dan pengikatan masalah.

Nils Gruschka ,menjelaskan bahwa ada tanda tanda penyerangan yang serius terhadap layanan web dan keamanan SAO. Paper ini menunjukan pengetahuan kita mengenai kejadian pertama dunia terhadap peyerangan dasar operasional layanan aplikasi. Mereka menyelidiki solusi proposal saat ini pada efeknya di dalam cahaya dan menyimpulkan bahwa mereka hanya bisa mencegah serangan ini.

rachna dahamija ,menjelaskan bahwa ini adalah ilustrasi pembelajaran dengan lengkap mengenai skenario kasus terbaik, ketika pengguna mengharapkan sebuah lelucon yang di persembahkan dan mengetahui motivasinya. Didalam pembelajaran, situs phising terbaik telah bisa untuk membodohi lebih dari 90% orang yang berpartisipasi. Penunjuk akan mendisain terhadap sinyal yang dianggap layak dimana mereka yang tidak mengerti dari banyak orang yang berpartisipasi. 5 dari 22 partisipasi (23%) yang hanya menggunakan isi dari website untuk menilai itu adalah kebenaran, tanpa melihat porsi orang yang ada di browser.

Lijun liao, mereka meninjau kembali masalah pembungkusan serangan dan menunjukan ketidakamanan pada pendekatan garis keamanan. Mereka memperkenalkan contermeasures berdasarkan penyaringan dan jalur dokumen mutlak. Mereka telah menunjukan bahwa contermeasures itu efektif dan tidak memerlukan modifikasi kebijakan keamanan. Pekerjaan dimasa depan mereka bertujuan untuk mendefinisikan sematic formal elemen XML signature dan menerapkan pendekatan yang disajikan.

Mohammad Ashiqur Rahaman, pertukaran pesan SOAP adalah salah satu layanan inti yang diperlukan untuk integrasi sistem di Service Oriented Architecture (SOA) lingkungan. Salah satu perhatian utama dalam SOA adalah demikian untuk memberikan pesan Tingkat Keamanan (sebagai lawan titik ke titik keamanan). Mereka mengamati bahwa sistem berkomunikasi dengan satu sama lain dalam SOA lebih pesan SOAP, sering tanpa perlindungan yang memadai terhadap serangan XML. Mereka sudah menyediakan solusi untuk melindungi integritas dari pesan SOAP dalam pekerjaan sebelumnya. Solusi ini didasarkan pada penggunaan informasi struktur pesan (SOAP Account) untuk pelestarian integritas pesan.Namun, karya sebelumnya tidak membahas masalah penempaan Rekening SOAP itu sendiri. Dalam tulisan ini, mereka membahas fitur integritas Akun SOAP dalam konteks yang lebih umum dari layanan web keamanan negara saat ini seni.

Michael McIntosh, Penggunaan dari XML Signature dapat mengakibatkan dokumen yang ditandatangani yang tersisa rentan terhadap modifikasi terdeteksi oleh musuh. Dalam penggunaan khas XML Signature untuk melindungi pesan SOAP, musuh mungkin mampu memodifikasi pesan yang valid untuk mendapatkan akses tidak sah ke sumber daya yang dilindungi.Makalah ini menjelaskan kerentanan umum dan beberapa eksploitasi terkait, dan mengusulkan penanggulangan yang tepat. Sementara serangan yang dijelaskan di sini mungkin tampak jelas para ahli keamanan setelah mereka menjelaskan, penanggulangan yang efektif memerlukan spesifikasi kebijakan keamanan hati-hati dan pelaksanaan yang benar oleh penyedia pesan yang ditandatangani dan konsumen.Karena pelaksana ini tidak selalu ahli keamanan, makalah ini memberikan panduan yang diperlukan untuk mencegah serangan ini.

Karthikeyan Bhargavan, mereka menganggap masalah menentukan dan memverifikasi protokol keamanan kriptografi forXMLweb layanan. Spesifikasi keamanan WS-Security menjelaskan unsur-unsur keamanan berbagai ofXML, seperti token nama pengguna, sertifikat kunci publik, dan tanda tangan digital, sebesar kosakata yang fleksibel untuk mengekspresikan protokol.Untuk menggambarkan sintaks dari elemen-elemen ini, mereka memperluas biasa XML model data dengan representasi simbolis nilai ofcryptographic. Mereka menggunakan predikat pada model data ini untuk menggambarkan semantik ofsecurity elemen dan protokol ofsample didistribusikan dengan Microsoft pelaksanaan WSE terhadap OFW-Security.Dengan menyematkan model data mereka dalam Abadi dan Fournet ini diterapkan pi kalkulus, mereka merumuskan dan membuktikan sifat keamanan sehubungan dengan model ancaman Dolev-Yao standar. Selain itu, mereka secara informal membicarakan masalah tidak ditangani oleh model formal. Untuk yang terbaik ofour pengetahuan, ini adalah pendekatan pertama dengan spesifikasi dan verifikasi ofsecurity protokol berdasarkan akun setia format XML.

Greg O'Shea, mereka mengidentifikasi kerentanan keamanan umum ditemukan selama ulasan keamanan layanan web dengan keamanan kebijakan didorong. Mereka menggambarkan desain penasihat untuk konfigurasi keamanan layanan web, alat pertama kedua untuk mengidentifikasi kerentanan tersebut secara otomatis dan untuk menawarkan nasihat perbaikan.Kami melaporkan pelaksanaannya sebagai plugin untuk Microsoft Web Services Enhancement (WSE).

Henrik Frystyk Nielsen, SOAP adalah protokol ringan untuk pertukaran informasi dalam desentralisasi, lingkungan terdistribusi.Ini adalah protokol berbasis XML yang terdiri dari tiga bagian: sebuah file yang mendefinisikan kerangka kerja untuk menggambarkan apa yang ada dalam pesan dan bagaimana proses itu, satu set aturan pengkodean untuk mengekspresikan contoh tipe data yang didefinisikan oleh aplikasi, dan konvensi untuk mewakili sedikit prosedur panggilan dan tanggapan. SOAP potensial dapat digunakan dalam kombinasi dengan berbagai protokol lainnya; Namun, satu-satunya yang mengikat didefinisikan dalam dokumen ini menjelaskan bagaimana menggunakan SOAP dalam kombinasi dengan HTTP dan Ekstensi Kerangka HTTP .

John Boyer, Dokumen ini menetapkan XML aturan dan kalimat pengolahan tanda tangan digital . XML Signatures menyediakan integritas, otentikasi pesan atau layanan otentikasi penandatangan untuk data dari jenis apa pun, apakah terletak di dalam XML yang mencakup tanda tangan atau di tempat lain. Dokumen ini menjelaskan mengenai algorithsm ,kalimat untuk menandai inti dari XML, aturan prosesing, penambahan tanda kalimat pada XML, pertimbangan keamanan, dan definisi dari XML tersebut.

Jonathan Marsh, Spesifikasi ini mendefinisikan XML Pointer Language (XPointer) Framework, sistem dapat diperluas untuk XML pengalamatan yang mendasari tambahan XPointer skema spesifikasi.Kerangka ini dimaksudkan untuk digunakan sebagai dasar untuk pengidentifikasi fragmen untuk setiap sumber daya yang jenis media Internet adalah salah satu tulisan, aplikasi, text eksternal parsing entitas, atau aplikasi eksternalis parsed kesatuan. jenis media berbasis XML lain juga didorong untuk menggunakan kerangka kerja ini dalam mendefinisikan bahasa fragmen pengenal mereka sendiri.

Lawrence Ang, Kepercayaan adalah masalah besar dalam transaksi Internet. Makalah ini menyajikan model kepercayaan di internet yang berfokus pada tiga dimensi kepercayaan. Ini menyelidiki nilai yang dirasakan sebuah tempat konsumen pada dimensi ini ketika diatur dalam konteks kategori produk yang berbeda, diskon harga dan kedekatan pembelian.Dikatakan bahwa pedagang Internet lebih bersedia memperhatikan tiga faktor tersebut, semakin besar persepsi kepercayaan dan karenanya semakin besar kemungkinan transaksi.

Batya Friedman, Penelitian ini mencirikan konsepsi pengguna 'keamanan web. Tujuh puluh dua individu, 24 masing-masing dari sebuah komunitas pedesaan di Maine, sebuah komunitas profesional pinggiran kota di New Jersey, dan komunitas teknologi tinggi di California, berpartisipasi dalam luas waktu (2 jam) wawancara semi-terstruktur (termasuk tugas menggambar) tentang keamanan Web. masyarakat keliru dievaluasi apakah sambungan aman atau tidak aman. tipologi empiris yang diturunkan disediakan untuk konsepsi keamanan berdasarkan pengguna penalaran verbal, bukit jenis pengguna tergantung pada di mengevaluasi apakah sambungan aman, dan konsepsi keamanan seperti yang digambarkan dalam pengguna 'gambar. implikasi desain yang dibahas.

Florian N. Egger, e-commerce Sukses desain pengalaman pengguna tergantung pada banyak faktor. Makalah ini berfokus pada penerimaan konsumen dari dan kepercayaan dalam sistem e-commerce, berdasarkan nilai transaksi dan risiko yang dirasakan. Model kepercayaan untuk e-commerce (MOTEC) oleh Egger (2000) memberikan kerangka membuat faktor eksplisit cenderung mempengaruhi kepercayaan pelanggan.Untuk setiap komponen Model, prinsip-prinsip desain yang disediakan, bersama dengan pedoman yang lebih konkret. Ini akan menunjukkan bahwa user interface hanya satu elemen dari pengalaman pelanggan. Merancang untuk kepercayaan karena itu memerlukan pengguna pengalaman strategi untuk melihat melampaui desain hanya dari situs web dan memperhatikan lebih manajemen umum dan masalah pemasaran.

B.J. Fogg, Dalam penelitian ini 2.684 orang dievaluasi kredibilitas dalam dua situs Web langsung dengan topik serupa (seperti situs kesehatan). mereka mengumpulkan komentar orang menulis tentang setiap kredibilitas dan dianalisis komentar untuk mengetahui fitur apa dari situs Web mendapatkan perhatikan ketika orang menilai kredibilitas. Mereka menemukan bahwa looki iDesign situs itu disebutkan paling sering, yang hadir dalam 46,1% dari komentar. Berikutnya yang paling umum adalah komentar tentang struktur informasi dan fokus informasi. Dalam makalah ini mereka berbagi sampel komentar peserta di atas 18 daerah yang orang perhatikan ketika mengevaluasi situs Web kredibilitas. Mereka mendiskusikan alasan untuk keunggulan desain tampilan, menunjukkan bagaimana studi masa depan dapat membangun apa yang telah kita pelajari di baris baru ini penelitian, dan implikasi desain garis enam untuk manusia dan komputer melakukan interaksi.

J.D.Tygar, Phishing adalah masalah model untuk menggambarkan keprihatinan kegunaan privasi dan keamanan karena kedua sistem desainer dan penyerang pertempuran menggunakan user interface untuk memandu (atau menyesatkan) pengguna.mereka mengusulkan skema baru, Dinamis Security Skins, yang memungkinkan web server jarak jauh untuk membuktikan identitasnya dengan cara yang mudah untuk pengguna manusia untuk memverifikasi dan sulit bagi seorang penyerang untuk menipu. Mereka menggambarkan desain perpanjangan ke browser Mozilla Firefox yang mengimplementasikan skema ini.Mereka menyajikan dua teknik interaksi baru untuk mencegah spoofing. Pertama, ekstensi browser mereka menyediakan jendela terpercaya di browser didedikasikan untuk username dan password masuk. Mereka menggunakan gambar fotografi untuk membuat jalur dipercaya antara pengguna dan jendela ini untuk mencegah spoofing dari jendela dan bidang entri teks.Kedua, skema mereka memungkinkan server jauh untuk menghasilkan gambar abstrak yang unik untuk setiap pengguna dan setiap transaksi. Gambar ini menciptakan "kulit" yang secara otomatis menyesuaikan jendela browser atau elemen antarmuka pengguna di isi dari halaman web jauh. ekstensi mereka memungkinkan browser pengguna untuk secara mandiri menghitung gambar bahwa mereka mengharapkan untuk menerima dari server. Untuk mengotentikasi konten dari server, pengguna visual dapat memverifikasi bahwa gambar cocok. Mereka menyesuaikan pekerjaan mereka dengan proposal anti-phishing yang ada. Berbeda dengan usulan lain, skema mereka menempatkan beban yang sangat rendah pada pengguna dalam hal usaha, memori dan waktu.Untuk

mengotentikasi dirinya, pengguna harus mengakui hanya satu gambar dan mengingat satu password entropi rendah, tidak peduli berapa banyak server dia ingin berinteraksi dengan. Untuk mengotentikasi konten dari server dikonfirmasi, pengguna hanya perlu melakukan satu operasi pencocokan visual untuk membandingkan dua gambar.Selain itu, menempatkan beban tinggi usaha pada penyerang untuk menipu indikator keamanan disesuaikan.

C´edric Fournet, WS-SecurityPolicy adalah bahasa konfigurasi deklaratif untuk mengemudi mekanisme keamanan layanan web. Mereka menggambarkan semantik formal untuk WS-SecurityPolicy, dan mengusulkan bahasa tautan yang lebih abstrak untuk menentukan tujuan keamanan layanan web dan klien. Oleh karena itu, mereka menyajikan arsitektur dan implementasi dari alat sepenuhnya otomatis yang mengkompilasi file kebijakan dari spesifikasi tautan, dan memverifikasi dengan menerapkan teorema prover apakah satu set file kebijakan yang dijalankan oleh sejumlah pengirim dan penerima dengan benar mengimplementasikan tujuan dari spesifikasi tautan, meskipun penyerang aktif. Kebijakan driven layanan web implementasi rentan terhadap kerentanan halus biasa terkait dengan protokol kriptografi; alat mereka membantu mencegah kerentanan tersebut, mereka dapat memverifikasi kebijakan ketika pertama kali disusun dari spesifikasi tautan, dan juga verifikasi ulang kebijakan terhadap tujuan asli mereka setelah modifikasi selama penyebaran.

Andrew D. Gordon, layanan Web spesifikasi keamanan biasanya dinyatakan sebagai campuran skema XML, misalnya pesan, dan penjelasan naratif. Mereka mengusulkan bahasa spesifikasi baru untuk menulis deskripsi mesin-checkable melengkapi protokol keamanan berbasis SOAP dan sifat mereka. bahasa TulaFale mereka didasarkan pada kalkulus pi (untuk koleksi penulisan prosesor SOAP berjalan secara paralel), ditambah sintaks XML (untuk mengekspresikan pesan SOAP), predikat logis (untuk membangun dan pesan penyaring SOAP), dan pernyataan korespondensi (untuk menentukan tujuan otentikasi protokol). implementasi mereka mengkompilasi TulaFale ke pi kalkulus diterapkan, dan kemudian berjalan berdasarkan resolusi-protokol verifier Blanchett ini. Oleh karena itu, kita secara otomatis dapat memverifikasi sifat otentikasi protokol SOAP.

Maarten Rits, Mengenai status tingkat keamanan pesan dalam Web Services, berbagai standar seperti WS-Security bersama dengan WS-Policy memainkan peran sentral. Meskipun standar tersebut cocok untuk memastikan end-to-end tingkat keamanan pesan yang bertentangan dengan point-to-point keamanan, serangan tertentu seperti penulisan ulang XML masih mungkin terjadi. Selain generasi dan validasi mekanisme keamanan kunci (misalnya tanda tangan) selalu prosesor tugas intensif. Berdasarkan beberapa skenario dunia nyata kami mengusulkan skema untuk memasukkan informasi Struktur SOAP dalam pesan SOAP keluar dan memvalidasi informasi ini sebelum kebijakan didorong validasi di akhir penerimaan. Hal ini memungkinkan kita untuk mendeteksi beberapa serangan XML menulis ulang pada awal proses validasi, dengan peningkatan kinerja. Kami melaporkan pada teknik yang efisien ini dan memberikan evaluasi kinerja. Kami juga memberikan wawasan ke dalam WS-Security, WS-Kebijakan dan fitur dan kelemahan standar terkait.

Tim Bray, Extensible Markup Language (XML) adalah bagian dari SGML yang benar-benar dijelaskan dalam dokumen ini. Tujuannya adalah untuk memungkinkan SGML generik untuk dilayani, diterima, dan diproses di Web dengan cara yang sekarang mungkin dengan HTML. XML telah dirancang untuk kemudahan mengimplementasi dan untuk interoperabilitas dengan kedua SGML dan HTML.

Yves Lafon, SOAP Versi 1.2 Bagian 0: Primer (Second Edition) adalah dokumen non-normatif dimaksudkan untuk memberikan tutorial mudah dimengerti pada fitur SOAP Versi 1.2. Secara khusus, ia menjelaskan fitur melalui berbagai skenario penggunaan, dan dimaksudkan untuk melengkapi teks normatif yang terkandung dalam Bagian 1 dan Bagian 2 dari SOAP 1,2 spesifikasi. Edisi kedua ini mencakup materi tambahan pada SOAP Pesan

Optimization Transmisi Mekanisme (MTOM), XML-biner Optimized Kemasan (XOP) dan Sumber Daya Perwakilan SOAP header Block (RRSHB) spesifikasi.