

KEAMANAN DATA DALAM NETWORK ATTACHED STORAGE

*TUGAS
KEAMANAN SISTIM LANJUT
EC 7010*



Disusun Oleh

SRI PRIHATININGSIH

23203130

**PROGRAM MAGISTER TEKNIK ELEKTRO
BIDANG KHUSUS TEKNOLOGI INFORMASI
INSTITUT TEKNOLOGI BANDUNG**

2004

Daftar Isi

Daftar Isi	2
Abstrak	3
1. Apa itu Network Attached Storage (NAS)	4
1.1.Ancaman terhadap penyimpanan data	6
1.1.1.Virus Kode Jahat yang bebas	6
1.2.Solusi Terhadap Ancaman Virus	8
1.2.1 ServerProtect's Three-Tiered Architecture.....	8
1.2.2.Rancangan Server Protect pada NAS	9
1.3.Bentuk dan Keuntungan NAS SolutionsVirus Scanning Protect Data Integrity	11
1.3.1.Updating Otomatis	11
1.3.2.Manajemen terpusat melalui rancangan 3 rangkaian.....	12
1.3.3.Scalability dan High Performance	12
1.3.4.Comprehensive Log Reports	12
2. Keamanan pada Network Attached Storage	13
2.1.Interface Drive Indepence Sistem File	13
2.2.Disk Tanpa Pengamanan Fisik	15
2.3.Pilihan Hardware Pengaman	16
2.4. Kunci Hirarkhi	17
3. Kesimpulan	20
Daftar Pustaka	21

Abstrak

Penyimpanan data telah menjadi suatu yang penting yang merupakan bagian dari lingkungan perusahaan IT yang berkembang pesat, sebagai pendorong inisiatif bisnis baru untuk meningkatkan jumlah informasi yang besar. Untuk menghadapi permintaan yang besar terhadap kapasitas penyimpanan, perusahaan-perusahaan maju telah mengembangkan solusi manajemen data berdasarkan inovasi rancangan penyimpanan yang baru, termasuk teknologi network attached storage (NAS) dan storage area network (SAN).

Karena perusahaan-perusahaan ini menggunakan solusi moderen untuk menambah skala, sistem penyimpanan berteknologi tinggi, mereka harus memperhatikan untuk tidak membahayakan standar keamanan Jaringan. Peralatan network attached storage dan data yang ada mudah diserang oleh virus, cacing dan bentuk lain kode yang bermusuhan. Proteksi anti virus merupakan peringatan yang sangat penting, baik untuk mengamankan integritas data yang disimpan dan mencegah kode bermusuhan dari penyebaran ke bagian-bagian lain dari Jaringan lewat sistem penyimpanan. Kebijakan anti virus perusahaan yang bertanggung jawab memerlukan solusi anti virus yang berdedikasi untuk network attached storage.

Keyword : *NAS dan SAN*

1. Apa itu Network Attached Storage (NAS)?

Bisnis sekarang ini memerlukan akses yang tetap terhadap data yang terbagi-bagi, seperti inventori, catatan pelanggan dan database karyawan. Aplikasi yang penting, seperti email, dan sumber-sumber yang penting, seperti Web server, juga memerlukan jumlah penyimpanan yang bertambah terus untuk melayani kebutuhan bisnis. Lebih-lebih, karena perusahaan-perusahaan mengadopsi teknologi baru untuk meningkatkan produktivitas, mereka mengembangkan akses internet berkecepatan tinggi, membangun intranet, menggunakan aplikasi software yang lebih rumit, dan bekerja dengan bentuk media yang lebih banyak. Hasilnya berupa sebuah "ledakan" dalam jumlah data yang dihasilkan, disimpan dan diakses.

Model penyimpanan tradisional melibatkan sebuah drive hard disk dan susunan disk atau sebuah sistem RAID yang ditempelkan secara langsung ke sebuah server atau mesin desktop. Dikenal dengan nama Direct Attached Storage (DAS), model ini masih banyak dipakai, tapi tidak dapat memenuhi kebutuhan masa depan. Karena ini menyebarkan data secara meluas diantara banyak server, model DAS tidak efisien dan tidak cocok untuk mengatur penyimpanan yang besar di dalam sebuah lingkungan jaringan. Dua konsep baru yang telah memulai menggantikannya adalah network attached storage (NAS) dan storage area network (SAN).

NAS adalah sistem yang berdiri sendiri, penyimpanan yang dapat dibagi yang menghubungkan secara langsung ke dalam jaringan dan dapat diakses ke dalam server yang beraneka ragam dan computer klien (seperti, Unix, Windows NT/2000, Netware, Linux, dll.). Aplikasi NAS penting dalam spesialisasi server untuk mengoptimalkan pembagian file ke dalam jaringan dan diantara kerangka yang berbeda-beda. dengan cara yang sederhana hanya menempelkan alat tersebut ke dalam jaringan, bagian IT dapat dengan cepat dan mudah mengembangkan kapasitas jaringan penyimpanan. Desain-desain khusus membantu meningkatkan efisiensi dan mengontrol pengeluaran-pengeluaran IT.

Sementara itu integrasi dengan jaringan selain merupakan salah satu kekuatan rancangan NAS, hal ini juga membawa ke dalam pembatasan yang besar. Karena

sistem penyimpanan membagi ke dalam jaringan yang sama dengan klien dan aplikasi server, lalu lintas data yang berat dapat menyebabkan efek yang tidak diinginkan, seperti bottlenecks dan mengurangi penampilan jaringan. Model Storage Area Network (SAN) menghindari hal ini dengan menciptakan alat yang terpisah, jaringan dedikasi, dihubungkan ke jaringan dengan software khusus dan penghubung. Kerangka SAN memungkinkan data yang terpusat dan manajemen solusi yang berskala besar yang dapat memaksimalkan penampilan sistem dengan memindahkan lalu lintas data dari jaringan yang regular. Secara umum, sebagian besar para ahli menganggap bahwa kedua model sebagai pengganti lebih dari pada eksklusif. Sebagai contoh, penggunaan NAS dapat menjadi komponen yang efektif di dalam sebuah SAN.

Dalam NASD, file manager memegang tanggung jawab untuk mengelola kebijakan "name space" dan kontrol akses pada sistem file namun, file manager dilewati dalam operasi kasus-kasus umum seperti transfer data. File manager menentukan keputusan kontrol akses berdasarkan pada kebijakan sistem file tingkat tinggi. Ketika operasi kasus umum, seperti transfer data, diminta oleh klien, maka *drive* menjalankan keputusan kontrol akses yang sebelumnya dispesifikasi oleh file manager. NASD menggunakan mekanisme kapabilitas untuk mengkomunikasikan keputusan kontrol akses dari file manager kepada *disk drive*. Apa yang membuat rancangan NASD secara signifikan berbeda dari rancangan klasik adalah keputusan kebijakan dan pelaksanaannya dipisahkan oleh jaringan yang tidak aman yang memperkenalkan resiko keamanan baru kepada data yang tersimpan pada *drive*.

Drive mempresentasikan kepada file manager dan klien dengan spasi nama yang rata yang mengacu pada variabel ukuran objek yang membentuk file sistem yang hierarkis yang diharapkan oleh pengguna (user). Objek merupakan abstraksi yang ditunjukkan oleh *disk drive* NASD ; sebuah file merupakan abstraksi yang ditunjukkan kepada pengguna (user) oleh file manager dan mesin klien. Pada tingkat minimum, sebuah *drive* mengandung komponen yang dapat ditemukan pada *disk* saat ini ; sebuah microprocessor, sebuah interface jaringan, buffer memory, dan perangkat penyimpanan. Beberapa implementasi *drive* dapat

mencakup hardware lain seperti hardware temper-resistant, support hardware cryptografik, atau konpoter kontroller (RAID) yang secara transparan menggabungkan sekelompok *drive* (SCSI) yang lebih sederhana. *Drive* dengan tingkat pengamanan tinggi akan mengandung coprocessor pengamanan tambahan, yaitu sebuah processor dan memori yang memiliki fungsi umum. Dalam beberapa kasus, rancangan *drive* akan mengorbankan beberapa pengamanan dengan menghapuskan hardware temper-resistant dan akselerator cryptografik untuk mengurangi biaya.

1.1. Ancaman terhadap Penyimpanan Data

1.1.1 Virus dan Kode Jahat yang Bebas

Virus dapat membahayakan integritas dan keamanan data dengan cepat dalam suatu sistem penyimpanan. Sebuah virus baru dan tidak dikenal yang masuk melewati pertahanan lain mungkin berakhir di dalam system penyimpanan. Jika ini merupakan virus yang merusak, hal ini menulari, merusak atau menghancurkan sejumlah data yang besar sebelum hal itu terdeteksi. Sekalipun virus-virus ini gagal memasuki sistem penyimpanan secara langsung, mereka dapat menyebabkan penularan atau merusak arsip yang harus dimasukkan ke dalam NAS dari desktop atau sistem lain dimana kode jahat diserang.

Sebuah virus computer adalah sebuah kode yang dapat dijalankan yang ditegaskan oleh kemampuannya untuk menjiplak. Bentuk lain dari tipe virus termasuk kemampuan masuk ke dalam komputer tanpa sepengetahuan.

beroperasi bertentangan dengan keinginan pengguna, memasukkan jiplakannya sendiri ke dalam file-file yang beraneka ragam dan membawa sebuah "payload" dengan perintah-perintah yang merusak. Sektor boot yang sederhana dan file virus yang merupakan hal umum pada satu dekade dulu telah berkembang menjadi keturunan yang baru : seperti virus polymorphic, yang merubah kode mereka untuk menghindari deteksi, cacing yang dapat menjiplak dan berkembang melalui jaringan tanpa mempengaruhi file. Trojans yang

menyerang sistem dengan muncul sebagai aplikasi yang tidak merusak, dan banyak kode jahat lain yang mengancam juga merupakan bagian dari pertumbuhan ancaman, walaupun secara tehnik mereka tidak mengancam, mereka tetap dianggap sebagai virus.

Selama bertahun-tahun, jumlah virus yang diketahui telah melampaui angka 50,000, dan mereka telah menjadi lebih cepat, lebih pandai dan lebih susah untuk dihapus. Mereka dapat menempelkan mereka sendiri terhadap jenis-jenis file dan berkembang lebih efisien, dalam cara-cara yang berbeda. Munculnya virus global akhir-akhir ini seperti Love Letter, Anna Kournikova dan Naked Wife Trojan telah menunjukkan betapa efektifnya kode jahat tersebut.

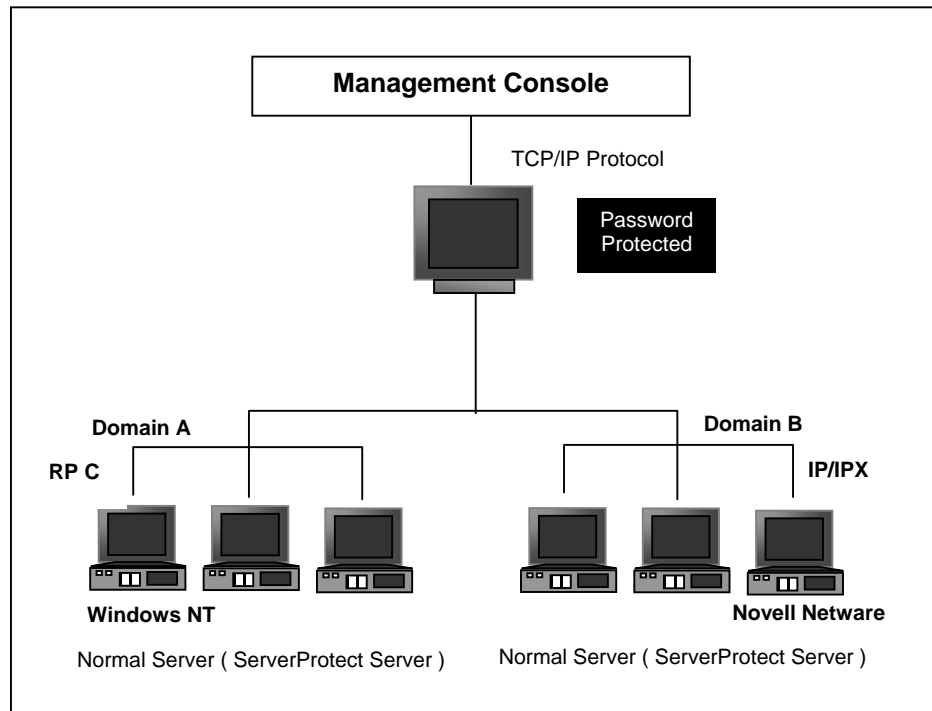
Sampai akhir tahun 1998, virus komputer masih berkembang secara umum melalui floppy disk, masih lamban dan prosesnya bisa diprediksi.

Dengan munculnya virus-virus baru setiap harinya, membuktikan bahwa isu tentang virus tidak akan hilang begitu saja dalam waktu yang cepat. Pada kenyataannya, survey tahunan *IC5A* sejak tahun 1995 menunjukkan bahwa masalahnya telah menjadi lebih buruk. Lebih dari 99% perusahaan yang disurvei melaporkan satu virus setiap 2000, sementara hampir 67% mengalami masalah penyimpanan dan 40% mengalami kehilangan data karena serangan virus. Sebagian besar perusahaan diperkirakan mengalami kerugian karena serangan virus setiap tahunnya antara \$ 100,000 dan US \$ 1,000,000. Sebuah laporan menyimpulkan bahwa perusahaan-perusahaan menghadapi resiko "bencana virus" yang lebih besar dibanding sebelumnya beroperasi bertentangan dengan keinginan pengguna, memasukkan jiplakannya sendiri ke dalam file-file yang beraneka ragam dan membawa sebuah "payload" dengan perintah-perintah yang merusak, Sektor boot yang sederhana dan file virus yang merupakan hal umum pada satu dekade dulu telah berkembang menjadi keturunan yang baru : seperti virus polymorphic, yang merubah kode mereka untuk menghindari deteksi, cacing yang dapat menjiplak dan berkembang melalui jaringan tanpa mempengaruhi file.

1.2. Solusi Terhadap Ancaman Virus

1.2.1 ServerProtect's Three-Tiered Architecture

Solusi ServerProtect for NAS dibuat berdasarkan versi asli dari ServerProtect untuk Windows NT/2000 dan Novell Netware file server. Sebagai sebuah server berdasarkan solusi antivirus komersial pertama, ServerProtect memiliki rancangan yang modern untuk menyediakan proteksi paling efektif.



Gb. 1 . Original ServerProtect aritecture

ServerProtect dibuat untuk melindungi server dan bidang yang banyak mulai dari virus pada saat instalasi dan mengatur dari sebuah console yang aman. Beroperasi melalui sebuah rancangan three-tier(tiga rangkaian) terdiri atas Management Console, Information Server, dan Normal Server. Administrator dapat menggunakan Management Console untuk membentuk Information Server (IS), yang pada gilirannya mengontrol Normal Server di bidang IS. Tiga rangkaian tersebut berdiri sendiri satu sama lain, dan semua dapat diinstal pada mesin yang sama, mesin yang terpisah-pisah, atau kombinasi keduanya.

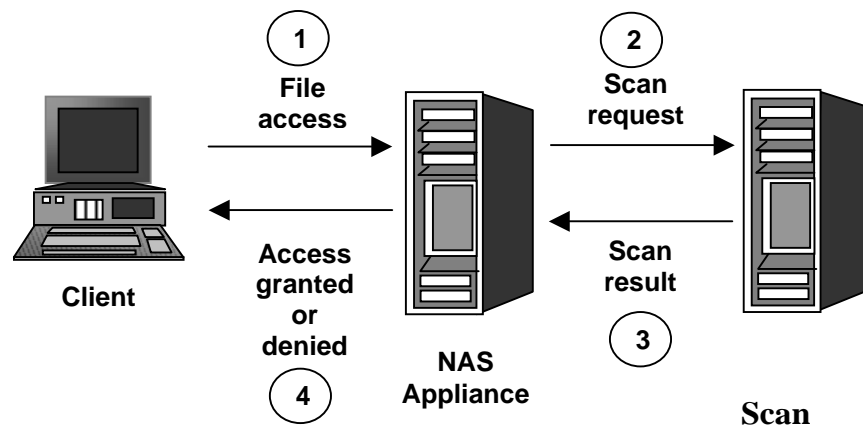
Management Console merupakan suatu console yang portable yang memungkinkan pengontrolan terpusat dari server jaringan dan bidang yang

banyak. Ini menunjukkan status semua server ServerProtect, memungkinkan konfigurasi yang simultan dari server pada bidang IS yang sama, dan menghasilkan laporan kejadian virus yang terintegrasi untuk semua server. Console dapat diinstal pada semua Win32.

Information Server merupakan suatu penghubung komunikasi untuk mengkoordinasikan aktivitas pertahanan antivirus di dalam bidangnya. Sebuah Information Server (IS) menyediakan single point untuk semua Normal Server yang ditentukan - menghemat waktu dan mengurangi beban pekerjaan pada administrator dengan membuatnya tidak perlu berkomunikasi secara langsung dengan setiap Normal Server. Di dalam pekerjaan dengan banyak Normal Server, administrator membagi sejumlah Normal Server di antara IS yang banyak untuk mengurangi beban pada setiap IS.

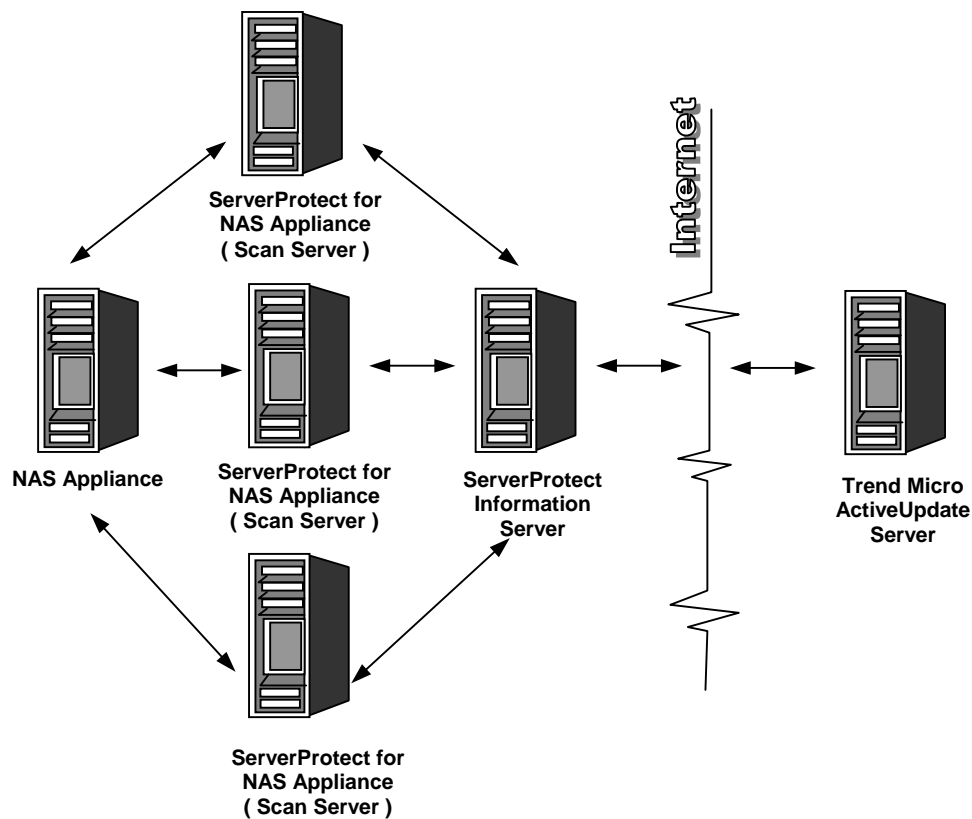
1.2.2 Rancangan Server Protect for NAS

ServerProtect for NAS menggunakan rancangan tiga rangkaian dari ServerProtect untuk melindungi penyimpanan data pada alat penyimpanan yang terhubung. Pada ServerProtect for NAS, Normal Server dikenal sebagai Scan Server. Scanner antivirus itu sendiri diinstal pada Windows NT atau server Windows 2000, file yang disimpan di dalam NAS dibaca berdasarkan akses. Melalui penggunaan remote procedure calls (RPC), sebuah application program interface (API) yang sederhana atau sebuah lightweight protocol, ServerProtect for NAS bekerja dengan alat network attached storage melalui jaringan, apapun platformnya.



Gb. 2. Virus Scanning Work Flow of serverProtect for NAS

Pada saat klien pengguna mencoba mengakses sebuah file pada alat penyimpanan, atau menyimpan sebuah file baru atau modifikasi, pengecekan virus terjadi. Jika nama file ekstensi muncul pada sebuah daftar tipe file yang sudah ditentukan sebelumnya, yang dapat dibentuk oleh Administrator, alat NAS memberitahu salah satu Scan Server yang terdaftar dan menyediakan jalan ke file untuk discan. ServerProtect lalu membuka suatu hubungan ke file, membaca virus yang dikenal dan tidak dikenal, dan memberitahu hasilnya pada solusi NAS. Jika tidak ada virus yang ditemukan, pengguna diizinkan untuk membuka file. Jika sebuah virus ditemukan, ServerProtect mengambil tindakan pada file berdasarkan salah satu settingnya, yang dibentuk oleh administrator. Umumnya, ServerProtect akan dibuat baik untuk "Karantina" atau "Membersihkan" file yang terinfeksi. Jika file dikarantina, pengguna ditolak mengakses dan administrator harus mengambil tindakan. Jika file dibersihkan, kode virus dipindahkan dan aplikasi NAS diberitahu, setelah pengguna diizinkan untuk mengakses file yang sekarang bersih. Jika percobaan untuk membersihkan file tidak memungkinkan atau tidak berhasil, ServerProtect lalu akan mengkarantina file dan pengguna ditolak mengakses.



Gb. 3. ServerProtect for NAS offers automatic updating and load balancing between multiple Scan Server

1.3 Bentuk dan Keuntungan NAS Solutions Virus Scanning Protects Data Integrity

1.3.1 Updating Otomatis

Sebuah scanner virus hanya efektif dengan update terakhirnya. ServerProtect for NAS dapat dibentuk untuk mendownload pola-pola virus terakhir secara otomatis dan membaca mesin update dari Trend Micro's ActiveUpdate server dan membagikannya ke Scan Server yang ditentukan. Untuk mengurangi waktu download dan melindungi jaringan, pendistribusian ke server yang ditentukan dilakukan melalui sebuah mekanisme update tambahan, yang mengharuskan bahwa ServerProtect for

NAS hanya mendownload virus terakhir yang harus ditambahkan sejak update terakhir.

1.3.2 Manajemen terpusat melalui Rancangan Tiga Rangkaian

ServerProtect Information Server menyediakan manajemen sederhana Windows NT Scan Server dari sebuah console manajemen portable. Scan Server yang banyak dapat dikelompokkan ke dalam sebuah bidang yang logis. Disarankan untuk menyimpan Scan Server untuk satu alat NAS ke dalam satu bidang.

Manajemen console ServerProtect memungkinkan para administrator membentuk semua server di dalam bidang yang sama secara simultan, dan menghasilkan laporan kejadian virus yang terintegrasi dari semua Scan Server. Hal ini mengkonsolidasikan tindakan yang dapat diambil terhadap file-file yang terinfeksi

Information Server memungkinkan pengguna untuk menjalankan tindakan yang dapat dijalankan oleh Scan Server pada sebuah file yang terinfeksi, Pilihan-pilihan yang mungkin termasuk karantina file yang terinfeksi, membersihkan virus dengan atau tanpa backup, atau membatalkan file yang terinfeksi.

1.3.3 Scalability dan High Performance

Untuk menambah scalability dan menambah tingkat tampilan, multiple ServerProtect Scan Servers dapat didaftarkan dengan alat-alat NAS setiap saat. Penambahan jumlah Scan Servers yang didaftar akan menambah tampilan scan. Pada saat ServerProtect Scan Server terdaftar pada alat NAS, hubungan dan penghubungan antara server dan alat NAS terbentuk secara otomatis. Kapan saja server mendeteksi setiap putusnya komunikasi, ini akan mengirimkan sinyal ke alat NAS untuk menghubungkan kembali. Hal ini memungkinkan administrator IT merawat dengan mudah efek keamanan dengan cara benar-benar terbuka terhadap pengguna jaringan.

1.3.4 Comprehensive Log Reports

ServerProtect for NAS menyediakan laporan log yang komprehensif untuk memungkinkan pengguna melacak dan mengatur sejumlah kejadian-kejadian antivirus termasuk infeksi virus, pola atau program update, waspada terhadap virus, menjalankan tugas-tugas, aktivitas scan, dan modifikasi dari sebuah console yang sederhana. Hal ini menyederhanakan tugas-tugas manajemen antivirus dan konfigurasi produk untuk administrator sambil menyediakan audit dan informasi aktivitas.

2. Keamanan Pada Network Attached Storage (NAS)

Namun, bagaimanakah manajer file mengkomunikasikan keputusan akses terhadap *drive* dengan cara yang sederhana, aman dan efisien? Secara singkat, kapabilitas merupakan tiket yang menjamin kualitas akses. Tidak seperti mekanisme kemampuan/kapabilitas klasik, kita tidak dapat bergantung pada seluruh inti yang dipercaya untuk mengelola keamanan sistem dalam jaringan yang saling bertentangan, Begitu juga kita tidak dapat menggunakan satu mesin saja untuk mendukung kapabilitas tersebut. Sistem ini akan beroperasi dalam lingkungan yang secara potensial saling bertentangan dengan lawan yang mampu menyadap lalu lintas jaringan dan mentransmisikan pesan yang tidak teratur di dalam jaringan.

Disini digunakan kapabilitas kriptografik yang digunakan oleh manajer file dan diperiksa oleh *drive* dengan support hardware minimal. Pemisahan antara kapabilitas yang dikeluarkan dan yang di-verifikasi memungkinkan kita untuk memisahkan penyimpanan file dari manajemen file ini haruslah dilakukan oleh mesin yang dipisahkan dengan jarak dan hanya dengan komunikasi tidak langsung : kontrol hak akses dikelola melalui informasi *kriptografik* yang di simpan dalam kapabilitas. Kapabilitas ini dipresentasikan oleh klien ketika mencoba mengakses *disk drive*.

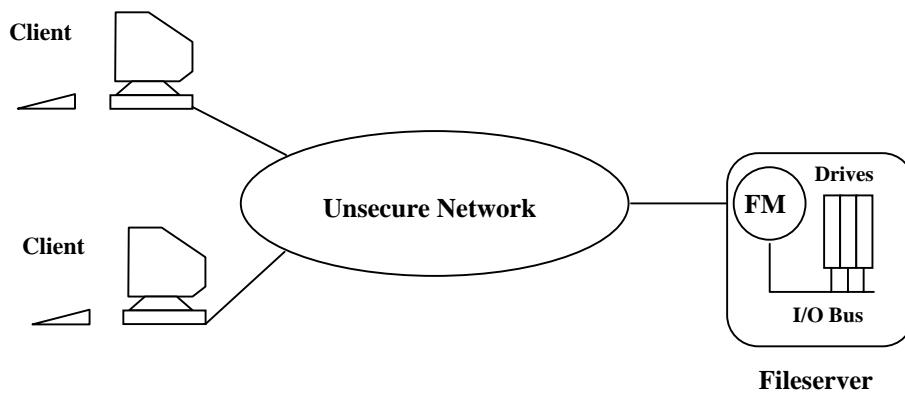
Rancangan ini memperkenalkan sejumlah kesempatan yang menarik. Di sini terdapat dua aplikasi yang telah mutakhir : yang memungkinkan sistem file multiple (berganda) untuk "build on top" pada interface *drive* yang sama ; dan

menyimpan *drive* dalam lingkungan yang aman secara non-fisik.

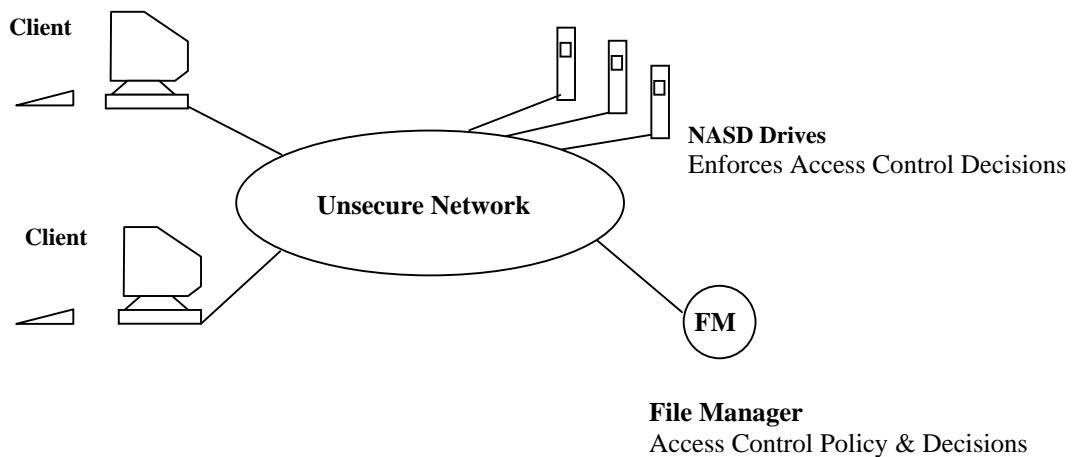
2.1 Interface *drive* independen sistem file

Sistem file yang didistribusikan secara klasikal diterapkan melalui satu atau lebih file *server* yang mempresentasikan interface sistem file tertentu yang didistribusikan kepada user (pengguna). Kebebasan sistem file dari interface memungkinkannya untuk digunakan untuk membangun sistem file tingkat tinggi yang menyajikan interface dan masih menggunakan berbagai sistem file di atas interface. Sebagai contoh, kita dapat membuat *striping server* yang mengeluarkan interface NASD ketika membuka data atas sekelompok *drive* NASD. Dari persepektif sistem file dan penggunaan (user), mereka berinteraksi dengan *drive* NASD ketika secara aktual mereka berinteraksi dengan *striping server* dan sekelompok *drive* NASD.

Perhatikan pilihan bagi implementor pada perangkat penyimpanan yang melekat pada jaringan. Penyimpanan yang ada dan sistem file yang didistribusikan berada dalam bentuk yang beragam. Namun, seluruh sistem file memiliki kelebihan dan kelemahan yang bervariasi tergantung pada lingkungan dan aplikasi. Dengan memungkinkan sejumlah sistem file untuk dibangun pada NASD, kami memungkinkan pemilihan sistem file terbaik untuk beragam pekerjaan dan memungkinkan dilakukannya pengembangan di masa yang akan datang sementara menggunakan *drive* NASD yang sama.



Gb. 4. Classical distributed file system structure



Gb. 5. NASD distributed file system structure

2.2 Disk Tanpa Pengamanan Fisik

NASD mempresentasikan kepada kita sebuah peluang untuk menggunakan *disk drive* yang dapat disimpan pada lokasi yang dapat diakses atau semi-dapat diakses (semi-accessible). Dalam sistem file yang terdistribusi secara klasik, pihak lawan dapat mencoba mencuri informasi dengan pertama-tama meminta supaya sistem file terdistribusi yang kita miliki untuk diamankan secara fisik : dengan akses yang hanya dapat dilakukan oleh seseorang yang terpercaya.

Dalam lingkungan kerja modern, sebagai contoh kantor kecil atau

lingkungan rumah, persyaratan ini nampak sulit untuk dipenuhi. Dengan penyebaran situs WWW kecil, kita sering melihat html, ftp, dan file *server* digunakan di kantor rumah atau lingkungan lainnya yang nampak tidak aman dimana akses fisik yang berbahaya terhadap *disk drive* mungkin saja terjadi.

Untuk *drive* yang aman secara fisik, kita dapat menggunakan struktur NASD untuk menerapkan "*end-to-end encrypsi*" antara klien dan *drive*. Untuk permasalahan *drive* yang lebih menantang yang tidak aman secara fisik, kami mengusulkan untuk menggunakan sejumlah kecil hardware tahan panas (*temper-resistant*) dalam *drive* NASD. Hardware ini dapat secara aman menyimpan kunci-kunci yang digunakan untuk melakukan *encrypsi* file ketika kunci-kunci ini disimpan dan dipanggil kembali, tanpa resiko terkuak (*bocor*)_walaupun jika diserang secara fisik. Seluruh *encrypsi*, *decrypsi* dan *re-encrypsi* pada *drive* dilaksanakan dalam hardware *temper-resistant*. Terlebih lagi, dikarenakan mekanisme kapabilitas kita yang efisien, tidak ada intervensi file manager yang diperlukan untuk sebagian besar akses. Jadi, sistem kita akan aman, scalable, dan terdistribusi dengan luas.

2.3 Pilihan Hardware Pengaman

Konfigurasi *drive* NASD yang berbeda akan menyajikan jaminan keamanan yang berbeda pula bagi pengguna (*user*). Disini disajikan beberapa contoh :

- Sebuah *drive* dapat menyajikan autentikasi saja pada porsi kontrol pesan dan tidak memproteksi porsi permintaan data. Pihak lawan yang mampu memodifikasi paket dalam transit dapat memodifikasi data yang dilihat oleh klien atau *drive* dengan berpura-pura berperan sebagai "perantara"
- Sebuah *drive* tidak dapat menyediakan privasi bagi operasi pengguna. Malahan, *drive* hanya dapat mem-validasi integritas operasi. Dengan pendekatan ini, pihak lawan dapat mengawasi data yang ditransmisikan dalam jaringan, namun tidak dapat memodifikasi atau memalsukan permintaan. Sistem file terdistribusi yang berada pada lapisan atas NASD dapat menyediakan privasi dengan menyimpan data yang di-

encrypsi pada NASD dan menggunakan manajemen kuncinya sendiri untuk melakukan sharing (berbagi) informasi.

2.4 Kunci Hierarkhi

NASD menggunakan suatu hirarki empat macam kunci: kunci induk (MasterKey), kunci pengarah (DriveKey), kunci sekat (PartionKeyN dan kunci kerja (KbN hitam dan emas KgN)

MasterKey: Suatu pengurus menggunakan kunci induk untuk mengendalikan hirarki kunci dan tugas administratif lain. Masterkey adalah suatu kunci abadi/kekal sangat harus digunakan dan dilindungi.

Bila menggunakan MasterKey seorang pengurus dapat menetapkan DriveKey.

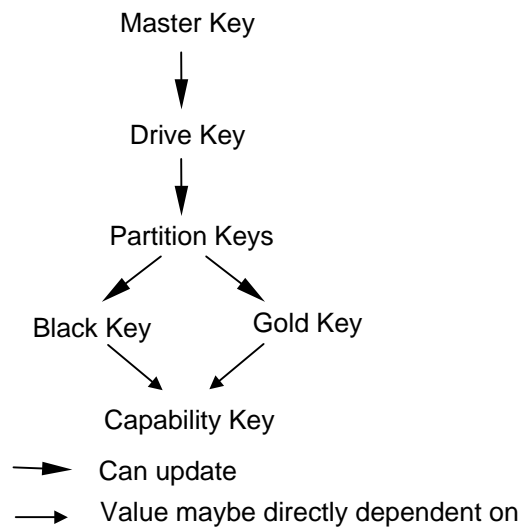
DriveKey: Drivekey mengatur partioning kapasitas drive dan dapat menyeting pengaturan sekat dan PartitionKeys.

PartitionKeyN: File manajer menggunakan PartitionKeys untuk mengatur partition dan untuk menetapkan WorkingKeys yang paling sering digunakan untuk operasi file manajer dan drive

WorkingKey: Manajer File menggunakan WorkingKeys untuk menghasilkan kapabilitas. Setiap drive memelihara dua workingkeys per partition

File manager dapat akses klien untuk menyimpan dan menyediakan klien dengan kapabilitas untuk mengakses objek, dengan menampilkan kapabilitas ke drive dan menggunakan sebuah pesan kunci permintaan. Klien dapat menyakinkan drive bahwa operasi diijinkan.

Kunci NASD dan mekanisme kapabilitas menggolongkan *file-drive* autentifikasi dan *client-drive* autentifikasi. Autentifikasi masih diperlukan tetapi metode yang tepat untuk melakukannya hanya desainer *file system*.



Gb. 6. Key Hierarchy Relationships

Master key

Master key tidak selalu dalam kondisi online dan tidak akan pernah menjadi pembuka untuk file manager. Kita harus juga membatasi jumlah dari text encrypted atau yang akan dicerna oleh master key. Master key digunakan untuk merubah drive key.

Master key digunakan untuk menset drive key ketika :

- Drive key dikenal atau diharapkan disetujui
- Kegagalan yang disebabkan oleh file manager dan pergerakan yang mengakibatkan perbedaan nilai pada Drive Key
- Tidak sering merubah key , dibuat jadwal untuk menjaga keamanan

Untuk merubah Drive Key harus mengikuti petunjuk **SetDriveKey**

UseMasterKey, ProtectionOptions, {}, SetDriveKey, NewKey, RequestN once, RequestDigest where *ProtectionOptions* \supseteq {**Integrity args, IntegrityData, PrivacyData**}

Master Key secara hirarkhi mengharapkan operasi yang sama untuk key yang lain.

Partition Key

Partition key umumnya digunakan untuk merubah kerja kunci-kunci yang disimpan didalam file manager, dan menjadikan yang disetujui. Persetujuan dari file manager akan menjadikan sumber yang terbuka dari penjagaan drive oleh partition key. Pemakaian hardware tergantung bagaimana kita dapat meminimalkan resiko pada key dengan pengamanan jaringan coprosesor pada file manager untuk melindungi partition key.

WorkingKey

DriveKey biasanya tidak didalam file manager, hal itu untuk membantu mengisolasi keamanan dari perbedaan file manager dan tidak dapat merubah PartitionKey untuk diperbaharui. Kunci ini harus dapat mengatur pergantian dan batas yang terbuka dari sebuah kunci. Kunci diperlukan untuk merubah secara umum terhadap motivasi penambahan dari kerjanya key secara hirarki.

WorkingKey untuk partisi N adalah Kunci warna Hitam (Kb_n) dan kunci warna emas (K₉_n). Kunci hitam dan emas dirubah dengan SetBlackWorkingKey N dan SetGoldWorkingKey N melalui pesan (sama dengan pesan SetDriveKey) sesuai interval yang dibutuhkan oleh file manager.

Jika hanya sebagai pemeliharaan SingleWorkingKey untuk setiap pembaharuan, key akan bekerja secara otomatis memperbaiki semua yang tidak benar. Dua workingkey untuk menghindari bagian yang cacat sebab file manager pada tahap berikutnya melepaskan workingkey yang telah usang dari kemampuan yang ada dengan workingkey yang baru.

KeyProtection

Sesungguhnya pengamanan kunci-kunci adalah merupakan pusat dari pengamanan perawatan dari system yang ada, batasan tingkat pengamanan dapat dicapai dengan penempatan drive dan file manager secara fisik dengan akses pengontrolan untuk pengamanan fasilitas, untuk mengikat pengamanan selanjutnya dengan menggunakan pengamanan coprosesor pada file manager dan drive pada penampilan key manajemen.

3. Kesimpulan

NASD Arsitektur adalah suatu pendekatan inovatif kepada permasalahan dari penampilan tinggi dan hemat biaya I/O berdasar pada Network Attached Storage System. Dengan menyediakan keamanan Network Attached Storage System memungkinkan klien untuk mendapatkan tampilan yang potensial dan skalabilas yang bermanfaat dalam Network Attached Storage System tanpa merugikan keamanan data mereka.

Inti sari skema kapabilitas ini adalah encapsulation bearer's mengakses dengan benar pada versi tertentu suatu obyek dengan menggunakan suatu kunci rahasia membagi bersama dengan capability issuer (manajer file) dan capability enforcer (NASD drive). Sesungguhnya, kunci yang rahasia adalah satu permanen dan 4 buah kunci yang membentuk suatu hirarki kunci. kunci dapat digunakan untuk penarikan kembali kapabilitas akses saat NASD menolak.

DAFTAR PUSTAKA

- [1] Howard Gobioff, Garth Gibson, Doug Tygar “ *Security for Network Attached Storage Devices*, October 23,1997, School of Computer Science, Carnegie Mellon University, Pittsburgh, PA 15213 .
- [2] Trend Micro,WP *Securing Data in Network Attached Storage (NAS) Environments: ServerProtec for NAS*, Cuperrtino, CA 95014.
- [3] Datalink, *NAS Device Backup Solutions*, April 5, 2002, Rev 2.