

Teknologi dan Privacy Data Web User

Oleh :

Janner Simarmata, ST., M.Kom

sijanner@yahoo.com

www.simarmata.org

www.kaputama.ac.id

*Dipublikasikan dan didedikasikan
untuk perkembangan pendidikan di Indonesia melalui*

MateriKuliah.Com

Lisensi Pemakaian Artikel:

*Seluruh artikel di **MateriKuliah.Com** dapat digunakan, dimodifikasi dan disebarkan secara bebas untuk tujuan bukan komersial (nonprofit), dengan syarat tidak menghapus atau merubah atribut Penulis. Hak Atas Kekayaan Intelektual setiap artikel di **MateriKuliah.Com** adalah milik Penulis masing-masing, dan mereka bersedia membagikan karya mereka semata-mata untuk perkembangan pendidikan di Indonesia. **MateriKuliah.Com** sangat berterima kasih untuk setiap artikel yang sudah Penulis kirimkan.*

Survei Resiko dan Tindakan Balasan

Penulis menguji keleluasaan resiko *privacy* untuk pengguna data pada lingkungan Web dan mengeksplorasi karakteristik dan aturan dari tindakan balasan teknis, termasuk mekanisme penyajian kebijakan *privacy*, fasilitas nama samaran, metoda *access-control*, dan metoda teknis untuk membatasi penggunaan data.

Peningkatan sejumlah user memberikan *personally identifiable information* (PII) situs web mereka, seperti username, alamat email, pola akses, minat, dan informasi lokasi. Secara paralel, para user khawatir terhadap seseorang yang mungkin akan memperoleh data user yang sensitif untuk tujuan yang tidak diharapkan dan yang tidak diinginkan oleh seseorang yang datanya akan dibebaskan ke orang lain. Penelitian AT&T menemukan bahwa 87 persen dari sample user adalah "seluruh atau sebagian mengenai ancaman terhadap *privacy* seseorang adalah ketika saat mereka online."¹

Para user menginginkan kontrol tersebut melalui:

- apakah para pengamat dapat melihat elemen lingkungan browsing mereka,
- situs di mana interaksi mereka menjadi kelihatan,
- berbagi informasi dengan situs yang mereka kunjungi, dan
- bagaimana mereka menggumpulkan atau berbagi PII yang mungkin bisa digunakan bersama.

Seperti halnya dengan keamanan, ini adalah sulit untuk menyeimbangkan *privacy* user dengan fitur kenyamanan yang baru. Teknologi yang dapat mendukung browsing yang nyaman juga membawa resiko pada data *privacy* user. Secara kebetulan, pada saat sekarang muncul teknologi yang menawarkan tentang *privacy*, seperti:

- Penyajian kebijakan *privacy* yang telah dirancang untuk proses otomatis, seperti *World Wide Web Consortium* (W3C), *Platform for Privacy Preferences* (P3P; www.w3.org),
- Fasilitas *pseudonym* (penetapan format pengenalan yang tidak bisa secara langsung dihubungkan ke perorangan) guna membatasi akses untuk identitas user dan korelasi data antar situs,
- Metoda *authorization* (seperti XACML) dan kontrol *rights-management*. Walaupun beberapa hal ini pada awalnya dirancang untuk mencukupi kebutuhan yang beda dari *privacy*, mereka menawarkan tool yang dapat mendukung proteksi *privacy*; dan
- Teknik pengukuran untuk mengontrol penggunaan data dan inferensi seseorang dapat tergambarkan dari hal ini.

Karakteristik elemen-elemen ini dan batasan akses data dan penggunaan hak dengan cara yang berbeda, sudah dikembangkan pada komunitas yang berbeda, dan alamat yang berbeda tetapi aspek overlap dari masalah. Di dalam artikel ini, kita mendiskusikan teknologi dan aturannya dalam mengatur *privacy* data user

yang relevan. Yang pada hakekatnya, nilai dari metoda teknis tergantung pada ketepatan implementasi, praktis operasionalnya, dan user interface; bidang ini bukanlah topik yang utama dari artikel ini. Prakarsa legislatif, seperti US *Health Insurance Portability and Accountability Act* (HIPAA), adalah juga faktor penting yang memotivasi dan mendukung perlindungan *privacy*, tetapi kebohongannya berada di luar lingkup materi ini.

Data Dilema

PII sering tidak praktis atau mustahil untuk menyelidiki kembali dan mengingat dari yang tidak diharapkan penerima. Dengan begitu, ukuran proteksi untuk mencegah penyingkapan yang tidak diinginkan menjadi kritis. Walaupun suatu studi terakhir menyarankan suatu trend tambahan bahwa situs adalah mengumpulkan PII yang dipilih dan menyediakan kontrol user yang lebih baik, proteksi data penting yang tersisa². Berbagi PII dengan situs adalah sangat menyenangkan sebab tak perlu untuk memasukkan ulang informasi pada kunjungan yang secara berurutan. Ini juga meningkatkan kesempatan bahwa data akan diekspos, yang mana pada gilirannya, terjadi penambahan resiko *privacy* dan prospek pencurian identitas. Para user menginginkan untuk mempertahankan kepemilikan PII dan melakukan sharing secara selektif, tetapi situs mungkin akan mempertimbangkan aset bisnis ini. Penentuan kebijakan *privacy* adalah suatu aturan yang penting di dalam menggambarkan batasan-batasan hubungan antara user dan situs.

Distribusi dari data individual ke berbagai tempat penyimpanan atau di bawah identitas yang berbeda dapat membantu dalam pengisian dan membagi aspek yang berbeda dari suatu *personal online individu*. Seorang user bisa jadi lebih senang untuk menyatakan PII tentang aktivitas atau ketertarikan pada situs yang berbeda dibandingkan penyingkapan semua informasi pada situs tunggal. Selanjutnya, seorang user ingin membuat kunjungan tersembunyi guna tujuan pribadi dari yang dibuat ini dimana bertindak sebagai seorang pegawai. Yang sialnya adalah, memberi akses cukup untuk data user dan korelasi berdasar pada karakteristik umum seperti alamat, pengenalan, dan pola pemakaian, berbagai situs mampu mengintegrasikan sharing informasi mereka dan memperoleh suatu gambaran yang lebih luas dari suatu PII individu dibandingkan dengan setiap situs orang dikumpulkan sendiri. Perhatian ini memotivasi kontrol pada sharing data yang dikumpulkan dan ukuran untuk mencegah korelasi identitas pemakai yang tidak sah dengan *colluding sites*. Ini adalah penting untuk menawarkan perlindungan dengan suatu cara yang biasa user temukan sehingga dapat dipakai dan dapat dimengerti.

Aspek Privacy Interaksi Web

Seringkali, kemampuan dan implementasi membawa presentasi dan perancangan situs lebih dari yang berhubungan dengan *privacy*. Faktor ini, dikombinasikan dengan pemasaran dan minat komersil, membiarkan teknologi yang merugikan *privacy* guna memperoleh adopsi yang tersebar luas. Standar *Secure Sockets Layer* (SSL, basis untuk *Internet Transport Layer Security* yang sekarang [TLS; www.ietf.org/rfc/rfc2246.txt])³ enkripsi sekarang pada umumnya, tidak melindungi data user dari *privacy* pada situs yang mereka akses.

HTTP

HTTP didefinisikan sebagai dasar komunikasi antara browser dan situs web. HTTP adalah suatu *stateless protocol*: masing-masing permintaan diproses secara independent berdasarkan prioritas permintaan; fitur *state management* menetapkan konteks antar permintaan-terutama *cookies* (yang akan dibahas kemudian)-pada umumnya dioperasikan bersama dengan HTTP. Meskipun begitu, HTTP requests individu membawa item data tertentu yang bisa digunakan untuk menemukan atau menghubungkannya dengan permintaan yang berikutnya.

Spesifikasi HTTP/1.1 (www.ietf.org/rfc/rfc2616.txt) mengidentifikasi beberapa *header fields* dengan karakteristik *privacy-sensitive* yang menjamin keabsahan browser' dalam memilih kontrol pada informasi yang dilepaskan (*released*)

- Field **Form**, jika mengirim, membawa suatu pengaksesan alamat email user. Bagian spesifikasi HTTP bahwa fieldnya tidak dikirim tanpa persetujuan user.
- Field **Referer** yang menyediakan suatu situs yang telah dikunjungi dengan URL dari halaman sebelumnya yang telah dikunjungi, dengan mengabaikan apakah situs tersebut sama dengan halaman yang diminta. Sebagai hasilnya, ketika ditampilkan link pada image pada situs yang lain, penyedia image dapat mengidentifikasi halaman yang menyebabkan image menjadi *reference*.
- Field header **Accept-Language**, dimaksudkan untuk mengijinkan penggunaan *content tailoring*, yang dapat menyediakan kesimpulan tentang suatu permintaan *user's national* atau keanggotaan *ethnic*.

Lagipula, sumber alamat host tersedia sebagai bagian dari suatu HTTP request, bersama dengan item data lain yang menggambarkan host, sistem operasi, dan jenis browser dan konfigurasinya. Memberikan unsur-unsur ini, adalah sering secara langsung untuk situs untuk menentukan (paling tidak dengan kemungkinan yang tinggi) bahwa akses yang berbeda dihubungkan dengan yang lainnya.

Cookies

Hari ini, *cookies* web menjadi mekanisme yang paling umum digunakan untuk menyediakan semantik *state-management* untuk interaksi Web.⁴ Mereka tidak hanya

dimaksudkan untuk memenuhi tujuan ini, tetapi penawaran ini adalah suatu hal yang menyenangkan, lebih fleksibel, dan metoda yang bersifat umum. Sekali komputer user menerima dan menyimpan suatu *cookies*, ini dikembalikan ke domain asalnya selama HTTP yang berikutnya mentransfer domain. *Cookie issuers* mempunyai beberapa fleksibilitas di dalam lingkup *tailoring* dari hosts yang mana *cookie* akan dikembalikan, tetapi bagian kunci dari mekanisme memastikan bahwa *cookie* yang dikeluarkan oleh host tidak akan dikembalikan pada host pada domain yang tidak berhubungan.

Ketika *cookies* menjadi masalah situs, mereka dapat mengendalikan *persistence*nya, yang biasanya jangkauannya dari beberapa menit ke tahun atau pada durasi suatu sesi browser. Secara normal, level *sesi-cookies* terletak pada browser memori, ketika *cookies* lama berdiam dan disimpan di dalam file. *Cookies* menyediakan dukungan yang nyaman untuk multistep transaksi web (seperti ketika penjual *online* menambahkan unsur-unsur pada suatu *virtual shopping cart*) dan menyederhanakan akses pada layanan *subscription-base*.

Cookies juga berharga untuk operator situs web yang menentukan berapa banyak user yang mengunjungi situs yang berbeda dan untuk menjejaki browsing behavior user, terutama untuk *cookies* yang lama tinggal secara terus menerus. Kapan saja suatu situs menerima *issued cookie*, ini dapat menentukan bahwa prioritas pengunjung adalah mengakses situs itu kembali.

Pemasang iklan sering menampilkan iklannya pada halaman atas yang mengambil bagian situs yang lain; dengan kata lain, suatu pengunjung dapat berpartisipasi pada situs yang diisyaratkan dengan browser user yang mengunjungi layanan iklan. Dengan diam-diam, menempelkan image "**Web bug**" yang hanya berupa pixel tunggal dan tak kelihatan, yang membiarkan track penyedia image dan berisi data tanpa penjagaan user.

Seringkali, jasa periklanan menyimpan cookie untuk menghubungkan antar user pengunjung situs web yang berbeda dari jasa pemasangan iklan. Ini Dapat menyediakan basis untuk mengumpulkan profil yang menguraikan interaksi subsets penting yang menyangkut Web itu sendiri. Seperti *cookies* "pihak ketiga", yang mana ditempatkan dengan lokasi situs lainnya dari akses user yang jelas, terutama yang penting dari suatu perspektif privacy sebab mereka menyediakan informasi pada situs bahwa user tidak secara langsung diminta untuk mengunjungi, dan sebab itulah mereka menyediakan pengumpulan informasi antar-batasan daerah.

Beberapa browsers awal yang membiarkan user menolak semua *cookies* atau didesak untuk tiap-tiap *cookies* yang datang berikutnya. Bagaimanapun juga, banyak situs web mempercayakan pada *cookies* yang digunakan dan isu juga banyak menggunakan prompt *per-cookie* yang sangat merepotkan, bertentangan dengan

akses untuk content yang diinginkan, atau mengacaukan suatu urutan akses halaman. Kotemporer browsers sering membiarkan user menyatakan pilihan *privacy* mereka lebih fleksibel--mereka dapat menetapkan kontrol untuk menerima *cookies* dari situs yang dipilih, menyediakan pengaturan berdasar pada nilai tempat user pada informasi situs atau kepercayaan pada situs yang sesuai dari penggunaan PII mereka.

Kebijakan Privacy dan P3P

Kebijakan Privacy menjelaskan dan membatasi tindakan dari respon situs web, dan aktivitas W3C'S P3P mencari untuk membuat kebijakan itu dapat diakses secara elektronik.⁵ P3P menggambarkan suatu penyajian untuk kebijakan *privacy* situs yang sesuai untuk proses otomatis, memungkinkan browser untuk menampilkan informasi kebijakan situs dan interseksinya dengan aturan user dan pilihannya. P3P bertujuan untuk membuatnya sedikit penting bagi user untuk membaca dan menginterpretasikan textual kebijakan *privacy* dengan representasi informasi kebijakan dalam bentuk browser atau agen lain dapat memprosesnya atau dilakukan atas namanya, yang menyediakan link pada kebijakan *human-readable* untuk acuan jika dibutuhkan. Yang penting, P3P menyediakan suatu pengkodean kebijakan mekanisme *-not enforcement*; yang bermanfaat dalam menggambarkan dan membatasi pemakaian data situs, tetapi ini penggunaan yang efektif dan memerlukan user untuk percaya bahwa situs beroperasi sejalan dengan kebijakan yang dinyatakan oleh mereka.

P3P menekankan indikator jenis data (sebagai contoh, fisik dan informasi kontak online, demografis, keuangan, kesehatan), jenis pemakaian data (sebagai contoh, di dalam fungsi proses yang sekarang, untuk individu atau analisa pseudonymous atau pengambilan keputusan, untuk telemarketing), dan kelas *data-sharing* (sebagai contoh, di dalam organisasi entitas, atau juga pada organisasi yang lain mungkin sama dalam praktek *sharing privacy*). Kebijakan umum P3P dikodekan sebagai dokumen XML; apalagi, spesifikasi P3P menggambarkan suatu format yang lebih pendek (kebijakan ringkas) dengan suatu lingkup terbatas pada praktis *privacy cookie-related* untuk transfer dengan HTTP headers. P3P tidak membiarkan user untuk menentukan data mana yang dapat disharing atau tidak dengan particular sites atau *user-defined groups of sites*. Sedemikian banyak para user boleh menerapkan P3P-specified usage controls bersama dengan authorization controls yang mengijinkan atau menyangkal akses data ke situs tertentu.

P3P akan memperoleh dukungan dalam browser terbaru dan antar situs web, dan menjadi standar yang paling terkemuka yang menyediakan secara rinci aspek pendukung *privacy*. Internet Explorer 6, sebagai contoh, menginterpretasikan kebijakan P3P secara ringkas, dan suatu situs harus menyajikan suatu kebijakan ringkas sebelum Web browser yang populer ini akan menerima suatu cookie *third-party* ketika default level *privacy*-nya aktif. Penyebaran

dan pengaruh P3P mungkin kelihatan meningkat, bersama dengan kemampuan tool prosesnya. Untuk melengkapi fokus P3P pada kebijakan *privacy* yang mengurus interaksi antara browsing user dan situs web, ini akan sangat menolong untuk menetapkan suatu standar untuk mengkomunikasikan informasi antar situs dan komponen unsur mereka pada transfer PII.

Fasilitas-Fasilitas Pseudonym

Beberapa transaksi web memerlukan beberapa format PII, seperti penagihan kartu kredit atau pengiriman fisik pembelian item. Di dalam konteks di mana jika kita dapat menghilangkan PII, *pseudonyms* dapat menyediakan suatu tindakan balasan penting terhadap korelasi antara identifikasi human user dan pengunjung situs web, atau antar pengunjung pada situs yang berbeda. Hati-hati, pengetahuan user dapat diadopsi dan memasukkannya dengan tepat, atau komponen teknologi dapat mengenerate algoritma dan mengatur mereka. Ada tiga tingkatan identifikasi:

1. *Persistent identifiers* dapat dilacak pada user (menyediakan identifikasi yang hidup di luar jangkauan transaksi tunggal atau interaksi).
2. *Persistent persona identities*, yang merahasiakan hubungan identitas user, tetapi membuatnya mungkin untuk menghubungkan pesan berurutan atau transaksi dari seseorang yang sama. Hak milik ini adalah berguna untuk menyelesaikan interaksi yang berkelanjutan, tetapi mungkin menyimpulkan link yang tidak diinginkan pada individu. Korelasi informasi yang diterima dari berbagai interaksi dengan persona tertentu bisa menyarankan identitas individu yang bersesuaian atau karakteristik lainnya.
3. *Single-Use identifiers*, yang merahasiakan identitas user dan juga membatasi link antar sesuatu yang dilakukan user.

Pada level dua dan tiga, identitas individu yang sesuai dengan persona tidaklah tersedia secara langsung sebagai bagian dari komunikasi biasa, suatu respon otoritas (sebagai contoh, orang dilibatkan di dalam suatu proses pendaftaran awal user) sering mengetahui koresponden mereka. Informasi ini boleh jadi dapat diakses oleh administrator atau sebagai jawaban atas proses yang sah. Jika tidak diinginkan, teknik *cryptographic blind* dapat disatukan ke dalam desain sistem untuk membatasi atau mencegah informasi *provider-held* dari yang sedang digunakan untuk merekonstruksi link antara pseudonym dan identitas human yang dihubungkan. Sama dengan identitas yang dirahasiakan, bagaimanapun juga, adalah mungkin untuk situs guna menghubungkan akses user (dengan beberapa level yang tidak tentu) dengan pengamatan pola kunjungan yang tetap atau hubungan alamat pesan atau berisi pola textual tertentu.

User dapat meningkatkan anonym mereka dengan *routing request* mereka secara tidak langsung melalui suatu layanan anonymisasi, yang akan mereplay pesan melalui satu atau lebih perantara untuk merahasiakan asal mereka. Contoh pendekatan dalam area ini meliputi *anonymizing proxies*, *asynchronous mix networks*, dan *Crowds system*.⁶⁻⁸ Layanan ini bertukar-tukar dalam tingkat teknologi mereka

yang menghalangi kompromi *privacy* dengan layanan operator. Pendekatan ini belum tersebar luas dan umum. Dalam arsitektur di mana suatu otoritas pusat membuktikan keaslian para user dan hasil laporan pada situs lain, otoritas pusat dapat meningkatkan *privacy* dengan pelaporan identitas user pada situs via *pseudonymous handles*.

Kerangka kerja federasi identitas aliansi Liberty⁹ menggunakan pendekatan ini; ketika penyedia identitas melaporkan pengesahan user ke berbagai penyedia layanan, masing-masing menerima suatu nilai berbeda yang mengidentifikasi user pada namespace penyedia layanan. Penyedia layanan individual tidak menerima *no globally meaningful user identifiers*, dan penyedia layanan tidak langsung menentukan apakah sebagian pseudonyms mereka menerima sesuai dengan user yang sama. Dalam beberapa kasus, bagaimanapun juga, hal ini mungkin untuk *colluding providers* guna menghubungkan akses berdasar pada informasi lainnya, sebagai contoh, dengan pengamatan sumber IP address bahwa mereka berturut-turut menerima ketika user melakukan browser mengikuti HTTP yang dialihkan dari satu situs ke situs yang lain.

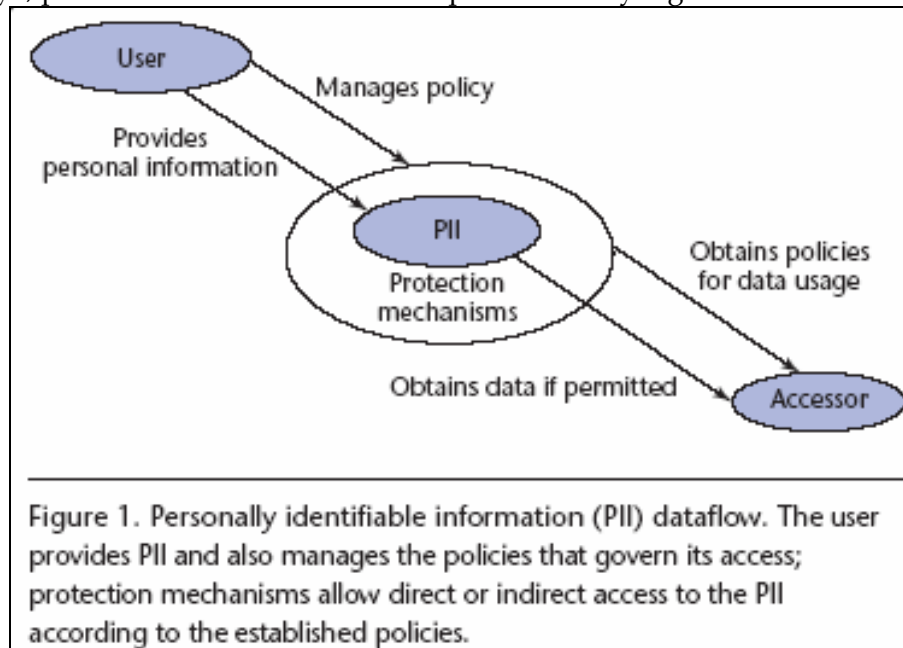
Authorisasi dan Fasilitas-Fasilitas Rights-Management

Ketika user membuat ketersediaan PII pada situs, mereka percaya bahwa teknologi dan administrasi situs tidak untuk penggunaan yang tidak sesuai. Fasilitas sistem operasi yang menengahi akses data mempunyai sejarah yang kaya dan panjang. Pada umumnya, user dan administrator mengarahkan kontrol ini, penyelenggaraan yang berdasar pada identitas yang dibuktikan keasliannya itu semua merupakan permintaan akses. Dalam beberapa sistem, otorisasi digambarkan dalam kaitannya dengan aturan, pemeriksaan, atau kemampuan tidak terikat pada identitas individu. Sebagai suatu kasus khusus dan penting, interface manajemen yang mengontrol *authorization permissions* pada PII harus mereka sendiri sebagai *subject* pada *authorization controls*, maka hanya individu yang sesuai yang dapat mendapatkan ijin itu. Yang terus meningkat, objek data di distribusikan antar jaringan; munculnya protokol untuk mengatur informasi accesscontrol di dalam lingkungan jaringan.

Kita dapat menerapkan teknologi ini untuk menguatkan kebijakan atas nama user, menengahi akses pada informasi user yang sensitif; sehingga, keamanan mereka tersedia yang merupakan komponen dasar *privacy-enabling*. Bagaimanapun juga, jika *access-control* atau *authorization* untuk menguatkan kebijakan yang menggambarkan atas nama kesatuan lain yang dibandingkan dengan user, kehadiran mereka mungkin tidak menambah proteksi *privacy*.

Teknologi *rights-management* yang membatasi spesifikasi penggunaan data, dibandingkan membuatnya tersedia untuk user atau memprosesnya untuk tujuan kewenangan ataupun tidak sama sekali, menghadirkan kembali suatu disiplin lebih baru; yang sekarang ini, banyak pekerjaan kelihatan di dalam area ini yang berhubungan dengan isi komersil hak cipta penyelenggaraan providers. Aplikasi ini

yang pada awalnya kelihatan agak jauh dari perlindungan PII, metoda teknis yang berhubungan secara cepat bisa membantu menengahi penggunaan PII. Suatu koneksi yang mungkin berada dalam prospek teknologi yang melindungi penyimpanan data tertentu dalam sistem dan komponen operator sistem dan, sebagai gantinya, pemesanan kontrol data untuk pemilik data yang beda.



Elemen-Elemen Layanan Autorisasi

Pusat layanan *thrust-authorization* pada *reference monitors*, komponen sistem yang menengahi permintaan akses. Secara umum, layanan otorisasi dipusatkan pada representasi dan menguatkan *decision rules*, dengan karakteristik dari peminta (*requestors*) dan objek yang dilindungi yang berisikan masukan rule tersebut. Sebagai contoh, mereka dapat membatasi situs yang mana PII user bisa disediakan. *Reference monitor* mungkin bisa jadi lokal, yang terdapat di sistem operasi tunggal, atau protokol mungkin mendistribusikan proses mereka antar *policy decision points* (PDP) dan *policy enforcement points* (PEP). Fasilitas otorisasi tergantung pada pengolahan dipercayai oleh *reference monitor* yang terlibat; jika data dibubarkan di bawah kendali dari entitas yang berbeda, bagaimanapun juga, kompromi pada komponen individu tidak menyiratkan kompromi dari semua user yang disimpan PII.

Sangat disayangkan, banyak user kekurangan otoritas atau keahlian untuk mengambil keuntungan penuh dari jasa otorisasi yang menjamin keamanan informasi mereka. Situasi mungkin akan bertambah buruk ketika sistem *identity-management* melingkupi fungsional mereka secara luas untuk mengatur kumpulan *user-attribute* dan lingkup arsitektur mereka ke arah pembagian atribut tersebut antar berbagai tempat penyimpanan. Di dalam suatu lingkungan terdistribusi yang bertambah banyak, adalah mungkin untuk menjadi lebih kuat untuk menyediakan

user dapat mengerti dan kontrol yang efektif pada penggunaan data mereka. Komponen yang berbeda mungkin menyajikan interface manajemen yang berbeda pula pada user, dan rule kebijakan dari unsur-unsur yang berbeda di dalam sistem. Perpaduan manajemen, dapat dimengerti untuk membubarkan PII ke berbagai sistem dan organisasi menghadirkan area penting untuk penyelidikan.

Standar otorisasi bisa menjadi penting sebagai arti untuk mendistribusikan kontrol melalui PII dan penyimpanan data lainnya di dalam suatu *interoperable fashion*. Suatu kandidat mekanisme, *eXtensible Access Control Markup Language* (XACML)¹⁰ aktivitas spesifikasi yang sedang dibincangkan di dalam *Organization for the Advancement of Structured Information Standards* (OASIS; www.oasis-open.org), telah menggambarkan suatu kerangka kerja XML-based untuk menyatakan kebijakan otorisasi. XACML yang juga meliputi suatu fasilitas untuk menyatakan obligasi (sebagai contoh, audit dan notifikasi) penegak yang harus memuaskan dalam konjungsi dengan akses otorisasi mereka.

Hal ini menyediakan suatu sintaks XML-based yang sesuai dengan *access control lists* (ACL), mengidentifikasi subjek, objek, dan akses yang sah pada subjek yang diwariskan kepada objek. Sebagai tambahan terhadap kontrol *identity-based* seperti halnya ACL konvensional, bagaimanapun juga, XACML juga dapat menyatakan kebijakan *rule-based*. Suatu metoda dapat diperluas untuk menyatakan kebijakan berdasar pada kombinasi unsur; operasi *XML-specified* yang dapat melengkapi fungsi *built-in* (sebagai contoh, *set intersection*, *arithmetic*, dan *Boolean operators*).

Dengan penjelasan suatu format pertukaran untuk mengungkapkan kebijakan otorisasi di dalam lingkungan *XML-processing*, XACML dapat membantu mengembangkan arsitektur *distributed-authorization*. Dari perspektif *privacy*, ini juga bisa menguraikan aturan yang mengatur akses ke data sensitif.

Teknologi Rights-Management

Manajemen *metoda digital rights* (DRM) yang secara khas melindungi isi objek, dengan kontrol objek yang menggambarkan penggunaan isi yang diijinkan. Beberapa metoda DRM dikhususkan untuk media tertentu (sebagai contoh, DVD movie), tetapi ini adalah mungkin untuk menyamakan konsep dan menerapkannya secara langsung. Potensi, suatu objek *DRM-protected* bisa membungkus suatu PII user, penerapan metoda DRM pada data yang dimiliki untuk menengahi penggunaan data user yang lain, (*privacy* dari user adalah mengakses *DRMprotected* dan teknologi DRM pada umumnya adalah topik yang penting,¹¹ tetapi tidak difokuskan pada artikel ini.) Semakin bertambahnya tingkat kesulitan teknik DRM dan pertanyaan kebijakan karena penyelenggaraan menyiratkan kehadiran suatu *reference monitor* yang beroperasi atas nama dan minat dari user atau komputer

pribadi. Ini akan menghadirkan model ancaman tantangan yang ekstrim untuk para perancang.

Lagipula, keamanan penyelenggara DRM mencegah pengakses data yang di otorisasi dari transformasi data yang mereka gunakan ke dalam format varian dari batasan DRM, yang menyiratkan kita harus memastikan bahwa banyak operasi *manipulation-data* yang dapat dilakukan hanya di dalam batasan-batasan sistem DRM. Isu ini mempersulit desain sistem DRM dan penyebarannya. Bagaimanapun juga, kita mengembangkan mekanisme yang efektif yang dapat mendukung DRM, kita juga bisa menggunakan mereka untuk melindungi PII user. Khususnya, tingkatan metoda dalam melindungi data terhadap perangkat lunak atau operator yang jahat pada sistem di mana data di *maintenance* dan menjadi tool data-privacy yang penting.

Kemunculan teknologi perangkat keras dan lunak bisa memudahkan pengembangan fasilitas *high-assurance rights-management* dan fitur *security-related*. Sebagai contoh, *Trusted Computing Platform Alliance* (TCPA; www.trustedcomputing.org) yang digambarkan sebagai sekumpulan PC *hardware-based* yang menyediakan integritas yang lebih powerful untuk proses konfigurasi, termasuk implementasi proteksi fungsi *cryptographic* dalam *Trusted Platform Module* (TPM). Pekerjaan berikutnya dalam *Trusted Computing Group* (TCG). Generasi berikutnya dari Microsoft's yang menjamin keamanan yang berbasis komputer(lihat NGSCB'S "*Security Model for the Next-Generation Secure Computing Base*" pada www.microsoft.com) mencari untuk mempekerjakan fasilitas perangkat keras guna melindungi objek *user-space* dari modifikasi, bahkan oleh dengan kode sistem operasi diistimewakan. Kernel security telah menjadi suatu komponen dasar dari metoda desain sistem operasi keamanan sejak awal 1970-an, tetapi aplikasi mereka pada praktek komersil umum yang telah relatif dibatasi.^{12,13} Di dalam NGSCB, suatu format kernel security (yang disebut, di dalam terminologi NGSCB, sebagai *nexus*) secara terpisah ada dari sistem operasi yang tradisional, dan menyediakan suatu lingkungan pelaksanaan proteksi untuk mengawasi proses *nexus computing agent* (NCA).

Inferensi dan Penggunaan Controlling Data

Banyak area teknologi keamanan berhubungan dengan metoda untuk mengontrol sekumpulan dari entitas yang dapat memperoleh akses pada data sensitif. Seperti kebutuhan DRM, tujuan privacy juga menyiratkan kebutuhan akan kontrol tambahan yang memungkinkan akses selektif pada data untuk melaksanakan penunjukan operasi tanpa pembuatan data yang tersedia untuk tujuan lain. Akses *permission-based* pada PII, di dalam proteksi suatu operasi lingkungan eksekusi atas nama pemilik data, secepatnya bisa menyediakan suatu format kontrol privacy. Sebagai contoh, teknologi bisa benar-benar powerful dengan beberapa batasan yang diuraikan di dalam kebijakan privacy P3P.

Beberapa aspek nampak menakutkan. Sekalipun lingkungan eksekusi sesuai, bisa jadi membebani untuk suatu situs untuk memelihara sebagian kejadian *reference monitor* terpisah untuk menguatkan perlindungan dan kebijakan untuk banyak user. Ini adalah tantangan untuk menguraikan suatu proses transaksi situs ke dalam suatu format yang membiarkan suatu modul dipercayai menengahi akses yang secara efektif tanpa menyumbangkan modul yang terlalu kompleks dan besar untuk mengevaluasi dengan tepat. Jika perangkat lunak tidak terpercaya, modul yang dipercayai harus tidak melepaskan PII di luar batasan-batasan nya. Di dalam suatu transaksi yang menyertakan berbagai sistem, sebagai contoh, suatu pengawasan entitas proses dipercayai harus menyediakan dan memasukkan suatu alamat email user yang di enkripsi sebelum sampai pada langkah proses yang lain, untuk mencegah modul tidak dipercayai dalam sistem kepunyaan nya dari ekstraksi data dasar.

Sistem akan menyediakan kunci dekripsi yang diperlukan hanya untuk modul *trusted* yang lain. Lagipula, suatu modul *trusted* harus menentukan apakah suatu permintaan spesifik untuk suatu operasi yang menggunakan PII adalah konsisten dengan batasan pemakaian penempatan pada informasi; ini memerlukan pengetahuan yang menyangkut proses konteks permintaan yang *ditrigger*.

Penelitian yang menyelidiki pengamanan database dan criptografi sedang diusulkan dengan pendekatan yang berbeda untuk menengahi akses data yang sensitip. Orang akan membatasi akses database untuk mengijinkan analisa data yang disimpan tanpa menyatakan PII dan individual yang mewakilinya. Sebagai contoh, kita mungkin mempertimbangkannya untuk bisa diterima guna menyingkap rata-rata pendapatan dari sample 10,000 orang, tetapi bukan untuk satu atau beberapa individu.

Ada beberapa metoda kontrol inferensi jenis sophisticated database.¹⁴ sebagai gantinya, metoda cryptographic yang dapat mendukung keamanan komputasi terdistribusi.¹⁴ Dengan menggunakan teknik ini, data dapat dipecah menjadi element-element dengan entitas dan nilai berbeda yang dapat dikombinasikan atau dibandingkan, tanpa menyatakan informasi dasar ke peserta lain di dalam perhitungannya. Teknik ini tidaklah umum di dalam sistem, tetapi mereka mungkin menjadi blok bangunan penting untuk para perancang dari mekanisme proteksi privacy masa depan.

Elemen-Elemen Proteksi Privacy

Di dalam lingkungan web, komprehensif *privacy* tergantung pada adanya jaminan dalam organisasi di mana data disimpan dan diatur dalam teknologi yang beroperasi pada data. Di dalam dunia teknis, kita memerlukan unsur-unsur yang berbeda untuk mencukupi tujuan yang saling terkait dengan *privacy* yang berbeda; di dalam disain sistem, fungsi ini secara alami didistribusikan dan tidak bisa terlampir secara lengkap di dalam modul *privacy* tunggal. Fungsi sistem operasi itu

memastikan integritas data yang disimpan dan melindunginya dari akses tidak sah adalah kritikal dari proteksi *privacy*, seperti menjadi fasilitas protokol yang dapat menyediakan proteksi ketika data berpindah ke suatu jaringan. Pada gilirannya, fungsi lokal yang tergantung pada trusted perangkat keras dan perangkat lunak sistem; proteksi *cross-network* biasanya didasarkan pada *cryptography*.

Penambahan dimensi proteksi adalah relevan: *privacy policy-based* dan pemakaian batasan kontrol bagaimana data dapat digunakan sekali ketika diperoleh, dan fasilitas pseudonym menyediakan level proteksi terhadap situs yang jahat dengan mengisolasi akses individu dari satu dengan yang lain dan dari individu yang bisa diidentifikasi. Gambar 2 mengilustrasikan hubungan antara fasilitas ini. User mengakses dua situs, masing-masing menerima element dari PII nya, tetapi situs tidak bisa membandingkan identifiers mereka untuk menentukan bahwa PII sesuai dengan user yang sama.

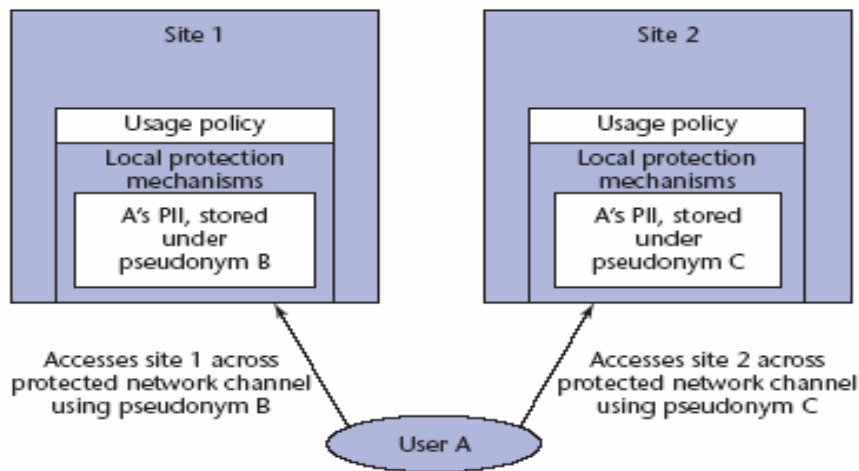


Figure 2. Personally identifiable information (PII) protection model.
(a) User A accesses site 1 across protected network channel using pseudonym B; (b) user A accesses site 2 across protected network channel using pseudonym C.

Selagi berbagai metoda yang kuat dan relevan tersedia untuk melindungi *privacy* user, merupakan tantangan yang penting untuk teknologi dan pengembang standard. Sebagai suatu yang umum, adalah penting untuk membuat kontrol *privacy* yang dapat dimengerti dan tersedia untuk para user. Kebutuhan primer yang lainnya adalah untuk ukuran teknis guna memperkuat proteksi terhadap sekumpulan PII, mengurangi level trust yang harus dilatakan user dalam suatu administrasi situs untuk bertahan pada suatu kebijakan yang diterima.

Sebagai tujuannya, para perancang dapat mencari representasi PII di dalam suatu format sisa proteksi di bawah kontrol user, bahkan ketika hal itu disimpan pada lokasi yang berbeda. Untuk memecahkan masalah ini dalam fashion yang

umum, PII yang manapun harus dirawat oleh suatu monitor kontrol yang mengawasi atas nama user atau mengakses secara tidak langsung menyelenggarakan penggunaan-nya dan inference controls. Pada masa datang, kita mungkin menyesuaikan dan meningkatkan metoda management yang tepat untuk sharing PII di dalam suatu format yang terbatas, membuatnya tersedia hanya untuk user yang ditunjuk. Selagi sebagian dari prospek ini bersifat spekulatif, mereka menghadirkan area penting untuk penyelidikan dan peluang penawaran untuk menyertakan riset yang hasilnya praktis.

References

1. L. Cranor, J. Reagle, and M. Ackerman, *Beyond Concern: Understanding Net Users' Attitudes about Online Privacy*, technical report TR 99.4.3, AT&T Labs-Research, Apr.1999; www.research.att.com/projects/privacystudy.
2. W.F. Adkinson Jr., J.A. Eisenach, and T.M. Lenard, *Privacy Online: A Report on the Information Practices and Policies of Commercial Web Sites*, Progress and Freedom Foundation, 2002; www.pff.org.
3. T. Dierks and C. Allen, "The TLS Protocol, Version 1.0," IETF RFC-2246, Jan. 1999; www.ietf.org/rfc/rfc2246.txt.
4. D. Kristol and L. Montulli, "HTTP State Management Mechanism," IETF RFC 2965, Oct. 2000; www.ietf.org/rfc/rfc2965.txt.
5. W3C, "The Platform for Privacy Preferences 1.0 (P3P1.0) Specification," World Wide Web Consortium Recommendation, 16 Apr. 2002; www.w3.org.
6. C. Gulcu and G. Tsudik, "Mixing Email with Babel," *Proc. ISOC Symp. Network and Distributed System Security*, IEEE Press, 1996, pp. 2-16.
7. S. Parekh, "Prospects for Remailers," *First Monday*, vol. 1, no. 2, 1996; www.firstmonday.dk/issues/issue2/remailers.
8. M.K. Reiter and A.D. Rubin, "Crowds: Anonymity for Web Transactions," *ACM Trans. Info. and System Security*, vol. 1, no. 1, 1998, pp. 66-92.
9. "Liberty ID-FF Architecture Overview, Version 1.2," T.Wason, ed., 2004; www.projectliberty.org.
10. Extensible Access Control Markup Language TC, "eXtensible Access Control Markup Language (XACML) Version 1.1," S. Godik and T. Moses, eds., Organization for the Advancement of Structured Information Standards, Aug. 2003; www.oasis-open.org.
11. J. Feigenbaum et al., "Privacy Engineering in Digital Rights Management Systems," *Proc., 2001 ACM Workshop on Security and Privacy in Digital Rights Management*, LNCS 2320, Springer, 2002, pp. 76-105.
12. S.R. Ames, M. Gasser, and R.R. Schell, "Security Kernel Design and Implementation: An Introduction," *Computer*, vol. 16, no. 7, 1983, pp. 14-22.
13. M. Gasser, *Building a Secure Computer System*, Van Nostrand Reinhold, 1988.

14. C. Farkas and S. Jajodia, "The Inference Problem: A Survey," *ACM Special Interest Group on Knowledge Discovery and Data Mining (SIGKDD) Explorations*, vol. 4, no. 2, 2002, pp. 6–11.
15. B. Pinkas, "Cryptographic Techniques for Privacy-Preserving Data Mining," *ACM Special Interest Group on Knowledge Discovery and Data Mining (SIGKDD) Explorations*, vol. 4, no. 2, 2002, pp. 12–19.

Tentang Penulis



Janner Simarmata. Lahir di Aek Nabara, 07 Januari 1976. Menyelesaikan program S1 pada jurusan Teknik Informatika (S.T) dari STMIK Bandung pada tahun 2000. Memperoleh gelar Magister Ilmu Komputer (M.Kom) dari Sekolah Pascasarjana UGM Yogyakarta, Program Studi Ilmu Komputer tahun 2006. Dosen Tetap di STMIK KAPUTAMA Binjai dan sekaligus menjabat sebagai Ketua Program Studi Teknik Informatika-S1. Pada 2007 menjadi Koordinator Pengembangan dan Informasi pada sebuah LSM Peduli Anak Bangsa di Medan. Penulis juga adalah penulis buku pada Penerbit Andi Yogyakarta sampai sekarang.