Internet Anonymity

Problem and Solutions

Claudia Eckert and Alexander Pircher

**Abstract**

layanan internet seperti World Wide Web atau email program yang sudah banyak di

digunakan untuk bekerja swasta dan bisnis. Sayangnya, dengan setiap akses banyak informasi yang spesifk bocor. Oleh karena itu, menggunakan populer internet layanan resultsin ancaman terhadap privasi pengguna, karena data ini dapat menguping oleh penyerang atau dikumpulkan oleh penyedia layanan untuk membuat profil pengguna. Untuk mengalahkan ancaman seperti layanan anonymi telah diperkenalkan terutama untuk email anonim dan berita bersih. Tapi layanan kerahasiaanya tersedia kurang banyak kekurangan dan tidak memberikan tingkat yang diperlukan anonimitas untuk pengguna internet. Hal ini terutama karena tesis jasa telah dilaksanakan dalam cara yang agak ad hoc kurang analisis sistematis.

Anonymous-proyek yang bertujuan untuk mengungkapkan dan mengatasi kekurangan dari pendekatan yang ada dengan mengikuti metodologi sistematis. kertas kami merangkum hasil utama dari Anonymous-proyek. Ini menjelaskan masalah dan keterbatasan layanan anonim saat ini dan menyajikan layanan baru kami.

1. **Pendahuluan**

Sebagai contoh, mari kita lihat di email biasa. Biasanya, pengirim akan bersedia untuk memberikan alamat email sendiri, tapi dia pasti tidak mau mengungkapkan informasi lain seperti URL halaman Web yang pernah dikunjungi nya. Sampai saat ini, beberapa program untuk kerahasiaanya layanan Internet telah

dikembangkan. Mereka menggunakan teknik yang berbeda sehubungan dengan menghindari data dan / atau data penyembunyian. Biasanya, menghindari data dicapai dengan menekan data yang relevan. enkripsi data menyediakan sarana yang tepat untuk menyembunyikan data yang ditransfer mencegah pihak ketiga yang tidak berwenang mengakses informasi plaintext. Tapi enkripsi data tidak berlaku untuk barang-barang data yang harus dapat diakses oleh mitra komunikasi yang berwenang untuk dapat benar menjalankan protokol transfer yang digunakan (misalnya HTTP, SMTP). Data bersembunyi dalam skenario tersebut dapat dicapai dengan mengganti mereka dengan beberapa pola yang seragam. Masalahnya adalah, bahwa layanan anonim yang ada hanya menyembunyikan atau anonim bagian dari data sensitif. Hasilnya adalah bahwa pengguna internet yang tidak anonim karena mereka bisa. Selain itu, di beberapa layanan penggantian data asli dengan pola seragam hasil dalam kesalahan selama eksekusi protokol. Semua kekurangan-kekurangan ini ditemukan pada layanan yang ada dapat dicegah jika

pengembangan pelayanan dilakukan berdasarkan analisis sistematis dari Internetservices. Menganalisis spesifikasi protokol protokol standar Internet memungkinkan untuk mengklasifikasikan data ditransfer ke dalam kelas data sensitif yang harus anonim dan semua sisa yang tidak penting. Selain itu, analisis yang serius dapat mengungkapkan sejauh mana data sensitif sebenarnya diperlukan untuk

melakukan protokol berhasil. Hal ini telah dilakukan dalam Anonymousproject kami [5]. Tujuan kami adalah untuk memperbaiki kekurangan yang ditemukan dengan mengembangkan layanan anonim yang lebih kuat dan lebih fleksibel dibandingkan dengan yang sudah ada.

Sisa kertas kami diatur sebagai berikut. Bagian 1.1 menyajikan hasil utama dari penyelidikan kami layanan Internet umum. Untuk dapat membandingkan kekuatan layanan anonim kami telah mengembangkan metrik sederhana yang akan kami jelaskan di bagian 1.2. Berdasarkan analisis kami dan metrik kami telah mengevaluasi layanan anonim yang ada. Hasilnya dirangkum pada bagian

2. Berdasarkan pengalaman kami, kami telah mengembangkan suite kami sendiri layanan anonim yang akhirnya akan disajikan dalam 3. Dalam 4 kami merangkum kontribusi utama dari kertas kami.

* 1. **Analisis Layanan Internet yang Relevan**

layanan Internet populer seperti HTTP, FTP, SMTP, atau NNTP adalah aplikasi client-server yang berjalan di atas protokol Internet (IP). Layanan ini memberikan paket data ke lapisan IP yang menambahkan header IP untuk setiap paket. Header IP berisi antara data lain alamat IP dari pengirim paket dan penerima. Oleh karena itu, sebuah layanan anonim hanya bisa mencoba untuk menyembunyikan alamat IP pengirim. Tapi teknik sederhana ini tidak berlaku jika protokol membutuhkan komunikasi dua arah antara pengirim dan penerima atau jika protokol harus mengirim pesan kembali ke pengirim, misalnya, dalam kasus-kasus kesalahan. Selain itu, kita harus melihat bahwa alamat IP sering sudah ditambahkan ke paket data pada lapisan protokol yang lebih tinggi oleh protokol aplikasi sendiri. Inilah sebabnya mengapa alamat data harus disaring pada per aplikasi protokol dasar di samping tingkat filtering IP. Seperti semua layanan yang diselidiki memiliki kesamaan bahwa anonimitas sehubungan dengan pihak ketiga dapat dicapai dengan menggabungkan teknik enkripsi, kita menghilangkan teknik ini dalam diskusi berikutnya kami.

* + 1. **HTTP (Hypertext Transfer Protocol)**

HTTP [3] adalah protokol request / respon yang menetapkan koneksi dua arah antara klien dan server. Sebuah pesan permintaan dari klien terdiri dari beberapa header dan payload pesan. Mengklasifikasikan data header ke privasi kritis dan tidak kritis data yang kita amati bahwa referer-entry jelas milik kelas pertama. Catatan ini berisi URL dari halaman dari mana server disebut. Oleh karena itu, server dapat memperoleh informasi konteks tentang kliennya hanya dengan memeriksa referer-bidang. Pertimbangkan misalnya seorang klien yang mengirimkan permintaan dalam konteks mesin pencari. Dalam hal ini, referer-entry berisi daftar hit seluruh pencarian sebelumnya dilakukan oleh klien. Dari sudut server tampilan daftar ini mungkin berisi informasi menarik tentang pesaing di pasar digital. Selain itu, kata-kata kunci yang dicari ditransfer dalam referer-entry mengungkapkan banyak informasi tentang klien bermaksud dan persyaratan.

berbagai menerima-bidang yang digunakan dalam pesan HTTP milik kelas data sensitif juga. Bidang ini biasanya mengandung rangkaian karakter yang disukai, bahasa dan skema pengkodean dll klien. Dengan hati-hati menganalisis menerima-bidang musuh mampu memperoleh banyak informasi penting mengenai klien HTTP. informasi alamat IP dapat ditemukan di bidang client-IP, X-Forwarded dan cache control yang karenanya milik kelas informasi sensitif juga. bidang sensitif lain adalah -Field agen pengguna yang mengidentifikasi klien agen pengguna dan opsional dari-entri menentukan alamat email dari pengguna yang terkait dengan pengguna-agen. informasi otentikasi ditransfer dalam bidang otorisasi dan proxy authorization-. Mereka mungkin berisi nama pengguna dan password pengguna yang biasanya hanya Base64 dikodekan. Selain semua header ini yang sepenuhnya ditentukan oleh spesifikasi protokol, pesan HTTP mungkin memiliki header yang dapat didefinisikan oleh pengguna dengan cara sewenang-wenang, mungkin berisi banyak informasi sensitif pengguna tertentu. Berbeda dengan field header yang dibahas di atas yang diciptakan oleh sistem klien yg tercinta-entri berisi data yang awalnya diciptakan oleh server dan disimpan di sisi klien. yg membuang yang ditransfer secara otomatis oleh klien-browser setiap kali klien kembali terhubung ke server. Informasi ditransfer memungkinkan server untuk kembali mengidentifikasi klien meskipun protokol HTTP yang mendasari adalah stateless. Masalahnya adalah, yang biasanya klien tidak mengetahui informasi apa yang dikirim ke server dikodekan dalam yg tercinta-entry. Sebagai klien sering mengungkapkan informasi privasi terkait tentang dirinya dengan mengisi Webforms disampaikan oleh server, server dapat mengekstrak informasi pengguna tertentu dan mengkodekan mereka dalam cookie. Setiap kali klien kembali menetapkan koneksi ke server, server hanya menerjemahkan yg tercinta untuk mengungkapkan identitas klien.

**Anonim HTTP**

Kami telah menganalisis 7.648 permintaan Web. Pertama, kami mengamati bahwa di 99% dari semua permintaan tersebut yang menerima-bidang yang terkandung data sensitif yang disebutkan di atas, tetapi yang tidak digunakan oleh penerima sama sekali. Oleh karena itu, dalam suatu layanan anonim data ini dapat baik benar-benar dihindari atau diganti dengan pola lain tanpa mengganggu fungsi server. Sebaliknya, informasi dalam bidang agent--friendly yang hadir di lebih dari 98% dari permintaan, sebenarnya digunakan oleh server untuk menyesuaikan penyajian halaman yang diperlukan untuk kemampuan tertentu dari browser klien. Oleh karena itu, layanan yang bertujuan kerahasiaanya data ini harus dikonfigurasi dalam cara yang fleksibel. Hal ini akan memungkinkan untuk menggunakan layanan yang disesuaikan bahkan dalam konteks kegiatan anonim.

Informasi yang terkandung dalam referer-bidang telah ditransfer di lebih dari 95% dari semua permintaan dianalisis. Ini luar biasa, karena informasi yang tidak diperlukan untuk menjalankan HTTP dengan benar. Seperti yang telah kita menunjukkan sebelumnya, musuh mungkin menyimpulkan banyak informasi sensitif tentang pengirim melihat referer-bidang. Oleh karena itu, kami sarankan untuk menghilangkan semua data dalam referer-bidang.

Analisis kami menunjukkan bahwa data dalam dari-bidang yang tidak digunakan oleh protokol itu sendiri atau oleh penyedia layanan. Karena akan mengandung banyak informasi menarik untuk pihak ketiga yang tidak sah, kami sangat menyarankan untuk menghilangkan bidang ini juga, Cookies telah diamati dalam setidaknya 30% dari semua permintaan dianalisis, meskipun layanan yang diminta adalah digunakan dengan benar tanpa mereka juga . Oleh karena itu, meninggalkan Data yg tercinta dengan layanan anonim tidak akan menyebabkan layanan denial-of-tidak dapat diterima.

Untuk menghindari transfer terlindungi dari informasi alamat IP dalam field header HTTP, kami sarankan untuk anonim bidang client-IP, X-forwardedfor dan cache control. Ini layak tanpa mengganggu fungsi protokol secara keseluruhan, karena bidang ini tidak diperlukan dalam rangka melaksanakan protokol dengan benar. Karena kolom header proxy otorisasi hanya diperlukan untuk mengotentikasi browser sehubungan dengan server proxy, kami merekomendasikan bahwa proxy harus anonim informasi ini sebelum meneruskan pesan dimodifikasi. Akhirnya, kami mengharuskan HTTP-anonymi harus dikonfigurasi sedemikian rupa bahwa semua header diketahui akan dianonimkan secara default. Tapi anonymi harus cukup fleksibel untuk memungkinkan selektif transfer disembunyikan data sundulan tersebut.

* + 1. **FTP (File Transfer Protocol).**

FTP [7] menyediakan layanan untuk secara efisien mentransfer data. Ia bekerja sesi-based dan membedakan antara kontrol dan payload data. Saluran kontrol terpisah didirikan untuk transfe data kontrol dan hubungan ini diadakan terbuka selama seluruh sesi. Sebaliknya, FTP membentuk koneksi baru untuk setiap mengirim atau menerima transaksi untuk mentransfer data payload. Perhatikan, bahwa setiap kali FTP membentuk koneksi baik untuk kontrol atau transfer data, alamat IP klien ditransmisikan. Selain itu, beberapa perintah memerlukan parameter yang mungkin berisi informasi sensitif. Perintah-perintah ini adalah user-perintah yang mengidentifikasi pengguna melalui ASCII-string, pass-perintah yang berisi user-password sebagai parameter, dan acct-perintah yang memerlukan parameter yang mengidentifikasi nama akun pengguna. Menggunakan layanan FTP anonim, saat ini internet browser biasanya memberikan password yang mengidentifikasi digunakan jenis browser (mis mozilla @ di Netscape Communicator). Selain itu, browser biasanya memiliki pilihan untuk mentransfer alamat email dari pengguna yang terdaftar dalam file konfigurasi browser.

**Anonim FTP**

Sejak FTP non-anonim memerlukan nama pengguna, kata sandi serta nama pengguna akun untuk dapat mengotentikasi FTP-client kerahasiaanya data ini di sisi mitra komunikasi (yaitu FTP-server) tidak mungkin. Hal yang sama berlaku untuk alamat IP klien yang diperlukan untuk membangun koneksi data. Seperti disebutkan sebelumnya, mengenkripsi semua data ini adalah tepat untuk menggagalkan serangan dari pihak ketiga yang tidak berwenang. Sehubungan dengan anonymous FTP kami sarankan untuk anonim alamat email ditransfer. Hal ini dapat dicapai misalnya dengan mengganti dengan yang fiktif menyembunyikan identitas sebenarnya dari pengguna FTP.

* + 1. **SMTP (Simple Mail Transfer Protocol).**

Seperti kita ketahui, bahwa ada banyak argumen yang baik yang meragukan kesesuaian email anonim kami selanjutnya hanya fokus pada satu aspek khusus yang kita anggap penting. Artinya, dalam pendapat kami pengirim email harus mengungkapkan identitasnya kepada penerima nya (s), tapi selain itu, ia tidak akan bersedia untuk mengekspos informasi lain mengenai privasi. Contoh untuk informasi tersebut yang harus ditekan adalah data tentang lingkungan eksekusi yang digunakan seperti sistem operasi dan perangkat keras. Yang lebih penting adalah penindasan data tentang konteks pengiriman seperti link ke pesan lainnya email mengacu pada.

Pengalihan email adalah tugas utama dari SMTP [6]. Untuk tujuan ini, SMTP membentuk koneksi dua arah antara klien dan server. Koneksi ini setelah digunakan untuk mentransfer beberapa mail. Analog dengan FTP SMTP membutuhkan alamat IP klien untuk membangun hubungan ini dan selanjutnya data sensitif dapat ditransfer dengan memanggil perintah SMTP tertentu. Surat-perintah menentukan parameter yang berisi jalur kembali ke pengirim email. Jalur ini digunakan dalam kasus-kasus kesalahan untuk mengirim ulang surat ke pengirimnya. Data-perintah yang digunakan untuk mentransfer data email. Data itu sendiri terdiri dari bagian header dan bagian payload. Satu dalam arti barang sundulan penting kami adalah return-path. Ini menentukan alamat pengirim serta jalur kembali ke alamat ini. Jalur ini dibangun sebagai berikut. Setiap pengirim yang mengambil bagian dalam mentransfer mail ke tujuan akhir, menambahkan alamat sendiri serta tanggal dan waktu informasi ke jalan. Oleh karena itu, jalan menunjukkan secara rinci seluruh rute di mana surat itu diteruskan ke receiver-nya.

identitas pengirim dapat diturunkan dari item header lain juga. Kritis dalam arti kita adalah dari, pengirim dan balasan-entri tersebut. Dari field berisi identitas agen pengiriman (misalnya mesin atau seseorang). Masuknya pengirim berisi identitas pengirim dalam kasus di mana penulis pesan tidak pengirimnya. balasan-ke lapangan menentukan kotak surat yang menjawab bisa mengirim. Selain itu, di-reply-to dan referensi tajuk bidang berisi data bermasalah juga. Mereka mengidentifikasi email yang mail saat menjawab serta semua pesan lain yang dirujuk dalam surat.

Selain bidang yang ditentukan dalam standar SMTP mail mungkin berisi sewenang-wenang user-didefinisikan serta disebut sundulan diperpanjang (dimulai dengan X) bidang.

**Anonim SMTP**

Analisis kami menunjukkan bahwa sebagian besar field header yang terkandung dalam mail yang tidak diperlukan oleh SMTP. Oleh karena itu, kami sarankan untuk anonim semua item header yang membawa informasi melampaui identifikasi pengirim langsung. Artinya, setidaknya di-reply-to, kembali-jalan dan lapangan referensi harus anonim untuk menyembunyikan data penting sejauh mungkin tidak hanya berkenaan dengan pihak ketiga namun sehubungan dengan penerima email resmi juga. Seperti disebutkan sebelumnya, beberapa header ini sebenarnya berguna dalam kasus trouble shooting. Oleh karena itu, layanan anonim harus cukup fleksibel untuk memungkinkan konfigurasi individu.

Sejak header diperpanjang ciri pengirim cukup baik dan, di samping itu, mungkin berisi data sewenang-wenang kami sangat menyarankan untuk menekan semua header nonstandardized tetapi banyak digunakan tersebut. Jika penindasan lengkap tidak layak data harus diganti dengan pola acak. Ini tidak akan mengganggu pelaksanaan SMTP karena protokol tidak memerlukan header diperpanjang. Jelas, header tidak diketahui (user-defined) harus benar-benar ditekan oleh anonymi.

* + 1. **NNTP (Network News Transfer Protocol).**

Seperti sebelumnya, kita tidak berdebat mendukung untuk posting anonim, tetapi fokus pada kehebatan untuk membatasi transfer data sensitif untuk minimum. Artinya, kami sangat tertarik pada data tersebut yang secara otomatis ditambahkan ke sebuah posting (atau surat, lihat bagian sebelumnya) tanpa memberikan kesempatan untuk mengendalikan atau mengatur ini pengguna.

NNTP [4] menawarkan layanan untuk membaca, pos dan mendistribusikan artikel berita. Untuk tujuan ini, klien membuat sambungan dua arah untuk server berita. Koneksi ini kemudian dapat digunakan untuk beberapa tindakan seperti membaca dan posting artikel. Seperti protokol SMTP NNTP menentukan field header untuk artikel berita. header ini sebanding dengan yang digunakan dalam SMTP dan tidak perlu dibahas lagi.

Selain itu, header berita dapat berisi field yang disebut organisasi. Bidang ini menunjukkan organisasi yang pengirim milik. Oleh karena itu membawa data menarik yang mungkin menjadi ciri pengirim cukup baik. Analog dengan HTTP dan SMTP NNTP memungkinkan untuk menggunakan header non-standar yang mungkin berisi data pengguna tertentu yang sewenang-wenang.

**Anonim NNTP**

Karena kesamaan antara SMTP dan NNTP kami merekomendasikan tindakan anonim yang sama. Artinya, anonymi harus menyembunyikan atau menekan semua data sundulan secara otomatis. Sekali lagi itu akan sangat membantu, jika anonymi adalah cukup fleksibel untuk selektif de-anonimkan item data. Tak satu pun dari header nonstandardized diperlukan untuk fungsi yang benar dari protokol. Oleh karena itu, semua header berbahaya potensial ini harus anonim secara default. Tapi karena beberapa data ini dapat digunakan oleh beberapa server itu harus mungkin untuk selektif de-anonim set yang diperlukan data.

* 1. **Tingkatan Anonimitas**

ayat menyajikan metrik sederhana untuk membandingkan kekuatan layanan anonim. Pertama, kami ingin menangkap gagasan anonimitas lebih tepat. Anonim dalam pengertian kami berarti modifikasi data terkait privasi dengan tujuan agar data tunggal membawa data privasi-kritis tidak bisa lagi berhubungan dengan orang tertentu kecuali sejumlah besar uang, waktu dan manusia listrik akan dihabiskan.

Sebuah bentuk yang lebih lemah diberikan oleh pseudo-anonimitas. Di sini, data yang terkait privasi dimodifikasi sesuai dengan aturan tugas tertentu (biasanya dengan menggunakan nama samaran) dengan efek bahwa data tunggal membawa data privasi-kritis tidak bisa lagi berhubungan dengan orang tertentu tanpa sepengetahuan aturan penugasan.

Sekarang, kita akan mendefinisikan beberapa tingkat anonimitas untuk dapat membedakan antara layanan anonim kekuatan yang berbeda. Kekuatan yang berbeda dari tingkat hasil dari lingkup yang berbeda dari tindakan anonim. Kami membedakan antara tiga lingkup berikut: anonimitas (1) terhadap mitra komunikasi, (2) terhadap pihak ketiga, dan melawan (3) anonymi itu sendiri. Bentuk terkuat dari anonimitas disediakan, jika layanan anonim mencakup semua tiga lingkup.

**Level 1** Pseudo-anonimitas sehubungan dengan mitra komunikasi:

Mitra komunikasi tidak dapat mengaitkan item data tunggal dengan orang tertentu. Tapi semua langkah-langkah untuk mencapai pseudo-anonimitas semata-mata dilakukan oleh mitra komunikasi sendiri. Artinya, jenis anonim dapat tidak dipengaruhi oleh pengguna dan juga tidak mampu mengontrol keberhasilan dan kebenaran layanan. Di sisi lain, pengguna benar-benar lega dari mengatasi tindakan anonim. Layanan pada tingkat ini tidak memberikan anonimitas sehubungan dengan pihak ketiga.

**Level 2** Pseudo-anonimitas sehubungan dengan layanan anonim:

Berbeda dengan tingkat 1, data pribadi kritis hanya ditransfer ke layanan anonim dan tidak ke mitra komunikasi, yang menyediakan tingkat yang lebih tinggi anonimitas. Mitra komunikasi semata-mata tahu nama samaran dari pengguna tanpa bisa mengasosiasikannya dengan orang yang nyata. Tetapi menggunakan layanan sebuah anonim tersebut tidak sepenuhnya transparan bagi pengguna karena mereka harus secara eksplisit menyebutnya. Dan, seperti sebelumnya, layanan pada tingkat ini tidak memberikan anonimitas sehubungan dengan pihak ketiga.

**Level 3** Anonimitas sehubungan dengan mitra komunikasi:

Analog dengan level 1 semua tindakan anonim dilakukan oleh mitra komunikasi tanpa dikendalikan oleh pengguna. Tidak ada anonimitas sehubungan dengan pihak ketiga disediakan.

**Level 4** Anonimitas sehubungan dengan layanan anonim:

Analog dengan tingkat 2 privasi data-kritis anonim oleh pihak ketiga sebelum dikirim ke mitra komunikasi. Sekali lagi kita tidak memiliki perlindungan terhadap pihak ketiga.

**Level 5** Anonimitas sehubungan dengan pihak ketiga:

Pengguna dilindungi terhadap mitra komunikasi serta terhadap pihak ketiga menengah.

**Level 6** Anonimitas sehubungan dengan anonymi yang:

Sampai ke tingkat 5 anonymi selalu memiliki pengetahuan tentang penggunanya serta mitra komunikasi mereka. Pada tingkat ini kita mengharuskan anonymi tidak dapat menyimpulkan hubungan antara pengguna dan titik akhir komunikasi. Selain itu, tingkat membutuhkan anonimitas terhadap pihak ketiga menengah.

1. **ANONYMIZER – STATE-OF-THE-ART**

Sebagian besar kegiatan di wilayah anonimitas Internet berkonsentrasi pada email dan anonimitas berita sedangkan layanan kerahasiaanya untuk daerah WWW dan FTP hampir tidak tersedia. Karena kita tertarik anonimitas data terkait klien, kami tidak menyelidiki proyek yang berkonsentrasi pada server anonimitas seperti JANUS-proyek [2].

* 1. **WWW AND FTP**

Layanan anonim yang paling sederhana hanya anonim file log dari WWWserver (mis http://www.media.mit.edu/~daniels/software/scramble.html). Kami menyebutnya seperti anonymi file log anonymi. File log mencatat semua akses ke server. Jika anonymi file log terintegrasi ke dalam Web-server maka data dapat disimpan di file log dalam bentuk yang sudah anonim. Tergantung pada fakta apakah anonimitas atau pseudo-anonimitas yang ditawarkan, anonymizers seperti hanya memberikan tingkat 3 atau tingkat 1 layanan dengan semua masalah di atas. Lebih buruk lagi, langkah-langkah yang tergabung dalam pendekatan yang ada yang rusak dalam arti sehingga tidak semua data penting benar-benar anonim. Menjadi lebih konkrit, pendekatan ini hanya menyembunyikan nama host, IP addresss dan nama pengguna. Tapi analisis kami (lihat bagian sebelumnya) mengungkapkan bahwa banyak bidang data lainnya yang berisi data pribadi penting masih ada, seperti misalnya referal atau useragent bidang. Data ini disimpan disembunyikan dalam file log dari server.

**Server proxy**

implementasi lain dari WWW atau FTP anonymi mengintegrasikan layanan mereka ke server proxy. Sebuah contoh yang populer untuk jenis teknologi anonim adalah Junkbuster (http :: / www.junkbuster.com). Menggunakan pendekatan proksi memungkinkan untuk memodifikasi atau menyembunyikan data penting sebelum pesan dikirim ke tujuan mereka. Misalnya, Junkbuster menekan forwarding cookie, dan dari- serta -fields referal dan pengganti data pengguna-agen seragam oleh Mozilla / 3.01 Emas. Tapi, dengan Junkbuster semua bidang lain yang berisi data penting seperti menerima -fields diteruskan ke tujuan akhir tanpa modifikasi. Terutama, semua field header tidak diketahui akan diteruskan tanpa anonim. Oleh karena itu, layanan anonim yang ditawarkan oleh Junkbuster tidak lengkap.

Karena anonymi proxy yang terintegrasi tidak mengenkripsi transfer data antara browser dan proxy server, anonymi seperti hanya bisa diklasifikasikan ke level 4 atau hanya 2 dalam kemudahan semu anonimitas.

**Web-Anonymizer**

Web-Anonymizer bekerja sangat mirip dengan anonymi proxy yang terintegrasi. Salah satu perwakilan populer adalah Anonymizer (http://www.Anonymizer.com). Tetapi berbeda dengan pendekatan proxy, layanan yang diperlukan Web-anonymi diintegrasikan ke dalam Web-server. Akibatnya, layanan ini dapat digunakan di belakang firewall dan data antara browser dan web-server dapat ditransfer dalam bentuk terenkripsi.

Sayangnya, keunggulan ini disertai dengan overhead manajemen tambahan dibandingkan dengan proxy pendekatan. kegiatan anonim tambahan yang diperlukan jika Web-halaman atau file yang telah diminta oleh klien tidak sendiri berisi referensi. Jika klien mengklik referensi ini langsung ada layanan anonim akan diterapkan ke Web ini mengakses. Oleh karena itu, referensi tersebut harus dimodifikasi untuk memastikan bahwa setiap panggilan (klik pada referensi) akan langsung dikirim ke Web-anonymi. Jelas, ini mempersulit pelaksanaan Web-anonymi jauh yang dapat menyebabkan layanan yang keliru. Selanjutnya, anonymi seperti biasanya bekerja jauh lebih lambat dari proxybased solusi.

Kami telah hati-hati mempelajari atas layanan Anonymizer disebutkan (lih [5]). Analisis kami menunjukkan bahwa Anonymizer sebenarnya anonymizes banyak data pribadi penting seperti dari, referal dan ladang yg tercinta. Tapi data penting lainnya seperti, misalnya, klien-IP dan kontrol cache diteruskan dimodifikasi. Selain itu, tidak mungkin untuk selektif de-aktifkan penindasan cookies. Oleh karena itu, server yang membutuhkan cookie tidak dapat diakses melalui layanan Anonymizer. Selain itu, harus diperhatikan bahwa Anonymizer tidak mengenkripsi data ditransfer. Karena pembatasan ini tidak ditentukan oleh arsitektur Web-server yang melekat tingkat anonimitas dilaksanakan oleh Anonymizer lebih rendah (hanya level 4) daripada yang dicapai pada prinsipnya. Bahkan, anonymizers tersebut dapat memberikan tingkat 5. Web-server anonymi bahkan bisa ditingkatkan dengan menggunakan mereka dengan cara Cascading yang akan menghasilkan tingkat 6 anonimitas.

**Crowds**

The Crowds-proyek [8] mengikuti pendekatan yang sama sekali lain dengan bersembunyi pengguna dalam kerumunan. Untuk tujuan ini, pesan pengguna dikirim terenkripsi ke anggota yang dipilih secara acak dari kerumunan yang memilih penerima lain di antara kerumunan atau mengirimkan pesan ke tujuan akhir. Jelas, kerumunan kecil tidak cukup untuk menjamin anonimitas. Keramaian layanan menekan banyak data penting seperti dari, cache control, yg membuang, X-diteruskan dan bidang referer. Selain itu, anonymizes yang menerima serta data user-agent dengan mengganti data asli dengan nilai default. Tapi ini dapat menyebabkan masalah, jika server yang menafsirkan data ini berjalan ke dalam kesulitan dengan menggunakan nilai default. Misalnya, nilai zip digunakan untuk mengganti item data lain di lapangan menerima-encoding tidak didefinisikan dalam spesifikasi HTTP dan dapat mengakibatkan tindakan server yang rusak. Selanjutnya, di bawah Crowds header diketahui mungkin mengandung informasi penting yang ditransfer tanpa modifikasi. Kelemahan lain dari layanan Massa adalah bahwa hal itu tidak dapat digunakan bersamaan dengan firewall di sisi klien. Meskipun tesis masalah Crowds berlaku secara cascading. Oleh karena itu, anonimitas level 6 dicapai pada prinsipnya. Tetapi harus diperhatikan bahwa pijat pengiriman jauh tertunda melalui air terjun Crowds server. Perhatikan, bahwa klien permintaan WWW tidak dapat menentukan anggota kerumunan yang terlibat dalam pengiriman pesannya. Artinya, anggota tidak dapat diandalkan, anggota dipercaya atau node yang tidak online mungkin dipilih secara acak. Layanan ini dapat ditingkatkan, jika klien dapat memilih rute tergantung pada informasi tentang ketersediaan saat ini dan beban anggota kerumunan.

* 1. **EMAIL AND NEWS**

Karena email dan berita adalah layanan asynchronous tidak perlu bahwa pesan dikirim ke tujuan akhir mereka segera. Hal ini dimanfaatkan oleh layanan remailer yang merupakan anonymizers paling populer di daerah ini. Ide asli kembali ke D. [1] Chaum yang mengusulkan pendekatan campuran untuk mengubah pesan. Seorang pengguna dari layanan remailer harus secara eksplisit mengirim pesan ke remailer. remailer menghapus informasi header dan meneruskan pesan. Untuk menggagalkan serangan arus lalu lintas, remailer biasanya menunda penerusan pesan dan menempatkan pesan boneka ke dalam aliran pesan. fungsi semacam ini menjadi ciri khas yang disebut Tipe 1 atau cypherpunk remailers. Daftar remailers tersedia dapat ditemukan di bawah http://anon.efga.org/Remailers/TypeIList. Kelas kedua dari remailers adalah Tipe 2 remailers atau Mixmaster (http://anon.efga.org/Remailers/TypeIIList/type2.list). Tapi, menggunakan kelas ini email anonymi memerlukan klien email tertentu yang mengenkripsi pesan dan padds mereka ke panjang seragam biasanya 30kbyte.

Untuk dapat menggunakan remailers dalam kaskade remailer, pengirim harus menyandikan rantai alamat remailer terenkripsi ke dalam surat-suratnya. Setiap remailer menghilangkan masuknya rantai yang telah dienkripsi dengan kunci publik. entri terenkripsi berisi alamat dari mailer berikutnya dalam rantai. Setelah mendekripsi nya entri mailer mampu meneruskan email dengan benar. Teknik ini memastikan bahwa hanya remailer pertama dalam rantai tahu identitas pengirim asli dan semata-mata remailer terakhir dalam rantai tahu alamat tujuan akhir. Meskipun chaining seperti layak, pelayanan remailing praktek hanya menggunakan satu remailer. Sebagai konsekuensinya, remailer yang dilihat semua data penting yang terkandung dalam bidang data sundulan sebagai hanya payload pesan dienkripsi. Oleh karena itu, saat ini remailers hanya menawarkan tingkat anonymi 5 sedangkan tingkat 6 dicapai oleh cascading remailers.

1. **Layanan Anonymi Baru**

Bagian sebelumnya menunjukkan kekurangan dari anonymizers yang ada. Mereka tidak memberikan layanan anonim yang cukup anonim semua data penting (khususnya, IP-alamat dan menerima bidang dihilangkan) dan penonaktifan langkah-bijaksana tindakan anonim yang hampir didukung. Selain itu, sebagian besar pendekatan menerapkan tingkat anonim yang lebih rendah daripada yang mungkin dicapai.

Oleh karena itu, dalam Anonymous-proyek [5] kita dikembangkan dan diimplementasikan layanan anonim baru untuk mengatasi kekurangan terungkap.

* 1. **LOG-FILE ANONYMIZER**

Kami log-file anonymi telah dikembangkan untuk Apache Web-server. Kami menganonimkan log-entri yang berisi informasi berikut: *hostname,identd-name, user-name, time, request line, status, amount of bytes being sent, referer, user-agent*. Apache-server telah diatur sedemikian rupa sehingga ke depan semua data tesis untuk anonymi log-file kita. Data ini anonim seperti yang ditunjukkan dalam tabel 1.

Yang dihasilkan log-file kompromi. anonymi kami mencoba untuk menawarkan tingkat yang sesuai anonimitas bagi penggunanya (yaitu tingkat 3) sambil menjaga informasi yang cukup bagi penyedia layanan, misalnya, untuk, menghasilkan statistik akses bermakna. anonymi kami mencakup semua data penting privasi. Kami menyadari bahwa mengganti nama host dengan nama top-level dapat menyebabkan masalah jika server memerlukan informasi yang lebih tepat untuk melakukan analisis tertentu (misalnya mengenali akses yang berasal dari robot). Oleh karena itu, untuk entri ini juga untuk yang lain kami menawarkan pilihan untuk mengkonfigurasi tindakan anonim sesuai dengan kebutuhan server individu. Namun demikian, itu harus jelas bahwa anonymi log-file tidak teknik anonim pilihan pertama kami, karena penggunaan tidak mampu mengontrol dan mengkonfigurasi dengan tepat.

|  |  |
| --- | --- |
| **Data** | **Modification** |
| Hostname | ,< top-level-domain> (e.g. de) |
| Identd-name | - |
| User-name | - |
| Time | [day/month/year:hours:00:00 zone] |
| Request | No modification |
| HTTP-version | HTTP/1.0 |
| Referer | - |
| User-agent | Anonymizing browser, OS, language |

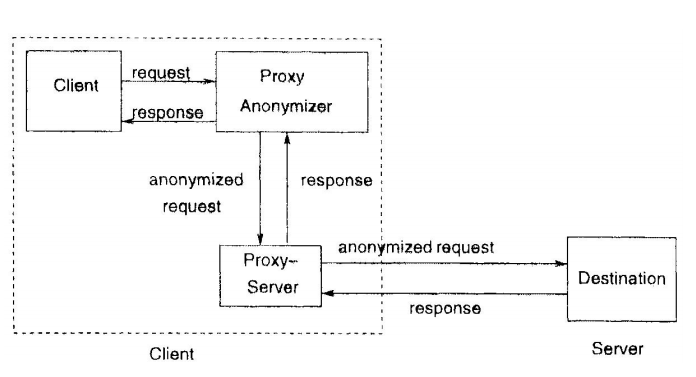
*Table 1 Anonymized log-file entries*

**Example:**

|  |  |
| --- | --- |
| The protocol entry | is anonymized to: |
| sunsystem.in.tum.de | .de |
| [18/Apr/2000:13:13:27+02000] | [18/Apr/2000:13:13:00:00+02000] |
| "GET /images/logo.gif HTTP/1.1" | "GET /images/logo.gif HTTP/1.0" |
| "http://www.in.tum.de/" -"Mozilla/4.5[en](Win98;I)" | "Netscape(Windows)" |

* 1. **PROXY ANONYMIZER**

The proxy yang menerima permintaan dan mengirimkannya ke server proxy asli setelah tersembunyi dan memodifikasi item data yang relevan (lihat gambar 1). Oleh karena itu, anonim dilakukan di sisi pengguna. Tapi anonymi proxy yang kita tidak terganggu dengan manajemen cache atau tugas manajemen lainnya karena ini masih dilakukan oleh server proxy asli.

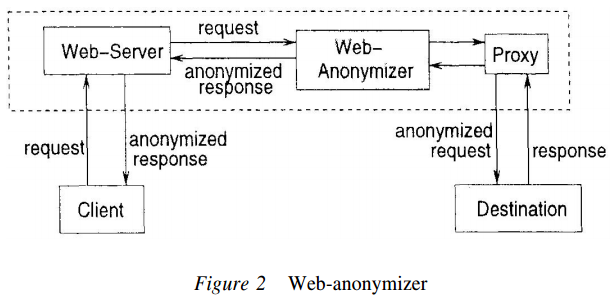


Gambar Proxy anonymizer

The proxy yang terdaftar dalam file konfigurasi browser. Seorang pengguna individual dapat mengkonfigurasi anonymi melalui halaman penyiapan. Artinya, pengguna dapat memilih data yang akan ditempatkan ke field header dan ia dapat selektif menonaktifkan kegiatan anonim bagi mereka field header penting kita sebelumnya telah dijelaskan. Misalnya, pengguna dapat menentukan item data yang harus ditulis ke dalam menerima, bidang dari atau user-agent. Selain itu, ia dapat menggantikan data dalam bidang-bidang yang berisi informasi tentang sistem operasi pengguna, platform perangkat keras nya dll Akibatnya, permintaan dari klien yang berbeda dianonimkan dengan cara non-seragam. Menyadari permintaan anonim karena itu sulit bagi musuh. Selanjutnya, anonymi proxy yang kami memungkinkan untuk mengkonfigurasi nilai data bahwa server menambahkan ke ladang cache-info, client-IP, X-diteruskan, melalui, diteruskan. Sejak beberapa server benar-benar menggunakan atau membutuhkan informasi yang terdapat dalam bidang tuan rumah, referer, yg membuang, cache-control dan konten-jenis, anonymi proxy yang kami memberikan pilihan untuk selektif mengaktifkan atau menonaktifkan penyembunyian bidang ini. Karena alasan yang disebutkan di bagian sebelumnya, anonymi kami secara otomatis menekan field header semua tidak diketahui. Proxy anonymi mencapai tingkat anonimitas 4.

* 1. **WEB-ANONYMIZER**

Untuk menggunakan Web-anonymi yang diintegrasikan ke dalam Web-server pengguna harus menentukan file yang harus anonim dan harus secara eksplisit menyebut layanan kami melalui URL. Data akan dianonimkan dan kemudian diteruskan ke tujuan tertentu. Kami hanya meneruskan data yang sebenarnya diperlukan untuk melaksanakan layanan yang diminta. Misalnya, dalam kasus metode GET kami akan mentransfer host-header sedangkan dalam kasus metode POST host-orang, konten-panjang-dan konten-jenis-header diteruskan. Semua jawaban server-side dianonimkan sebelum dikirimkan ke klien (lihat gambar 2). Oleh karena itu, akses berikutnya dari klien pada link yang terdapat dalam halaman jawaban dari server (grafis misalnya dirumuskan) secara otomatis dialihkan melalui Webanonymizer kami. Selain link anonim yang ada di HTML-data yang kami juga anonim referensi dalam program JavaScript. Selanjutnya, berbeda dengan Anonymizer sebelum disebutkan, kami juga menyembunyikan referensi FTP dan email serta referensi berita secara otomatis diteruskan ke layanan anonim kami (lihat di bawah). Kami Web-anonymi menekan semua header tidak diketahui dan menyembunyikan semua data pribadi yang penting dibahas dalam bagian 1.1. Data dapat dienkripsi dengan klien meminta, tapi sampai sekarang, tidak ada server Cascading anonim telah dilaksanakan belum. Oleh karena itu, pada saat ini anonymi kami mencapai level 5.

****

Gambar Web Anonymizer

to select an appropriate remailer are (1) the availability of the service and (2) the functionality that is supported by the service. For instance, our remailer selection takes into account whether the remailer supports the required message format or news support. The availability of remailers is evaluated based on a remailer statistics that is updated once per hour. The level of anonymity can be increased if the sender uses a SSL connection to our anonymizing service which guarantees anonymity with respect to third parties as well. This level is not achievable by just calling a remailer using an email encryption program like PGP, because these programs solely conceal the mail payload and leave the traffic information unmodified. Since no cascading of our service is provided yet, our anonymizing services reaches level 5. Our Web-anonymizer, and the email as well as news gateways are available in the Internet see http://anonymouse.home.pages.de/.

* 1. **EMAIL AND NEWS-GATEWAYS**

Email dan berita kami anonymizers bertujuan menghindari transfer data penting privasi. Untuk tujuan ini, layanan anonim kami meminta pengguna untuk mengisi formulir HTML dengan data email yang akan dianonimkan bersama-sama dengan alamat penerima. Layanan kami hanya bertindak sebagai gateway karena mereka meneruskan data ke layanan remailer dalam Internet dan mengirim sebuah pengakuan tentang forwarding sukses kembali ke klien. Gateway menyembunyikan semua data kecuali alamat penerima, baris subjek dan payload email sebelum mengirimnya ke remailer. Sebuah remailer secara dinamis dipilih dari daftar remailers. Kriteria untuk memilih remailer yang sesuai adalah (1) ketersediaan layanan dan (2) fungsi yang didukung oleh layanan. Misalnya, pilihan remailer kami memperhitungkan apakah remailer mendukung format pesan atau berita dukungan yang diperlukan. Ketersediaan remailers dievaluasi berdasarkan pada statistik remailer yang diperbarui sekali per jam. Tingkat anonimitas dapat ditingkatkan jika pengirim menggunakan koneksi SSL untuk layanan anonim kami yang menjamin anonimitas sehubungan dengan pihak ketiga juga. tingkat ini tidak dicapai dengan hanya memanggil remailer menggunakan program enkripsi email seperti PGP, karena program ini hanya menyembunyikan payload mail dan meninggalkan informasi lalu lintas yang tidak dimodifikasi. Karena tidak ada Cascading layanan kami disediakan belum, layanan anonim kami mencapai tingkat 5. kami Web-anonymi, dan email serta gateway berita yang tersedia di internet melihat http://anonymouse.home.pages.de/.

1. **CONCLUSION**

Dengan meningkatnya penggunaan layanan internet kita dihadapkan dengan ancaman berat terhadap privasi pengguna. Semua layanan Internet secara luas digunakan dan protokol mentransfer banyak data penting privasi. Dengan menganalisis data ini, musuh mampu menghasilkan profil pengguna rinci. layanan anonim telah diusulkan dan dilaksanakan untuk menggagalkan ancaman terhadap privasi. Log file anonymi tawaran yang sangat sederhana, user-transparan dan efisien solusi, tapi pengguna tidak dapat mengontrol kegiatan anonim. proxy server yang didukung browser menawarkan langkah-langkah sederhana dan efisien juga. layanan anonim yang dilakukan pada sisi klien dan, karenanya, dikendalikan. Tapi mereka tidak dapat digunakan di belakang firewall dan mereka tidak mendukung anonimitas terhadap pihak ketiga. Fitur-fitur diuraikan dapat ditawarkan oleh Web-anonymizers. Mereka dapat digunakan di belakang firewall dan dukungan dienkripsi transfer data. Tapi Web-anonymi menderita tindakan anonim lambat dan rumit. Email dan berita biasanya anonim dengan menggunakan remailers, tetapi informasi tentang pengirim ditransfer disembunyikan untuk remailer dan kelebihan beban atau tidak tersedia remailer mungkin menyebabkan penundaan pesan tidak dapat diterima. Analisis kami dari layanan kerahasiaanya tersedia mengungkapkan banyak kekurangan yang parah. Dalam proyek Anonymous kami telah mengimplementasikan layanan baru untuk mengatasi permasalahan yang ada.

**References**

[1] D.L. Chaum. Untraceable Electronic Mail, Return Addresses and Digital Pseudonyms. Communications of the ACM, 24(2):84, 1981.

[2] T. Demuth and A. Rieke. Securing the anonymity of content providers in the world wide web. In Security and Watermarking of Multimedia Contents, pages 494–502, San Jose, 1999.

[3] R. Fielding, J. Gettys, J. Mogul, H. Frystyk, and T. Berners-Lee. RFC 2068: Hypertext Transfer Protocol — HTTP/1.1, January 1997.

[4] B. Kantor and P. Lapsley. RFC977: Network news transfer protocol, February 1986.

[5] A. Pircher. Anonymity in the Internet. Technical Report, TU-München, Master Thesis (in german), August 2000.

[6] J. Postel. RFC 821: Simple mail transfer protocol, August 1982.

[7] J. Postel and J. K. Reynolds. RFC 959: File transfer protocol, October 1985.

[8] Michael K. Reiter and Aviel D. Rubin. Crowds: Anonymity for web transactions. ACM Transactions on Information and System Security, 1(1):66–92, 1998.