TEKNIK PENULISAN KARYA ILMIAH

NAMA : NADYA DAMAYANTI

NIM : 09011181520008

KELAS : SK2A

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2016

Pada pencarian paper saya di google scholar,

Menurut paper Hristo Bojinov, dia mempersembahkan sebuah pendekatan baru identifikasi alat yang diperbolehkan untuk menggunakan alat tanpa bergantung pada pengidentifikasi halus. Metode pengambilan sidik jari variasi sensor eksploitasi kalibrasi di sistem speaker-microphone dan di accelerometer. Harapannya dari hasil ilustrasi tersebut memberikan akses kode tidak terpercaya untuk hardware jinak.

Menurut paper Desmond C.C Loh, mengusulkan sebuah teknik baru pengambilan sidik jari bahwa perbedaan antara perbedaan lebih nirkabel unik Local Area Network simple melalui waktu analisis dari 802.11 menyelediki permintaan rangka. Teknik ini bisa digunakan untuk mendeteksi penipuan, pengintaian jaringan, dan implementasi dari mengontrol akses terhadap serangan penyamar. Perbedaan ini dengan adanya teknik wireless fingerprinting, teknik ini pasif, non-invasive, dan tidak memerlukan kerjasama dari fingerprinting hosts.

Menurut paper Nikita Borisov, Standar 802.11 untuk jaringan nirkabel termasuk Equivalent Wired Privacy (WEP) protocol, digunakan untuk melindungi komunikasi link-layer dari menguping dan serangan lainnya. Kami telah menemukan beberapa kelemahan keamanan yang serius dalam protokol, yang berasal dari penyalahgunaan primitif dari kriptografi. Kekurangan menyebabkan angka serangan praktis yang menunjukkan bahwa WEP gagal untuk mencapai tujuan keamanan. Dalam tulisan ini membahas secara rinci masing-masing kelemahan, yang mendasari pelanggaran prinsip keamanan, dan berikutnya serangan.

Menurut paper Qing Li, kami telah menyajikan alternatif untuk tradisional metode otentikasi identitas berorientasi untuk mendeteksi perangkat spoofing pada jaringan nirkabel. Strategi kami menggunakan hubungan yang ada dalam aliran paket yang datang dari individu identitas jaringan. Setiap kali musuh parodi tertentu identitas, keberadaan beberapa sumber yang menyebabkan hubungan ini menjadi sulit bagi musuh untuk menempa. Akibatnya, menjadi kemungkinan bahwa musuh akan mengungkapkannya. Diusulkan dua keluarga yang berbeda dari hubungan yang cocok untuk jaringan nirkabel. Keluarga pertama melibatkan memperkenalkan tambahan field dalam paket dikirimkan, sedangkan keluarga kedua melibatkan sifat implisit terkait dengan transmisi dan penerimaan paket. Secara khusus, kami mengusulkan penggunaan monotonisitas dari bidang nomor urut dan penggunaan dari bidang pengenal sementara yang berkembang sesuai dengan satu arah fungsi rantai. Selanjutnya, untuk hubungan berdasarkan implisit sifat-terkait paket, kami mengusulkan bahwa statistik lalu lintas interarrival dapat digunakan untuk mendeteksi skenario lalu lintas anomali. Kami menggambarkan bagaimana RRCCs ini dapat ditambah dengan pengukuran dari tingkat keparahan ancaman dalam rangka memfasilitasi multilevel klasifikasi. Dalam semua kasus, kita menggunakan hubungan ini untuk membangun menempa tahan konsistensi cek (RRCCs) untuk mendeteksi anomali tingkah laku. RRCC kami tidak memerlukan penggunaan eksplisit atau pembentukan kunci kriptografi dan, dengan demikian, RRCCs cocok untuk skenario aplikasi mana pemeliharaan materi tidak praktis. Kami mendukung validitas diusulkan kami metode melalui percobaan yang dilakukan pada ORBIT 802.11 test jaringan nirkabel.

Menurut paper Bartlomiej Sieka, makalah ini menyajikan suatu metode untuk mengidentifikasi 802,11 node. itu menggunakan pengukuran waktu yang tepat bersama-sama dengan metode statistik dan Support Vector Machine (SVM) classifier untuk mengklasifikasikan komunikasi radio sebagai berasal dari transcelver yang diberikan. Tidak memerlukan perangkat keras khusus dan identifikasi tidak disengaja. Percobaan dilakukan dan menyajikan beberapa hasil klasifikasi awal. lima berbeda 802.11 perangkat sidik jari dengan tingkat keberhasilan 86%.

Menurut paper Steven J. Murdoch, layanan lokasi tersembunyi, seperti yang ditawarkan oleh sistem anonimitas seperti Tor, memungkinkan server untuk dioperasikan di bawah nama samaran. Sebagai Tor adalah sebuah jaringan overlay, server hosting tersembunyi dapat diakses baik secara langsung maupun melalui saluran anonim. pola lalu lintas melalui satu saluran memiliki diamati efek di sisi lain sehingga memungkinkan pseudonim, layanan ini identitas dan alamat IP yang akan dihubungkan. Salah satu solusi yang diusulkan untuk kerentanan ini adalah untuk Tor node untuk memberikan kualitas tetap pelayanan kepada setiap koneksi, terlepas dari lalu lintas lainnya, sehingga mengurangi kapasitas tetapi menolak gangguan tersebut serangan. Namun, bahkan jika setiap koneksi tidak berpengaruh yang lain, meskipun total masih akan mempengaruhi beban pada CPU, dan dengan demikian output panas nya. Sayangnya untuk anonimitas, hasil suhu pada jam condong dapat jarak jauh dideteksi melalui pengamatan cap waktu. serangan ini bekerja karena ada model abstrak anonymitynetwork node tidak memperhitungkan ketidaksempurnaan tak terelakkan perangkat keras mereka berjalan di. Selain itu, kami sarankan teknik yang sama dapat dimanfaatkan sebagai klasik channel rahasia dan bahkan dapat memberikan geolocation.

Menurut paper Liang Xiao, media nirkabel berisi informasi domain-spesifik yang dapat digunakan untuk melengkapi dan meningkatkan tradisional mekanisme keamanan. Dalam tulisan ini kami mengusulkan cara untuk mengeksploitasi variabilitas spasial respon saluran radio dalam lingkungan hamburan kaya, seperti khas lingkungan dalam ruangan. Secara khusus, kami menjelaskan algoritma otentikasi fisik-lapisan yang memanfaatkan saluran menyelidik dan pengujian hipotesis untuk menentukan apakah upaya komunikasi saat ini dan sebelumnya dibuat oleh terminal mengirimkan sama. Dengan cara ini, pengguna yang sah dapat diandalkan dikonfirmasi dan pengguna palsu dapat diandalkan terdeteksi. Kami menganalisis kemampuan penerima untuk membedakan antara pemancar (pengguna) sesuai dengan frekuensi saluran mereka tanggapan. Karya ini didasarkan pada respon saluran umum dengan kedua variabilitas spasial dan temporal, dan menganggap korelasi antara waktu, frekuensi dan domain spasial. Simulasi hasil, menggunakan alat ray-tracing WiSE untuk menghasilkan waktu respon rata-rata, memverifikasi efektivitas pendekatan di bawah kondisi saluran yang realistis, serta kemampuan untuk bekerja di bawah variasi channel diketahui.

Menurut paper Chang-Tsun Li, melakukan eksplorasi besar-besaran pengidentifikasi umum dan menghitung jumlah host mengidentifikasi informasi yang mereka ungkapkan. Data set dari Hotmail dan Bing, menunjukkan bahwa umum pengidentifikasi dapat membantu melacak host dengan presisi tinggi dan ingat. Studi kami juga menginformasikan penyedia layanan dari informasi potensi kebocoran ketika mereka anonim dataset (misalnya, mengganti alamat IP dengan awalan IP) dan merilis data untuk kolaborator pihak ketiga atau

ke publik. Sebagai contoh, kami menunjukkan bahwa hash browser informasi (yaitu, string UA yang anonim) saja bisa cukup mengungkapkan ketika diperiksa dalam satu domain jaringan. Selanjutnya, kasar awalan IP mencapai akurasi yang sama host-pelacakan dengan yang alamat IP yang tepat informasi ketika mereka dikombinasikan dengan hash string UA.

Menurut paper Kai San Choi, Identifikasi sumber kamera adalah proses cerdas yang kamera telah digunakan untuk menangkap tertentu gambar. Dalam tulisan ini, kita mempertimbangkan masalah yang lebih mendasar mencoba untuk mengklasifikasikan gambar yang ditangkap oleh sejumlah model kamera. Terinspirasi oleh karya sebelumnya yang menggunakan sensor ketidaksempurnaan, kami mengusulkan untuk menggunakan penyimpangan lensa intrinsik sebagai fitur dalam klasifikasi. Secara khusus, kita fokus pada lensa radial distorsi sebagai ciri khas utama. Untuk setiap gambar dalam penyelidikan, parameter dari intensitas pixel dan pengukuran penyimpangan diperoleh. Kami kemudian mempekerjakan classifier untuk mengidentifikasi kamera sumber gambar. Simulasi dilakukan untuk mengevaluasi tingkat keberhasilan metode kami. Hasil penelitian menunjukkan bahwa ini adalah layak Prosedur dalam identifikasi sumber kamera dengan probabilitas tinggi akurasi. Membandingkan dengan prosedur hanya menggunakan intensitas gambar, pendekatan kami meningkatkan akurasi dari 87% menjadi 91%.

Menurut paper Roberto Caldelli, Membedakan jenis sensor yang telah mengakuisisi citra digital bisa menjadi penting dalam banyak skenario di mana teknik forensik digital dipanggil untuk memberikan jawaban. Sebuah metodologi baru yang memungkinkan untuk menentukan apakah foto digital telah diambil oleh kamera atau telah dipindai oleh scanner diusulkan. seperti teknik mengeksploitasi fitur geometris tertentu dari kebisingan pola sensor diperkenalkan oleh sensor dalam kedua kasus dan dengan beralih ke analisis frekuensi dapat menyimpulkan jika periodisitas hadir dan akibatnya yang merupakan asal dari konten digital. hasil eksperimen disajikan untuk mendukung kerangka teoritis.

Menurut paper Mo Chen, kami menyediakan kerangka kerja terpadu untuk mengidentifikasi kamera digital sumber dari gambar dan untuk mengungkapkan gambar digital diubah menggunakan foto-respon non-keseragaman suara (PRNU), yang merupakan sidik jari stochastic yang unik dari sensor pencitraan. The PRNU diperoleh dengan menggunakan estimator Kemungkinan Maksimum berasal dari model sederhana dari output sensor. Kedua forensik tugas digital kemudian dicapai dengan mendeteksi keberadaan sensor PRNU di daerah tertentu dari gambar di bawah penyelidikan. deteksi dirumuskan sebagai masalah pengujian hipotesis. Distribusi statistik dari statistik uji optimal diperoleh dengan menggunakan prediktor statistik uji pada blok gambar kecil. prediktor yang memungkinkan akurat dan bermakna estimasi lebih dari probabilitas penolakan palsu kamera yang benar dan deteksi terjawab dari wilayah dirusak. Kami juga mencakup penerapan tolok ukur kerangka ini dan rinci validasi eksperimental. Kekokohan metode forensik yang diusulkan diuji pada pengolahan citra umum, seperti kompresi JPEG, koreksi gamma, mengubah ukuran, dan denoising.

Menurut paper Nitin Khanna, gambar digital dapat ditangkap atau yang dihasilkan oleh berbagai sumber termasuk kamera digital, scanner dan komputer software grafis. Dalam

banyak kasus itu adalah penting untuk dapat untuk menentukan sumber gambar digital seperti untuk pidana dan investigasi forensik. Makalah ini menyajikan metode untuk membedakan antara gambar yang diambil menggunakan digital kamera, komputer yang dihasilkan gambar dan gambar yang diambil menggunakan scanner. Metode yang diusulkan di sini didasarkan pada perbedaan dalam proses generasi gambar yang digunakan dalam ini perangkat dan independen dari konten gambar. Metode didasarkan pada menggunakan fitur suara pola residual yang ada di gambar yang diperoleh dari kamera digital dan scanner. Sisa suara hadir di komputer gambar yang dihasilkan tidak memiliki struktur yang mirip dengan suara pola kamera dan scanner. Percobaan menunjukkan bahwa fitur berbasis pendekatan menggunakan classifier SVM memberikan akurasi yang tinggi.

Menurut paper Hong Mei Gou, Sebagian besar gambar digital yang tersedia saat ini mengakuisisi menggunakan kamera digital atau scanner. Sementara kamera menyediakan reproduksi digital dari pemandangan alam, scanner sering digunakan untuk menangkap hard-copy art di lingkungan yang lebih terkontrol. Dalam tulisan ini, teknik-teknik baru untuk forensik scanner nonintrusive yang memanfaatkan intrinsik fitur sensor suara yang diusulkan untuk memverifikasi sumber dan integritas scan gambar digital. Scanning kebisingan dianalisis dari beberapa aspek menggunakan sampel gambar hanya dipindai, termasuk melalui denoising gambar, analisis wavelet, dan prediksi lingkungan, dan kemudian mendapatkan fitur statistik dari masing-masing karakterisasi. Berdasarkan fitur statistik yang diusulkan pemindaian kebisingan, pengenal scanner yang kuat dibangun untuk menentukan model / merek dari pemindai yang digunakan untuk menangkap gambar yang dipindai. Memanfaatkan fitur noise ini, kami memperluas ruang lingkup forensik akuisisi untuk membedakan scan gambar dari foto kamera-diambil dan grafis yang dihasilkan komputer. Kebisingan diusulkan fitur juga memungkinkan gangguan forensik untuk mendeteksi operasi postprocessing gambar dipindai. hasil eksperimen disajikan untuk menunjukkan efektivitas dari mempekerjakan fitur noise yang diusulkan untuk melakukan berbagai analisis forensik pada scanner dan scan gambar.

Menurut paper Pravin Prabhu, mengevaluasi tujuh teknik untuk mengekstraksi tanda tangan yang unik dari perangkat flash NAND berdasarkan efek diamati dari variasi proses. empat dari teknik menghasilkan tanda tangan yang dapat digunakan yang mewakili berbagai trade-off antara kecepatan, ketahanan, keacakan, dan memakai dikenakan pada perangkat flash. Kami menggambarkan bagaimana menggunakan tanda tangan untuk mencegah pemalsuan dan unik mengidentifikasi dan atau otentikasi perangkat elektronik.

Menurut paper Blaise Gassend, dia menjelaskan gagasan dari Physical Random Function (PUF) dan menunjukan bahwa sebuah silicon PUF bisa di buat. Dia menjelaskan pendahuluan analisis dari masalah tersebut dan percobaan dia menunjukkan model bangunan itu susah dengan butuh ketelitian tapi lebih butuh kerja untuk menyelesaikan kedua analisis dan percobaan.

Menurut paper Jae W. Lee, Makalah ini menjelaskan teknik yang mengeksploitasi variasi delay statistik kabel dan transistor di IC untuk membangun kunci rahasia unik untuk setiap IC. Untuk menguji kelayakan, kami buat sirkuit kandidat untuk menghasilkan respon

berdasarkan karakteristik delay-nya. Kami menunjukkan bahwa ada variasi delay yang cukup di IC melaksanakan rangkaian diusulkan untuk mengidentifikasi IC individu. Selanjutnya, fungsi sirkuit andal selama rentang praktis variasi lingkungan seperti suhu dan tegangan.

Menurut paper Sergey Morozov, Makalah ini menjelaskan teknik yang mengeksploitasi variasi delay statistik kabel dan transistor di IC untuk membangun kunci rahasia unik untuk setiap IC. Untuk menjelajahi nya kelayakan, kami dibuat sirkuit kandidat untuk menghasilkan respon berdasarkan karakteristik delay-nya. Kami menunjukkan bahwa ada variasi delay yang cukup di IC melaksanakan rangkaian diusulkan untuk mengidentifikasi IC individu. Selanjutnya, fungsi sirkuit andal selama rentang praktis variasi lingkungan seperti suhu dan tegangan.

Menurut paper Daniel E. Holcomb, aplikasi RFID menciptakan kebutuhan untuk penerbangan murah keamanan dan privasi di lingkungan berpotensi bermusuhan. Pengukuran menunjukkan bahwa inisialisasi SRAM menghasilkan sidik jari fisik. Kami mengusulkan sistem Fingerprint Ekstraksi dan Nomor Acak di SRAM (FERNS) yang panen identitas statis dan keacakan dari yang ada volatil penyimpanan CMOS. identitas hasil dari pembuatan-waktu secara fisik perangkat acak ambang mismatch, dan hasil angka acak dari run-time secara fisik gangguan acak. Kami menggunakan data eksperimen dari tags virtual, memori mikrokontroler, dan tag WISP UHF RFID untuk memvalidasi prinsip di balik pakis. Kami menunjukkan bahwa SRAM 256byte dapat digunakan untuk mengidentifikasi sirkuit antara populasi 160 tag virtual, dan berpotensi dapat menghasilkan angka 128bit random mampu melewati uji statistik kriptografi.

Menurut paper G. Edward Suh, Fisik Fungsi Unclonable (PUFS) adalah sirkuit yang inovatif primitif yang mengambil rahasia dari karakteristik fisik sirkuit terpadu (IC). Kami menyajikan desain PUF yang mengeksploitasi karakteristik delay melekat kabel dan transistor yang berbeda dari chip ke chip, dan menggambarkan bagaimana PUFS dapat mengaktifkan murah otentikasi IC individu dan menghasilkan kunci rahasia volatile untuk operasi kriptografi.

Menurut paper Ting-Fang Yen, banyak layanan web bertujuan untuk melacak klien sebagai dasar untuk menganalisis perilaku mereka dan memberikan personalisasi jasa. Meskipun banyak perdebatan mengenai koleksi informasi klien, ada beberapa kuantitatif studi yang menganalisis efektivitas host-pelacakan dan privasi terkait risiko. Dalam tulisan ini, kami melakukan studi skala besar untuk mengukur jumlah informasi yang diungkapkan oleh tuan rumah umum pengidentifikasi. Kami menganalisis dataset anonim sebulan dikumpulkan oleh layanan web-mail Hotmail dan Bing mesin pencari, yang meliputi jutaan host di seluruh ruang alamat IP global. Dalam pengaturan ini, kita membandingkan menggunakan beberapa pengenal, termasuk informasi peramban, alamat IP, cookies, dan ID pengguna login. Kami lebih menunjukkan privasi dan keamanan implikasi host-pelacakan dalam dua konteks. Pada bagian pertama, kita mempelajari penyebab cookie churn dalam layanan web, dan menunjukkan bahwa banyak pengguna yang kembali masih dapat dilacak bahkan jika mereka menghapus cookie atau menggunakan private browsing. Dalam kedua, kami menunjukkan bahwa host-pelacakan dapat dimanfaatkan untuk meningkatkan keamanan. Secara khusus,

oleh informasi menggabungkan di host, kita mengungkap serangan berbahaya tersembunyi terkait dengan lebih dari 75.000 akun bot yang meneruskan cookies untuk lokasi didistribusikan.

Menurut paper Jeyanthi Hall, Radio Frequency Fingerprinting (RFF) adalah teknik, yang telah digunakan untuk mengidentifikasi perangkat nirkabel. Ini pada dasarnya melibatkan deteksi sinyal transien dan ekstraksi sidik jari. Fase deteksi, di pendapat kami, adalah bagian belum penting paling menantang dari proses RFF. Pendekatan saat ini, yaitu Threshold dan Langkah Bayesian Perubahan Detector, yang menggunakan karakteristik amplitudo sinyal untuk deteksi sementara, berkinerja buruk dengan jenis tertentu dari sinyal. Makalah ini menyajikan algoritma baru yang memanfaatkan karakteristik fase untuk deteksi tujuan. Validasi menggunakan sinyal Bluetooth telah menghasilkan di tingkat keberhasilan sekitar 85-90 persen. Kami mengantisipasi bahwa tingkat deteksi yang lebih tinggi akan menghasilkan lebih tinggi tingkat klasifikasi dan dengan demikian mendukung berbagai perangkat authetication skema dalam domain nirkabel.

Menurut paper Tadayoshi Kohno, memperkenalkan daerah terpencil sidik jari perangkat fisik, atau sidik jari fisik perangkat, sebagai lawan dari sistem operasi atau kelas perangkat, jarak jauh, dan tanpa jari kerjasama diketahui perangkat cetak ini. Kami mencapai tujuan ini dengan memanfaatkan kecil, mikroskopis penyimpangan dalam perangkat keras: jam skews. teknik kami tidak memerlukan modifikasi untuk perangkat sidik jarinya. teknik kami melaporkan pengukuran konsisten ketika ukur adalah ribuan mil, banyak hop, dan puluhan milidetik jauh dari perangkat sidik jari, dan ketika perangkat sidik jari terhubung ke Internet dari lokasi yang berbeda dan melalui teknologi akses yang berbeda. Selanjutnya, seseorang dapat menerapkan teknik pasif dan semi-pasif kami ketika perangkat sidik jari berada di belakang NAT atau firewall, dan juga ketika sistem perangkat Waktu dipertahankan melalui NTP atau SNTP. Satu dapat menggunakan teknik kami untuk memperoleh informasi tentang apakah dua perangkat di Internet, mungkin bergeser dalam waktu atau IP alamat, sebenarnya perangkat fisik yang sama. Contoh aplikasi meliputi: forensik komputer; pelacakan, dengan beberapa probabilitas, perangkat fisik seperti menghubungkan ke Internet dari titik akses publik yang berbeda; menghitung jumlah perangkat belakang NAT bahkan ketika perangkat menggunakan konstan atau random IP ID; jarak jauh menyelidik blok alamat untuk menentukan apakah alamat sesuai dengan maya host, misalnya, sebagai bagian dari Honeynet virtual; dan unanonymizing jejak jaringan anonim.

Menurut paper Jeffrey Pang, 802.11 perangkat dan jaringan memungkinkan siapa pun untuk melacak setiap gerakan dengan mudah. Setiap perangkat 802.11 mentransmisikan alamat MAC global yang unik dan gigih dan dengan demikian adalah diidentifikasi. Sebagai tanggapan, penelitian terbaru telah diusulkan menggantikan pengenal tersebut dengan nama samaran (yaitu, sementara, unlinkable nama). Dalam tulisan ini, kami menunjukkan bahwa nama samaran yang cukup untuk mencegah pelacakan dari 802.11 perangkat karena implisit pengidentifikasi, atau ciri dari 802.11 lalu lintas, dapat mengidentifikasi banyak pengguna dengan akurasi yang tinggi. Misalnya, bahkan tanpa nama yang unik dan alamat, kami memperkirakan bahwa musuh bisa mengidentifikasi 64% dari pengguna dengan akurasi 90% ketika mereka menghabiskan hari pada sibuk hot spot. Kami menyajikan prosedur otomatis

berdasarkan empat pengidentifikasi implisit yang sebelumnya tidak dikenal yang dapat mengidentifikasi pengguna di tiga 802.11 jejak nyata bahkan ketika nama samaran dan enkripsi dipekerjakan. Kami menemukan bahwa mayoritas pengguna dapat diidentifikasi menggunakan teknik kami, tapi kemampuan kita untuk mengidentifikasi pengguna adalah tidak seragam; beberapa pengguna tidak mudah diidentifikasi. Meskipun begitu, kami menunjukkan bahwa bahkan identifier implisit tunggal cukup untuk membedakan banyak pengguna. Oleh karena itu, kami berpendapat bahwa pertimbangan desain melampaui menghilangkan pengidentifikasi eksplisit (yaitu, nama yang unik dan alamat), harus diatasi untuk mencegah pelacakan pengguna di jaringan nirkabel.

Menurut paper Kevin Simler, analisis perilaku pengguna dan pola mobilitas berdasarkan jejak akses ke server departemen e-mail. Berbeda dengan sebelumnya, kami mempertimbangkan layanan tunggal dan meneliti bagaimana komunitas pengguna terhubung itu sambil bergerak di berbagai nirkabel penyedia layanan yang berbeda dan kabel jaringan. Dengan mengukur layanan e-mail mampu memantau sejumlah besar sesi berasal dari satu set beragam lokasi karena e-mail adalah salah satu dari beberapa layanan yang pengguna biasa mengakses. Kontribusi kami meliputi: pendekatan yang unik untuk penggalian informasi mobilitas pengguna dari jejak interaksi aplikasi klien; pendekatan baru untuk pemodelan perilaku pengguna dan mobilitas; dan demonstrasi bagaimana model tersebut dapat digunakan untuk menghasilkan jejak sintetis. Secara keseluruhan, meskipun beberapa pengguna sangat mobile, kita menemukan sebagian besar pengguna memiliki tingkat rendah mobilitas - 70% dari pengguna mengakses e-mail mereka dari 2 atau lebih sedikit lokasi yang unik. Kami juga menemukan bahwa kita diamati dengan sesi yang lebih lama dari yang dilaporkan oleh studi mobilitas sebelumnya dalam jaringan nirkabel.

Menurut paper Kasper Bonne Rasmussen, menunjukkan kelayakan jari mencetak radio node sensor nirkabel (Chipcon 1000 radio, 433MHz). Kami menunjukkan bahwa, dengan jenis perangkat, penerima dapat membuat radio perangkat jari cetakan dan kemudian mengidentifikasi asal-usul pesan berubah antara perangkat, bahkan jika isi pesan dan pengenal perangkat yang tersembunyi. Kami menganalisis lebih lanjut implikasi dari perangkat sidik jari pada keamanan protokol sensor jaringan, khususnya, kami mengusulkan dua mekanisme baru untuk mendeteksi lubang cacing di jaringan sensor.

Menurut paper Vladimir Brik, merancang, melaksanakan, dan mengevaluasi teknik untuk mengidentifikasi kartu antarmuka jaringan sumber (NIC) dari IEEE 802.11 membingkai melalui analisis frekuensi radio pasif. Teknik ini, disebut PARADIS, memanfaatkan ketidaksempurnaan menit hardware transmitter yang diperoleh pada pembuatan dan hadir bahkan dalam NIC dinyatakan identik. Ketidaksempurnaan ini adalah transmitter-spesifik dan menampakkan diri sebagai artefak dari sinyal yang dipancarkan. Dalam PARADIS, kita mengukur membedakan artefak frame nirkabel individu dalam modulasi domain, menerapkan klasifikasi mesin-belajar yang cocok alat untuk mencapai derajat lebih tinggi secara signifikan dari NIC akurasi identifikasi dari skema sebelumnya dikenal. Kami eksperimen menunjukkan efektivitas PARADIS dalam membedakan antara lebih dari 130 identik 802.11 NIC dengan akurasi lebih dari 99%. Hasil kami juga menunjukkan bahwa keakuratan PARADIS adalah tahan terhadap kebisingan dan fluktuasi dari saluran nirkabel. Meskipun

penawaran implementasi kami secara eksklusif dengan IEEE 802.11, pendekatan itu sendiri umum dan akan bekerja dengan skema modulasi digital.

Menurut paper Daniel B. Faria, Jaringan nirkabel rentan terhadap serangan berbasis identitas banyak di mana perangkat berbahaya menggunakan ditempa alamat MAC untuk menyamar sebagai klien tertentu atau untuk membuat beberapa identitas sah. Misalnya, beberapa layanan link-layer di IEEE 802.11 jaringan telah terbukti rentan terhadap serangan tersebut bahkan ketika 802.11i / 1X dan mekanisme keamanan lainnya dikerahkan. Dalam makalah ini kami menunjukkan bahwa perangkat transmisi dapat kokoh diidentifikasi oleh signalprint, sebuah tuple dari kekuatan sinyal nilai-nilai yang dilaporkan oleh jalur akses bertindak sebagai sensor. Kami menunjukkan bahwa, dari alamat MAC atau isi paket lainnya, penyerang tidak memiliki banyak kontrol mengenai signalprints mereka hasilkan. Selain itu, menggunakan pengukuran dalam jaringan testbed, kami menunjukkan yang signalprints sangat berkorelasi dengan fisik lokasi klien, dengan nilai yang sama kebanyakan ditemukan di dekat. Dengan penandaan paket-paket mencurigakan dengan mereka sesuai signalprints, jaringan mampu kokoh mengidentifikasi setiap pemancar independen dari isi paket, yang memungkinkan deteksi kelas besar serangan berbasis identitas dengan probabilitas tinggi.

Menurut paper Jason Franklin, Termotivasi oleh proliferasi perangkat nirkabel diaktifkan dan sifat tersangka kode driver perangkat, kami mengembangkan teknik fingerprinting pasif yang mengidentifikasi driver perangkat nirkabel yang berjalan pada perangkat IEEE 802.11 compliant. Teknik ini berharga untuk seorang penyerang yang ingin melakukan pengintaian terhadap target potensial sehingga ia dapat meluncurkan driver-eksploitasi tertentu. Secara khusus, kami mengembangkan teknik fingerprinting unik yang akurat dan efisien mengidentifikasi driver wireless tanpa modifikasi atau kerja sama dari perangkat nirkabel. Kami melakukan evaluasi teknik fingerprinting ini yang menunjukkan keduanya cepat dan akurat sidik jari driver perangkat nirkabel dalam kondisi jaringan nirkabel dunia nyata. Akhirnya, kita membahas cara-cara untuk mencegah sidik jari yang akan membantu dalam meningkatkan keamanan komunikasi nirkabel untuk perangkat yang menggunakan 802,11 jaringan.

Menurut paper Neal Patwari, Kemampuan penerima untuk menentukan kapan pemancar lokasi telah berubah adalah penting untuk konservasi energi pada jaringan sensor nirkabel, untuk keamanan fisik radio benda tagged, dan untuk keamanan jaringan nirkabel di deteksi serangan replikasi. Dalam tulisan ini, kami mengusulkan tanda tangan tautan sementara diukur untuk mengidentifikasi secara unik hubungan antara pemancar dan penerima. Ketika pemancar perubahan lokasi, atau jika seorang penyerang di sebuah Lokasi mengasumsikan identitas pemancar, berpose algoritma Link perbedaan andal mendeteksi perubahan dalam saluran fisik. Deteksi ini bisa dilakukan pada penerima tunggal atau bersama-sama oleh beberapa penerima. Kami mencatat lebih dari 9.000 tanda tangan tautan di lokasi dan dari waktu ke waktu untuk menunjukkan bahwa metode kami meningkatkan tingkat deteksi dan mengurangi tingkat alarm palsu, dibandingkan dengan metode yang ada.

Menurut paper Ryan M. Gerdes, Sebagai bagian dari intrusi Mendeteksi pada Layer Satu (Dilon) proyek, kami menunjukkan bahwa perangkat Ethernet dapat unik diidentifikasi dan

dilacak menggunakan sesedikit 25 Ethernet frame dengan menganalisis variasi dalam sinyal analog mereka disebabkan oleh hardware dan manufaktur inkonsistensi. Sebuah detektor optimal, filter cocok, digunakan untuk membuat sinyal profil, yang membantu dalam mengidentifikasi perangkat sinyal berasal dari beberapa aplikasi non-tradisional Filter disajikan dalam rangka meningkatkan kemampuannya untuk membedakan antara sinyal dari perangkat tampaknya identik dari banyak manufaktur yang sama. Hasil eksperimen menerapkan filter ini untuk tiga model yang berbeda dari Ethernet kartu, total 16 perangkat, disajikan dan dibahas. Aplikasi penting dari teknologi ini termasuk intruksi deteksi (menemukan peniruan simpul dan jaringan sabotase), otentikasi (mencegah tidak sah akses ke jaringan fisik), pengumpulan data forensik (mengikat perangkat fisik untuk insiden jaringan tertentu), dan monitoring jaminan (menentukan apakah perangkat akan atau dalam proses gagal).

MIND MAP MOBILE DEVICE IDENTIFICATION VIA SENSOR FINGERPRINTING.