**Multi-stage Attack Detection and Signature Generation with ICS Honeypots**

Emmanouil Vasilomanolakis, Shreyas Srinivasa, Carlos Garcia Cordero, Max Muhlhauser

Seiring berkembangnya Industrial Control System (ICS), banyak ditemukan serangan bertahap *(multi-stage attack)* terhadap jaringan ICS. Perangkat ICS harus dapat dilindungi secara holistik dan efisien, terutama ketika perangkat ini merupakan pendukung sebuah infrastruktur penting. Sistem Deteksi Intrusi (IDS) saat ini dianggap sebagai garis pertahanan wajib untuk perlindungan jaringan kritis. Mayoritas IDS di jaringan dunia nyata secara pasif memantau dan melakukan deteksi berbasis tanda tangan.

Honeypots adalah sistem yang hanya memiliki nilai yang harus diselidiki, diserang, dan dikompromikan. Tujuannya adalah untuk menarik pengguna jahat, mempelajari aktivitas mereka, dan pada saat yang sama, mengurangi serangan di permukaan. Penting untuk diketahui bahwa karena honeypots tidak menampilkan tujuan lain, menurut definisi, interaksi apa pun dengan mereka dianggap sebagai serangan. Dengan demikian, mereka tidak menunjukkan false positive, yaitu, semua lalu lintas masuk dianggap berbahaya.

Pada kasus ini, digunakan metode HosTaGe, yang merupakan *open-source low-interaction mobile Honeypot*. HosTaGe ini adalah honeypots portabel ringan untuk perangkat seluler yang bertujuan mendeteksi perangkat jahat di jaringan nirkabel. Mekanisme deteksi yang digunakan dapat membedakan 3 serangan yang berbeda, salah satunya MSLD *(Multi Stage Level Detection)*. MSLD mengacu pada serangan yang berasal dari sumber yang sama dan upaya untuk mengeksploitasi berbagai jenis protokol dalam rentang waktu yang kecil, tipe ini dapat diidentifikasi oleh Honeypot dengan EFSM. ICS memiliki emulasi protokol spesifik, untuk meningkatkan kemampuan emulasi protokol HosTaGe dengan menambahkan (atau meningkatkan) dukungan untuk protokol yang digunakan dalam ICS, seperti *Modbus, S7, SNMP, HTTP, Telnet, SMB* dan *SMTP*.

Dalam penggunaannya, Honeypot dapat mendeteksi serangan pada jaringan ICS dengan mekanisme deteksi EFSM dan mendapatkan tanda dari serangan yang diamati. Namun, honeypots dalam penggunaannya diperiksa oleh mesin pencarian tertentu, yaitu Shodan. Shodan adalah mesin pencari khusus yang menjelajah internet dan berupaya mengidentifikasi perangkat yang terhubung.

**N-BaIoT: Network-based Detection of IoT Botnet Attacks Using Deep Autoencoders**

Yair Meidan, Michael Bohadana, Yael Mathov, Yisroel Mirsky, Dominik Breitenbacher, Asaf Shabtai, and Yuval Elovici

Proliferasi perangkat IoT yang dapat lebih mudah untuk terkena serangan botnet berbasis IoT. Untuk mengurangi ancaman baru ini, ada kebutuhan untuk mengembangkan metode baru untuk mendeteksi serangan yang diluncurkan dari perangkat IoT yang dikompromikan dan membedakan antara serangan berbasis IoT selama satu jam dan milidetik.

Metode yang ingin digunakan untuk mendeteksi serangan botnet IoT dilakukan pendekatan berbasis jaringan yang menggunakan teknik deep learning untuk mendeteksi kegiatan anomali. Hal ini bergantung pada autoencoder dalam untuk setiap perangkat, dilatih pada fitur statistik yang diekstraksi dari data lalu lintas jinak. Ketika diterapkan pada data baru (mungkin terinfeksi) dari perangkat IoT, anomali yang terdeteksi dapat menunjukkan bahwa perangkat tersebut dikompromikan. Metode ini terdiri dari tahapan utama berikut ini:

1. pengumpulan data,
2. ekstraksi fitur,
3. pelatihan detektor anomali,
4. pemantauan terus menerus.

Deep autoencoder akan mencoba mengkompresi snapshot, ketika autoencoder gagal merekonstruksi snapshot, maka itu merupakan indikasi kuat bahwa perilaku yang diamati adalah anomali. Prediktabilitas perilaku lalu lintas dapat langsung diterjemahkan ke dalam ukuran kinerja deteksi anomali. Sebagai contoh, perangkat IoT dengan tingkat prediksi lalu lintas yang tinggi akan membuat tindakan aneh terlihat menonjol, dan karenanya TPR akan meningkat dan waktu deteksi akan berkurang dalam kasus ini. Untuk validasi empiris kami mengekstraksi fitur statis dan dinamis dari set pelatihan (jinak).

Sebagai pengembangan metode ini, direncanakan untuk mengevaluasi teknik pembelajaran transfer dengan menilai keakuratan model yang dilatih pada perangkat tertentu ketika mereka diterapkan pada perangkat yang identik, mungkin ketika terhubung ke jaringan organisasi lain. Ini dapat membantu (1) menghemat waktu (misalnya, organisasi dapat menggunakan model yang telah dipelajari sebelumnya di tempat lain, tanpa perlu mengumpulkan data dan melatih model itu sendiri), dan (2) mendeteksi perangkat IoT yang dikompromikan yang telah terkontaminasi sebelum menghubungkan ke organisasi. jaringan, sehingga organisasi tidak memiliki data jinak dari mereka untuk pelatihan model.

**Robust Malware Detection for Internet Of (Battlefield) Things Devices Using Deep Eigenspace Learning**

Amin Azmoodeh, Ali Dehghantanha, Senior Member, IEEE, and Kim-Kwang Raymond Choo, Senior Member, IEEE,

Internet of Things (IoT) dalam pengaturan militer umumnya terdiri dari beragam perangkat dan node yang terhubung ke internet (contoh perangkat medis untuk mengenakan seragam tempur yang dapat dipakai), yang merupakan target berharga bagi penjahat cyber, terutama yang disponsori negara atau penjahat negara. Serangan paling umum yang digunakan adalah penggunaan malware.

Baru-baru ini ada minat dalam memanfaatkan *machine learning* dan teknik *deep learning* dalam deteksi malware (misal membedakan antara aplikasi malware dan jinak), karena potensi mereka untuk meningkatkan akurasi dan ketahanan. Biasanya, kriteria berikut digunakan untuk mengevaluasi utilitas pembelajaran mesin dan teknik pembelajaran mendalam dalam deteksi malware:

• True Positive (TP): menunjukkan bahwa malware diidentifikasi dengan benar sebagai aplikasi jahat.

• True Negative (TN): menunjukkan bahwa suatu jinak terdeteksi sebagai aplikasi yang tidak berbahaya dengan benar.

• False Positive (FP): menunjukkan bahwa jinak terdeteksi secara salah sebagai aplikasi jahat.

• False Negative (FN): menunjukkan bahwa malware tidak terdeteksi dan dilabeli sebagai aplikasi yang tidak berbahaya.

Metode deep learning untuk mendeteksi malware Internet Of Battlefield Things (IoBT) melalui urutan Kode Operasional (OpCode) perangkat. OpCodes ditransmisikan ke dalam ruang vektor dan menerapkan pendekatan deep Eigenspace learning untuk mengklasifikasikan aplikasi jahat dan berbahaya.

Eigenspace deep learning adalah grafik sebagai struktur data yang kompleks untuk mewakili hubungan antar simpul adalah tipe data yang lazim dalam pembelajaran mesin. Ada sangat sedikit data mining dan algoritma pembelajaran mendalam yang menerima grafik sebagai input. Oleh karena itu, alternatif yang memungkinkan adalah menanamkan grafik ke dalam ruang vektor. Memang, embedding grafik adalah jembatan antara pengenalan pola statistik dan penambangan grafik. Vektor eigen dan nilai eigen adalah dua elemen karakteristik dalam spektrum grafik, yang secara linear dapat mengubah matriks adjacency grafik menjadi ruang vektor.

Hasil pendekatan pendeteksian malware IoT dan IoBT dilakukan berdasarkan pilihan sekuensial dari urutan OpCodes sebagai fitur untuk tugas klasifikasi. Grafik fitur yang dipilih dibuat untuk setiap sampel dan pendekatan deep Eigenspace learning digunakan untuk klasifikasi malware. Hasil evaluasi menunjukkan kekuatan pendekatan dalam deteksi malware dengan akurasi 98.37% dan tingkat presisi 98.59%, serta memiliki kemampuan untuk mengurangi serangan penyisipan kode sampah.

**IoT Malware: Comprehensive Survey, Analysis Framework and Case Studies**

Andrei Costin, Jonas Zaddach

Malware komputer dalam semua bentuknya hampir setua PC pertama yang menjalankan OS komoditas, sejak setidaknya 30 tahun. Namun, jumlah dan variasi "perangkat komputasi" meningkat secara dramatis selama beberapa tahun terakhir. Oleh karena itu, fokus pembuat dan operator malware perlahan namun pasti mulai bergeser atau berkembang menuju malware Internet of Things (IoT).

Kurangnya alat yang tersedia adalah tantangan yang signifikan untuk analisis malware IoT. Meskipun ada kotak pasir untuk menganalisis malware Linux, emulator ada untuk meniru platform non-x86, dan alat ada untuk mengintrospeksi keadaan sistem, interaksi antara komponen paling sering tidak berfungsi dan memerlukan konfigurasi kecil dan rumit serta perubahan kode. Tujuan kami adalah untuk menyediakan kerangka kerja analisis dinamis yang mudah diatur, siap digunakan tanpa konfigurasi lebih lanjut, dan menyediakan jumlah IoC yang layak.

Kami membangun kotak pasir analisis dinamis kami berdasarkan sumber terbuka Cuckoo Sandbox. Malware dijalankan di emulator sistem Qemu. Sistem Linux di dalam emulator adalah kernel Linux yang dibuat khusus, yang diinstrumentasi dengan SystemTap dan runtime busybox. Membangun rantai alat dan perangkat lunak sistem dicapai dengan buildroot. Seluruh pengaturan dibundel sebagai wadah Docker, yang menjelaskan semua dependensi proyek dan menyederhanakan penyebaran.

Celeda et al. menjelaskan teknik untuk analisis dinamis malware Chuck Norris Botnet pada modem yang terinfeksi. Penulis menggunakan perangkat Linux khusus / dev / mem untuk mengambil konten memori. Perubahan konfigurasi ke sistem, seperti konfigurasi firewall iptables, dilacak secara manual. Modifikasi sistem file terbatas pada direktori / var, karena sistem file modem dipasang hanya-baca. Sampel dari penelitian ini tidak tersedia pada saat penulisan ini 7. Kami akan merilis set data kami secara publik dengan kontrol versi dan pelacakan perubahan sebagai dasar untuk peneliti lain.

Minn et al. menyajikan arsitektur honeypot telnet interaksi rendah untuk malware IoT. Setelah menangkap malware di honeypot, mereka selanjutnya menganalisis sampel dalam kotak pasir Qemu dengan perangkat lunak sistem buildroot berbasis OpenWRT. Sistem ini menjebak empat keluarga malware yang berbeda, di mana 17 binari dianalisis lebih lanjut. Meskipun data dari karya ini bersifat publik, perangkat lunaknya tidak, membuat perbandingan data paling sulit. Kami akan menerbitkan perangkat lunak kami bersama dengan data kami untuk memungkinkan peneliti lain perbandingan yang lebih nyaman dengan penelitian kami.

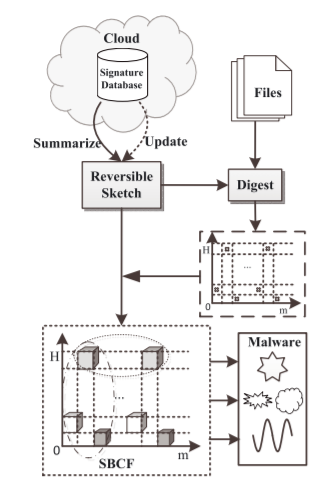
**CloudEyes: Cloud-based malware detection with reversible sketch for resource-constrained internet of things (IoT) devices**

Hao Sun, Xiaofeng Wang, Rajkumar Buyya, and Jinshu Su

The McAfee Labs menunjukkan serangan pada perangkat IoT akan meningkat dengan cepat karena pertumbuhan berlebih dalam jumlah objek yang terhubung, kebersihan keamanan yang buruk dan tingginya nilai data pada perangkat ini. Berbagai ancaman yang ada selama beberapa dekade, seperti Spam, Kebocoran Privasi, Botnet, Penyangkalan layanan dan Ancaman persisten tingkat lanjut, masih merajalela dalam paradigma IoT.

Adanya usulan tentang sistem anti-malware berbasis cloud, yang disebut CloudEyes, yang menyediakan layanan keamanan yang efisien dan tepercaya untuk perangkat yang terbatas sumber daya. Untuk server cloud, CloudEyes menghadirkan penyaringan silang ember yang mencurigakan, mekanisme deteksi tanda tangan baru berdasarkan pada struktur sketsa yang dapat dibalik, yang memberikan orientasi retrospektif dan akurat dari fragmen tanda tangan berbahaya. Untuk klien, CloudEyes mengimplementasikan agen pemindaian ringan yang memanfaatkan intis dari fragmen tanda tangan untuk secara dramatis mengurangi rentang pencocokan yang akurat. Selanjutnya, dengan mengirimkan koordinat sketsa dan hashing modular, CloudEyes menjamin privasi data dan komunikasi murah.

Untuk keluar dari konsumsi waktu yang tinggi, yang terutama disebabkan oleh jumlah besar tanda tangan, CloudEyes mengadopsi struktur sketsa reversibel untuk representasi dan orientasi tanda tangan yang efektif. Selain itu, ia merancang mekanisme interaktif seimbang untuk melindungi privasi data dan mengurangi konsumsi komunikasi.



**Lightweight Node-level Malware Detection and Network-level Malware Confinement in IoT Networks**

Sai Manoj Pudukotai Dinakarrao, Hossein Sayadi, Hosein Mohammadi Makrani, Cameron Nowzari, Setareh Rafatirad, and Houman Homayoun

Seiring dengan fungsionalitas utama komunikasi, perangkat IoT juga berbagi risiko keamanan yang mendasari Sistem CyberPhysical (CPS), tetapi lebih rentan terhadap serangan seperti itu karena keamanan sering diabaikan dalam desain perangkat IoT. Akibatnya, karena perangkat IoT sedang online dengan langkah-langkah perlindungan yang sangat minim, bahkan jika ada, membuat mereka terkena serangan cyber yang potensial. Ini membuat mereka rentan terhadap serangan keamanan, dan tidak layak untuk menggunakan deteksi perangkat berbasis perangkat lunak yang ada karena keterbatasan sumber daya. Lebih jauh, dari sudut pandang musuh, kelayakan untuk penyebaran malware melalui jaringan yang terhubung tanpa tindakan pertahanan yang dibangun dengan lemah, dan konektivitas yang luas menjadikan perangkat IoT target potensial untuk serangan. Serangan-serangan ini dapat ditargetkan pada berbagai perangkat seperti router dan CCTV.

Untuk pendeteksian malware diusulkan pendekatan dua cabang, di mana detektor malware runtime (HaRM) yang menggunakan nilai Hardware Performance Counter (HPC) untuk mendeteksi malware dan aplikasi jinak dibuat. Informasi ini diberikan selama runtime ke pengendali prediktif model stokastik untuk membatasi penyebaran malware tanpa menghambat kinerja jaringan. Dengan solusi yang diusulkan, akurasi deteksi malware runtime sebesar 92,21% dengan runtime 10ns tercapai, yang merupakan urutan besarnya lebih cepat daripada solusi deteksi malware yang ada. Mensintesiskan output ini dengan model strategi penahanan prediktif mengarah pada pencapaian throughput jaringan rata-rata hampir 200% dari jaringan IoT tanpa pertahanan yang tertanam.

**Evaluation of HaRM: Node-Level Malware Detection**

1. Malware Detection Accuracy

Akurasi Deteksi Malware dievaluasi ketika pengklasifikasi ML yang berbeda digunakan dalam kerangka kerja HaRM. Validasi silang 10 kali lipat digunakan untuk memverifikasi kinerja deteksi malware dengan fitur yang berkurang, misalnya HaRM. Untuk akurasi deteksi, kami menghitung nilai persentase sampel yang diklasifikasikan dengan benar.

1. Processing Overheads

Meskipun mayoritas pengklasifikasi yang dikerahkan telah menunjukkan akurasi deteksi malware yang memadai, konsumsi sumber daya dan latensi yang terlibat untuk deteksi malware memainkan peran penting dalam memilih model ML yang paling cocok untuk deteksi malware runtime di HaRM. Jejak perangkat keras HaRM dievaluasi pada FPGA untuk perbandingan yang adil. Kami menggunakan Vivado HLS untuk mengembangkan implementasi HDL dari classifiers (HaRM) dan menggunakan Xilinx Virtex 7 FPGA.

HaRM yang diusulkan menggunakan informasi on-chip HPC untuk mendeteksi malware tanpa menimbulkan overhead pemrosesan sambil memfasilitasi deteksi malware runtime. Sayangnya, karena algoritma pendeteksian malware tidak sempurna, outputnya tidak dapat langsung digunakan dalam masalah kontrol optimal teoritis.

**Combating Malware with Whitelisting in IoT-based Medical Devices**

Raghu Nallani Chakravartula, V. Naga Lakshmi, PhD

Malware di lingkungan IoT memiliki tantangan besar dikarenakan sistem yang saling berhubungan dan saling beroperasi. Solusi anti-malware berbasis tradisional signature tidak akan cukup untuk perangkat IoT berbasis perawatan kesehatan. Pendekatan baru menggunakan whitelisting di perangkat kesehatan medis berbasis IoT dan menggambarkan peningkatan kinerja dibandingkan solusi tradisional.

Penilaian kinerja solusi malware berbasis signature dibandingkan pendekatan whitelisting mengacu pada CPU, File IO, dan pemanfaatan memori. Grafik kinerja menunjukan dampak minimal pada CPU, File IO, dan pemanfaatan memori dengan dan tanpa solusi whitelisting. Mengimplementasikan whitelisting kedalam sistem pemantauan pasien dan mengukur kinerja terhadap baseline.

**Reassessing Android Malware Analysis: From Apps to IoT System Modelling**

Abraham Rodríguez-Mota, Ponciano Jorge Escamilla-Ambrosio, Jassim Happa, Eleazar Aguirre-Anaya

Aplikasi berbasis Internet of Things (IoT) semakin rentan terhadap gangguan dari serangan dunia maya. Pengembang dan peneliti berusaha untuk mencegah tumbuhnya model gangguan, mengurangi dan membatasi dampaknya. Menggunakan web tool bernama GARMDROID dan pemetaan data analisis malware ke SysML block definition diagram.

Visualisasi fitur yang diminta oleh aplikasi android dapat menyediakan pengetahuan tentang izin yang diminta oleh aplikasi. SysML Block Diagram berdasarkan fitur perangkat keras yang diminta oleh aplikasi menjadi cara yang layak untuk memasukan aspek keamanan.

Mengintegrasikan hasil penelitian ini dengan orang lain dari teknik yang lebih rumit, seperti Machine Learning, untuk memberikan analisis yang lebih rinci dan holistik.

**An SVEIR Defending Model with Partial Immunization for Worms**

Fangwei Wang, Hongfeng Gao, Yong Yang, and Changguang Wang

Cacing internet dapat menyebar dengan cepat ke seluruh jaringan, mengurangi keamanan jaringan, dan menyebabkan kerugian ekonomi yang besar. Makalah ini membahas masalah dengan menghadirkan model serangan cacing melalui penggabungan tingkat kejadian jenuh dan tingkat imunisasi parsial, bernama model SVEIR. Metode numerik digunakan untuk memecahkan dan mensimulasikan sistem yang dikembangkan dan juga memverifikasi model SVEIR yang diusulkan.

Analisis teoritis menunjukkan bahwa ketika jumlah reproduksi dasar lebih kecil dari atau sama dengan satu, model SVEIR memiliki keseimbangan bebas infeksi, dan secara global asimtotik stabil. Artinya, itu menyiratkan bahwa cacing akhirnya mati.

Hasil simulasi konsisten dengan analisis teoritis. Model SVEIR yang kami usulkan akan sangat berguna untuk menganalisis ketersediaan dan efisiensi imunisasi parsial. Imunisasi parsial akan efisien jika laju imunisasi parsial sangat kecil.

**Analysis of Security Mechanisms Based on Clusters IoT Environments**

Paulo Gaona-García , Carlos Montenegro-Marin , Juan David Prieto , Yuri Vanessa Nieto

Internet hal didasarkan pada sensor, komunikasi jaringan dan kecerdasan yang mengelola seluruh proses dan data yang dihasilkan. Sensor adalah indera sistem, karena ini, mereka dapat digunakan dalam jumlah besar. Sensor harus memiliki daya rendah konsumsi dan biaya, ukuran kecil dan fleksibilitas besar untuk penggunaannya di semua keadaan. Oleh karena itu, keamanan perangkat jaringan ini, sensor data dan perangkat lain, merupakan perhatian utama seiring pertumbuhannya cepat dalam hal node saling berhubungan melalui data sensor.

Untuk tujuan penelitian ini, diambil lima fiskal paling sering frasa, seperti: ‘IoT dan keamanan’, ‘Middleware’, ‘RFID’, ‘Internet’, ‘Komputasi cloud’, ‘Jaringan sensor nirkabel’ dan ‘6LoWPAN’.

Dalam kebanyakan kasus, informasi ini bergerak melalui jaringan nirkabel atau melalui jaringan publik, yang rentan terhadap serangan. Jika saluran komunikasi tidak dilindungi secara memadai dengan mengenkripsi data, bisa mudah bagi penyerang untuk melakukan serangan.

Sebagai pekerjaan masa depan, diramalkan akan melakukan karakterisasi ini masalah, sehingga dari model ontologis dan agen cerdas itu dapat dilakukan identifikasi mekanisme keamanan yang tepat dari masalah yang paling sering terjadi dalam kelompok penerapan IOT.