SIARAN PERS

Inilah Cara Samsung Hadirkan Keamanan Data bagi Pengguna

Oleh Seungwon Shin (VP and Head of Security Team, Mobile eXperience Business, Samsung Electronics)

▲ Seungwon Shin,[1] VP dan Head of Security Team di Mobile eXperience Business, Samsung Electronics

Era Penuh Bahaya

Sekarang adalah waktu yang sangat baik bagi para penjahat dunia maya. Kondisinya saat ini ideal bagi siapa saja yang memiliki niat buruk dan memiliki pengetahuan teknis untuk menjalankannya.

Peningkatan jumlah pekerja *remote* juga berarti banyaknya orang yang memiliki ketergantungan pada Wi-Fi publik yang tidak aman. Arena baru seperti *blockchain* membuat pengguna yang awam dan bingung siap untuk menjadi sasaran penipuan. Serangan siber terus meningkat. Dan ini bukan hanya di tempat yang kita perkirakan. Peperangan dimulai dengan serangan digital pada infrastruktur penting, berbulan-bulan sebelum serangan fisik diluncurkan.

[1] Dr. Seungwon Shin adalah VP and Head of Security Team di Mobile eXperience Business, Samsung Electronics. Dia telah memimpin inovasi keamanan di seluruh ekosistem Samsung Galaxy, termasuk pengembangan secure AP dan Samsung Knox Vault. Dia juga mengawasi respons Samsung terhadap ancaman keamanan yang sedang berlangsung dengan perlindungan *real-time* dan prediksi ancaman, bekerja sama erat dengan mitra dan komunitas riset yang lebih luas. Dia adalah anggota INTERPOL DarkNet Working Group serta Ketua FIDO Korea Working Group. Sebelum bergabung dengan Samsung, dia menjabat sebagai Associate Professor di School of Electrical Engineering di KAIST, dengan spesialisasi Dark Web.

Semua peristiwa ini berlangsung, di saat sekarang ketika kita semakin banyak menggunakan smartphone dalam hidup kita. Smartphone telah menjadi dompet, kunci rumah, dan kartu identitas bagi kita. Sebuah gangguan tunggal dapat menghancurkan, jadi kini semakin penting bagi kita untuk memastikan keamanan perangkat yang kita miliki. Mari kita periksa hal-hal yang benar-benar membuat perangkat aman – sehingga Anda dapat keluar menikmati dunia dan hidup tenang, tanpa khawatir data pribadi jatuh ke tangan yang salah.

Apa Itu Keamanan… dan Apa Hal yang Tidak Aman

Pada titik ini, Anda mungkin berpikir bahwa Anda baik-baik saja, karena Anda telah melakukan pencegahan yang wajar. Akan tetapi ada banyak kesalahpahaman umum tentang keamanan. Anda tidak mengizinkan aplikasi membagikan nama, email, atau kebiasaan. Anda bahkan menonaktifkan izin pelacakan aplikasi. Bagus, tapi itu tidak berarti data sudah aman. Jangan mencampuradukkan privasi dan keamanan. Hal tersebut diibaratkan, menutup tirai rumah tidak akan ada gunanya jika seseorang menendang pintu rumah kita. Anda berpikir Anda telah memilih ekosistem seluler yang aman, yang serupa dengan taman bertembok. Tetapi peretas terus beradaptasi dengan target mereka. Wi-Fi yang tidak aman, penipuan rekayasa sosial – ini adalah ancaman nyata terlepas dari jenis ekosistem yang Anda gunakan.

Anda tidak membuka lampiran email yang mencurigakan. Bagus, tetapi ada serangan 'zero-click', yang membahayakan perangkat tanpa interaksi pengguna. Itu terjadi dengan Pegasus, spyware yang mengeksploitasi kelemahan dalam sistem pesan populer. Yang diperlukan hanyalah pengguna menerima pesan, dan peretas akan masuk. Merasa lebih aman daripada kondisi sebenarnya mengarah pada kelengahan – itulah yang diandalkan oleh penjahat dunia maya.

Memang meresahkan untuk berpikir bahwa ada begitu banyak ancaman dan tidak ada tempat yang aman. Namun itulah yang menginspirasi hasil kerja kami di Samsung Knox, platform keamanan kelas militer terdepan di industri kami yang disetujui oleh banyak pemerintah di seluruh dunia. Kami mencapai kepercayaan hingga di tingkat tersebut melalui pendekatan holistik dan berlapis-lapis perlindungan: kolaborasi terbuka, keamanan terintegrasi perangkat keras dan perangkat lunak, serta perlindungan *real-time*.

Kepercayaan Melalui Kolaborasi

Jika ada satu hal yang saya pelajari dari pekerjaan saya dengan INTERPOL, adalah bahwa kita lebih kuat dan lebih aman jika kita bekerja dengan satu sama lain. Kepercayaan dibangun melalui kolaborasi terbuka. Itulah salah satu keuntungan besar ekosistem Android. Siapa pun dapat memiliki akses ke *source code* OS Android, yang memungkinkannya untuk diperkuat secara kolektif. Ini memungkinkan beberapa nama besar di bidang teknologi untuk saling memeriksa dan mencari celah – dan bekerja sama untuk meningkatkan kapabilitas mereka.

Samsung bangga dengan model kemitraan dan kolaborasi terbuka ini, selain pekerjaan internal kami untuk senantiasa memperkuat sistem kami. Itu sebabnya kami bekerja sama dengan Google dan mengadakan pertemuan isu keamanan rutin untuk berbagi data ancaman satu sama lain. Kami juga bekerja dengan ratusan mitra untuk menstandardisasi keamanan untuk Android.

Perangkat Samsung Galaxy sendiri juga mendapat manfaat dari komunitas luas yang memahami ekosistem kami. Kami bekerja dengan akademisi dan peretas *white hat* melalui Mobile Security Rewards Program kami untuk mengidentifikasi dan menambal potensi kerentanan melalui pembaruan keamanan reguler kami, dan telah memberikan hadiah senilai lebih dari $3,5 juta untuk menghargai kolaborasi mereka yang berharga.

Dengan cara ini, kita dapat mengidentifikasi kelemahan atau bahkan memprediksinya dengan lebih baik sebelum menjadi masalah. Lebih banyak mata, lebih banyak kepala, akan menghasilkan solusi yang lebih baik. Membuka ekosistem kami tidak menghasilkan lebih banyak kerentanan, tetapi praktik keamanan yang lebih kuat dan lebih beragam.

Pendekatan Hulu ke Hilir Terintegrasi

Ini bukan hanya tentang perangkat lunak. Kami terus mengawasi setiap komponen mulai dari prosesor– kami dapat melakukannya sebagai perusahaan global terkemuka yang merancang dan memproduksi produknya sendiri. Anda aman sejak hari pertama menyalakan produk berkat perangkat keras yang dirancang khusus keamanannya dan perangkat lunak terisolasi yang terintegrasi di seluruh portofolio dan rantai pasokan kami. Itulah mengapa kami dapat yakin dengan integritas perangkat kami: perlindungan menyeluruh di semua tingkat pengalaman seluler, mulai dari chip di dalam produk hingga aplikasi yang Anda gunakan.

Seiring dengan kembalinya orang-orang ke dunia luar, ada risiko baru yang harus diwaspadai. Inilah sebabnya mengapa kami baru-baru ini melangkah lebih maju dengan Knox Vault, yang menggabungkan Secure Processor dengan Secure Memory Chip terbaru, untuk mengisolasi informasi paling penting (seperti PIN, kata sandi, biometrik, sertifikat digital, dan kunci kriptografik) dari isi lain perangkat untuk memastikan hal tersebut tidak pernah jatuh ke tangan yang salah. Misalnya, jika risiko keamanan utama terdeteksi pada perangkat, Samsung Knox akan mengunci layanan sensitif seperti Samsung Pay dan Samsung Pass untuk menyimpan data sebagaimana mestinya: hanya untuk mata penggunanya.

Perlindungan Setiap Saat

Jika Anda seperti saya, mungkin Anda jarang mematikan ponsel. Begitulah bagaimana beberapa orang mendapat masalah: beberapa perusahaan percaya bahwa sudah cukup menjalankan verifikasi keamanan hanya ketika ponsel dinyalakan. Itu sebabnya kami menjaga pengalaman seluler pengguna bahkan setelah tahap *boot up*. Penyerang tidak pernah beristirahat, jadi kita juga berlaku serupa.

Kami berkomitmen untuk menawarkan perlindungan *real-time* kepada pengguna. Setelah *booting,* teknologi Real-Time Kernel Protection (RKP) dan Defeat Exploit (DEFEX) kami terus bekerja untuk mendeteksi dan mencegah perubahan pada izin yang diberikan pengguna yang mencurigakan atau tidak sah. Kami memantau ancaman secara konstan dan bahkan memiliki tim Incident Response and Management, yang menggunakan pembelajaran mesin untuk memprediksi ancaman di masa depan.

Dan sementara banyak orang membeli ponsel baru setiap tahun, banyak yang suka memakai ponsel mereka untuk waktu yang lebih lama. Itu sebabnya kami merilis pembaruan keamanan reguler untuk menambal kerentanan apa pun, **hingga mencapai lima tahun setelah peluncuran perangkat.** Dalam lanskap keamanan siber yang terus berubah ini, orang yang ingin menggunakan ponsel mereka selama mungkin harus sama amannya dengan mereka yang menggunakan model terbaru.

Privasi yang Diinginkan, Keamanan yang Dibutuhkan

Gabungkan semuanya dan Anda akan memiliki pengalaman seluler yang cukup aman bagi para pemimpin dunia. Ini adalah fondasi keamanan yang dibangun dengan kolaborasi terbuka dan validasi industri, didukung oleh perlindungan perangkat keras dan perangkat lunak terkokoh yang pernah kami buat. Ini adalah keamanan yang Anda butuhkan.

Hanya dengan keamanan komprehensif yang ada, siapa pun dapat benar-benar menawarkan privasi yang transparan pada tingkat yang disesuaikan dengan prioritas masing-masing pengguna. Apa yang Anda lakukan dengan privasi itu adalah pilihan Anda. Anda bebas membuat pengalaman seluler sendiri sesuai selera, mengetahui bahwa kami akan selalu ada untuk membuat Anda tetap aman.

Dunia lebih terhubung dari sebelumnya, dan memiliki lebih banyak risiko. Akan tetapi juga tersedia lebih banyak peluang. Prioritas kami adalah menjaga Anda tetap terlindungi saat menjelajahi pengalaman baru. Dengan Samsung Galaxy, Anda bebas menjalani hidup – dengan privasi yang Anda inginkan dan keamanan yang Anda butuhkan.

###

Tentang Samsung Electronics Co., Ltd.
Samsung Electronics Co., Ltd menginspirasi dunia dan membentuk masa depan dengan ide-ide dan teknologi transformatif. Perusahaan ini mendefinisikan ulang dunia televisi, ponsel pintar, wearable, tablet, peralatan digital, sistem jaringan dan memori, sistem LSI, semikonduktor, dan solusi LED. Untuk berita terbaru, silakan kunjungi Samsung Newsroom di news.samsung.com.

Untuk keterangan lebih lanjut hubungi:
Jane Tjondro
Public Relations Professional
PT Samsung Electronics Indonesia
Email: j.tjondro@samsung.com